



Unable to locate subtitle

AWS Snowball Edge Guida per gli sviluppatori



AWS Snowball Edge Guida per gli sviluppatori: ***Unable to locate subtitle***

Copyright © 2026 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 delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è Snowball Edge?	1
Caratteristiche di Snowball Edge	1
Servizi correlati	2
Accesso al servizio Snowball Edge	3
Accedere a un dispositivo AWS Snowball Edge	3
Prezzi dello Snowball Edge	4
AWS monitoraggio di Snowball Edge	4
Risorse per utenti alle prime armi AWS Snowball Edge	4
informazioni sull'hardware del dispositivo	4
Configurazioni dei dispositivi	5
Specifiche del dispositivo	7
Hardware di rete supportato	11
Prerequisiti per l'utilizzo di Snowball Edge	13
Registrati per un Account AWS	15
Crea un utente con accesso amministrativo	15
Informazioni sul tuo ambiente	16
Lavorare con caratteri speciali	17
Crittografia Amazon S3 con AWS KMS	18
Crittografia Amazon S3 con crittografia lato server	23
Prerequisiti per l'utilizzo dell'adattatore Amazon S3 su Snowball Edge per processi di importazione ed esportazione	23
Prerequisiti per l'utilizzo dello storage compatibile con Amazon S3 su Snowball Edge	24
Prerequisiti per l'utilizzo delle istanze di calcolo su Snowball Edge	25
Come funziona Snowball Edge	27
Come funzionano i lavori di importazione	29
Come funzionano i lavori di esportazione	30
Come funzionano i processi di elaborazione e archiviazione locali	31
Come funzionano i job di elaborazione e archiviazione locali in cluster	31
Video e blog su Snowball Edge	32
Prezzi a lungo termine per i dispositivi Snowball Edge	33
Sostituzione dei dispositivi durante il periodo di tariffazione a lungo termine	33
Considerazioni sulla spedizione	35
Restrizioni di spedizione basate sulla regione	35
Nozioni di base	37

Creazione di un lavoro per ordinare un dispositivo Snowball Edge	38
Scelta di un tipo di lavoro	38
Scelta delle opzioni di elaborazione e archiviazione	40
Scelta delle funzionalità e delle opzioni	44
Scelta delle preferenze di sicurezza, spedizione e notifica	45
Rivedi il riepilogo del lavoro e crea il tuo lavoro	48
Annullamento di un lavoro	49
Clonazione di un lavoro per ordinare uno Snowball Edge	50
Ricevere lo Snowball Edge	51
Connessione alla rete locale	52
Ottenere le credenziali per accedere a Snowball Edge	54
Sbloccare Snowball Edge	55
Risoluzione dei problemi relativi allo sblocco di Snowball Edge	58
Configurazione degli utenti locali	58
Riavvio del dispositivo Snowball Edge	61
Spegnimento dello Snowball Edge	65
Restituzione del dispositivo	69
Spedizione per il reso	70
Corrieri di spedizione	70
Monitoraggio dello stato di importazione	80
Ottenere rapporti e registri sul completamento del lavoro	80
Migrazione di dati di grandi	84
Pianificazione di un trasferimento di grandi dimensioni	84
Passaggio 1: scopri cosa stai trasferendo sul cloud	85
Fase 2: Calcola la velocità di trasferimento desiderata	85
Fase 3: Stabilisci quanti Snowball Edge ti servono	85
Fase 4: Crea le tue offerte di lavoro	86
Passaggio 5: Separa i dati in segmenti di trasferimento	86
Calibrazione di un trasferimento di dati di grandi dimensioni	87
Creazione di un piano di migrazione dei dati di grandi dimensioni	88
Passaggio 1: scegli i dettagli della migrazione	89
Passaggio 2: scegli le tue preferenze di spedizione, sicurezza e notifica	94
Fase 3: Rivedi e crea il tuo piano	95
Utilizzo del piano di migrazione dei dati di grandi dimensioni	95
Pianificazione degli ordini di lavoro consigliata	95
Elenco dei lavori ordinati	98

Dashboard di monitoraggio	98
Utilizzo AWS OpsHub per gestire i dispositivi	99
Scaricamento AWS OpsHub	100
Sblocco di un dispositivo	100
Sblocco di un dispositivo localmente	101
Sblocco di un dispositivo da remoto	104
Verifica della firma di AWS OpsHub	107
Gestione dei servizi AWS	111
Avvio di un'istanza compatibile EC2 con Amazon	112
Arresto di un'istanza compatibile EC2 con Amazon	115
Avvio di un'istanza EC2 compatibile con Amazon	116
Lavorare con coppie di chiavi	117
Terminare un'istanza compatibile EC2 con Amazon	117
Gestione dei volumi EBS	118
Importazione di un'immagine nel dispositivo come AMI compatibile EC2 con Amazon	120
Eliminazione di uno snapshot	124
Annullamento della registrazione di un AMI	125
Gestione dei cluster	126
Configura lo storage compatibile con Amazon S3 su Snowball Edge con AWS OpsHub	127
Gestione dello storage S3	134
Gestione dell'interfaccia NFS	137
Riavvio del dispositivo	146
Gestione dei profili con AWS OpsHub	148
Spegnimento del dispositivo	148
Modifica dell'alias del dispositivo	151
Gestione dei certificati a chiave pubblica tramite OpsHub	151
Scarica il certificato a chiave pubblica utilizzando OpsHub	152
Rinnovo del certificato a chiave pubblica utilizzando OpsHub	152
Ricevere gli aggiornamenti del dispositivo	153
Aggiornamento AWS OpsHub	154
Automatizzazione delle attività di gestione con AWS OpsHub	154
Creazione e avvio di un'attività	155
Visualizzazione dei dettagli di un'attività	158
Eliminazione di un'attività	159
Impostazione dei time server NTP per il dispositivo	159
Configurazione e utilizzo del client Snowball Edge	161

Scaricamento e installazione del client Snowball Edge	161
Configurazione di un profilo per il client Snowball Edge	163
Ricerca della versione client Snowball Edge	166
Ottenere le credenziali	167
Avvio di un servizio su Snowball Edge	168
Interruzione di un servizio su Snowball Edge	168
Visualizzazione e download dei log	169
Visualizzazione dello stato del dispositivo	171
Visualizzazione dello stato dei servizi	172
Visualizzazione dello stato delle funzionalità	177
Impostazione dei server temporali	178
Controllo delle fonti di orario	178
Aggiornamento dei time server	180
Convalida dei tag NFC	181
Aggiornamento delle dimensioni MTU	181
Trasferimento di file tramite l'adattatore S3	183
Scaricamento e installazione di AWS CLI	184
Installa AWS CLI su sistemi operativi Linux	184
Installa AWS CLI su sistemi operativi Windows	184
Utilizzo delle operazioni AWS CLI e dell'API sui dispositivi Snowball Edge	185
Autorizzazione con l'interfaccia API Amazon S3 per AWS Snowball Edge	185
Acquisizione e utilizzo delle credenziali locali di Amazon S3	186
Configurazione dell'adattatore S3 come endpoint AWS CLI	186
Funzionalità di Amazon S3 non supportate per l'adattatore S3	188
Suddivisione in batch di file di piccole dimensioni	188
AWS CLI Comandi supportati per il trasferimento dei dati	191
AWS CLI Comandi supportati per Amazon S3	192
Azioni API REST di Amazon S3 supportate per il trasferimento dei dati	196
Gestione dell'interfaccia NFS	198
Configurazione NFS per Snowball Edge	199
Configurare Snowball Edge per l'interfaccia NFS	199
Avvio del servizio NFS su Snowball Edge	201
Montaggio degli endpoint NFS sui computer client	203
Arresto dell'interfaccia NFS	203
Utilizzo di istanze EC2 di calcolo compatibili con Amazon	204
Descrizione delle istanze compatibili EC2 con Amazon	205

Prezzi delle istanze EC2	205
Utilizzo AMIs su Snowball Edge	206
Aggiungere un AMI al momento dell'ordine	208
Aggiungere un AMI da Marketplace AWS	208
Aggiungere un AMI dopo aver ricevuto il dispositivo	213
Aggiungere un'AMI Microsoft Windows a Snowball Edge	213
Importazione di un'immagine di macchina virtuale in uno Snowball Edge	215
Esportazione dell'ultima AMI Amazon Linux 2 per Snowball Edge	216
Importazione di un'immagine VM su un dispositivo Snowball Edge	217
Passaggio 1: preparare l'immagine della macchina virtuale e caricarla sul dispositivo Snowball Edge	217
Fase 2: configurare le autorizzazioni necessarie su Snowball Edge	219
Fase 3: Importazione dell'immagine della macchina virtuale come istantanea su Snowball Edge	226
Fase 4: Registrare l'istantanea come AMI su Snowball Edge	227
Fase 5: Avviare un'istanza dall'AMI su Snowball Edge	228
Azioni AMI aggiuntive per Snowball Edge	229
Utilizzo di AWS CLI e API Operations	233
Configurazioni di rete per le istanze di calcolo	234
Prerequisiti DNI e VNI	235
Configurazione di un'interfaccia di rete virtuale (VNI)	236
Configurazione di un DNI	237
Utilizzo di SSH per connettersi a un'istanza di calcolo	240
Trasferimento di dati da istanze di calcolo a bucket sullo stesso dispositivo	241
Avvio automatico delle istanze	242
Creazione di una configurazione di EC2 avvio compatibile	242
Aggiornamento di una configurazione di EC2 avvio compatibile	243
Eliminazione di una configurazione di avvio compatibile EC2	243
Elenco delle EC2 configurazioni di avvio compatibili	243
Creazione di un'interfaccia di rete virtuale su Snowball Edge	244
Descrizione delle interfacce di rete virtuali	245
Aggiornamento di un'interfaccia di rete virtuale	246
Eliminazione di un'interfaccia di rete virtuale	247
Utilizzo di un endpoint EC2 compatibile con Amazon	247
Specificare l'endpoint compatibile come endpoint EC2 AWS CLI	248
Comandi compatibili supportati EC2 AWS CLI	249

Operazioni API EC2 compatibili con Amazon supportate	264
Istanze EC2 compatibili con avvio automatico	267
Utilizzo di IMDS for Snow con istanze compatibili EC2	269
Versioni IMDS su Snowball Edge	270
Esempi di recupero dei metadati delle istanze utilizzando e IMDSV1 IMDSv2	274
Utilizzo dello storage a blocchi con istanze compatibili EC2	278
Controllo del traffico di rete con gruppi di sicurezza	280
Metadati di istanza EC2 e dati utente compatibili con quelli supportati	280
Dati utente dell'istanza di computer	282
Arresto delle istanze EC2 compatibili	283
Utilizzo su istanze compatibili AWS IoT Greengrass EC2	284
Configurazione -compatible per EC2 AWS IoT Greengrass	284
Installazione AWS IoT Greengrass su un'istanza EC2 compatibile su Snowball Edge	285
Usando AWS Lambda	288
Guida introduttiva a Lambda	288
Prerequisiti per AWS IoT Greengrass	288
Prerequisiti per Lambda	289
Implementazione di una funzione Lambda su un dispositivo Snowball Edge	290
Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge	291
Ordina uno storage compatibile con Amazon S3 su Snowball Edge	294
Configurazione e avvio dello storage compatibile con Amazon S3 su Snowball Edge	295
Prerequisiti	295
Configurazione dell'ambiente locale	295
Avvio dello storage compatibile con Amazon S3 sul servizio Snowball Edge	296
Visualizzazione di informazioni sugli endpoint	299
Utilizzo dei bucket S3	301
Utilizzo del AWS CLI	301
Utilizzo dell'SDK Java	302
Formato Bucket ARN	303
Formato di posizione del bucket	303
Determinare l'accesso al bucket	304
Recupero di un elenco di bucket o bucket regionali	304
Recupero di un bucket	306
Creazione di un bucket S3	307
Eliminazione di un bucket	307

Creazione e gestione di una configurazione del ciclo di vita degli oggetti utilizzando il AWS	
CLI	308
INSERISCI una configurazione del ciclo di vita su un bucket Snowball Edge	309
Copia di un oggetto	310
Elenco degli oggetti	312
Recupero di un oggetto	314
Eliminazione di oggetti	316
Azioni API REST supportate per lo storage compatibile con Amazon S3 su Snowball Edge	317
Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge con un cluster di dispositivi	
Snow	319
Quorum del cluster Snowball Edge	322
Riconnessione di un nodo del cluster non disponibile	323
Sostituzione di un nodo in un cluster	324
Configurazione dello storage compatibile con Amazon S3 sulle notifiche degli eventi Snowball	
Edge	336
Configurazione delle notifiche SMTP locali	339
Configurazione di Snowball Edge per le notifiche locali	339
Utilizzo di Amazon EKS Anywhere su Snowball Edge	341
Azioni da completare prima di ordinare un dispositivo Snowball Edge per Amazon EKS	
Anywhere on Snow AWS	343
Crea un'AMI Ubuntu EKS Distro	344
Costruisci un AMI Harbor	344
Ordinazione di un dispositivo Snowball Edge da utilizzare con Amazon EKS Anywhere on Snow	
AWS	344
Configurazione ed esecuzione di Amazon EKS Anywhere su dispositivi Snowball Edge	345
Configurazione iniziale	345
Configurazione ed esecuzione automatica di Amazon EKS Anywhere	346
Configurazione ed esecuzione manuale di Amazon EKS Anywhere	346
Configurazione di Amazon EKS Anywhere on AWS Snow per il funzionamento disconnesso ...	356
Configurazione del registro Harbor su un dispositivo Snowball Edge	356
Usa il registro Harbor sull'istanza di amministrazione di Amazon EKS Anywhere su Snowball	
Edge	357
Creazione e manutenzione di cluster	357
Procedure consigliate per la creazione di cluster su Snowball Edge	357
Aggiornamento dei cluster su Snowball Edge	357
Pulizia delle risorse del cluster su Snowball Edge	358

Utilizzo locale di IAM	359
Utilizzo di AWS CLI e API Operations	360
Comandi IAM AWS CLI supportati	360
Operazioni API IAM supportate su Snowball Edge	362
Versione e grammatica delle policy IAM supportate su Snowball Edge	364
Esempi di policy IAM su Snowball Edge	364
Consentire la GetUser chiamata per un utente campione su Snowball Edge tramite l'API IAM	365
Consentire l'accesso completo all'API Amazon S3 su Snowball Edge	365
Consentire l'accesso in lettura e scrittura a un bucket Amazon S3 su Snowball Edge	366
.....	366
Consentire l'accesso a elenchi, get e put a un bucket Amazon S3 su Snowball Edge	366
Consentire l'accesso completo all' EC2API Amazon su Snowball Edge	367
Consentire l'accesso per avviare e arrestare istanze EC2 compatibili con Amazon su Snowball Edge	367
Negare le chiamate verso uno Snowball Edge, DescribeLaunchTemplates ma consentire Describelmages a tutte le chiamate di farlo	368
Criteri per le chiamate API su Snowball Edge	369
TrustPolicy esempio su Snowball Edge	369
Usando AWS STS	371
Utilizzo delle operazioni AWS CLI e dell'API su Snowball Edge	371
AWS STSAWS CLI Comandi supportati su Snowball Edge	372
Esempio di comando per assumere un ruolo su Snowball Edge	372
Operazioni AWS STS API supportate su Snowball Edge	372
Gestione dei certificati a chiave pubblica	374
Elencare il certificato	374
Ottenere certificati	375
Eliminazione dei certificati	375
Requisiti delle porte per i servizi AWS	377
Utilizzo di Snowball Edge Device Management per gestire i dispositivi	379
Scelta dello stato di gestione dei dispositivi Snowball Edge quando si ordina uno Snowball Edge	380
Attivazione della gestione dei dispositivi Snowball Edge su Snowball Edge	381
Aggiungere le autorizzazioni per Snowball Edge Device Management a un ruolo IAM su Snowball Edge	382
Comandi CLI di Snowball Edge Device Management	383

Creazione di un'attività di gestione dei dispositivi Snowball Edge	384
Verifica dello stato di un'attività di Snowball Edge Device Management	385
Verifica delle informazioni sul dispositivo con Snowball Edge Device Management	386
Verifica degli stati delle istanze EC2 compatibili con Snowball Edge Device Management ...	387
Visualizzazione dei metadati delle attività di Snowball Edge Device Management	389
Annullamento di un'attività di gestione dei dispositivi Snowball Edge	390
Elenco dei comandi e della sintassi di Snowball Edge Device Management	391
Elenco Snowball Edge disponibile per la gestione remota	391
Elenco dello stato delle attività su tutti i dispositivi	392
Elenco delle risorse disponibili sui dispositivi	394
Elenco dei tag dei dispositivi o delle attività	395
Elenco delle attività per stato	396
Applicazione di tag ad attività o dispositivi	397
Rimuovere i tag dalle attività o dai dispositivi	397
Aggiornamento dei dispositivi Snowball Edge	399
Prerequisiti per l'aggiornamento del software	400
Scaricamento degli aggiornamenti	400
Installazione degli aggiornamenti	404
Aggiornamento del certificato SSL	411
Aggiornamento di Amazon Linux 2 AMIs	412
Comprendere i lavori	413
Dettagli del lavoro	414
Stati del processo	416
Stati dei job del cluster Snowball Edge	419
Processi di importazione	421
Processi di esportazione	421
Utilizzo delle chiavi oggetto Amazon S3 con processi di esportazione	423
Procedure consigliate per i lavori di esportazione	431
Informazioni sui processi di elaborazione e archiviazione locali	431
Informazioni sui processi di archiviazione locale	432
Informazioni sullo storage locale su un cluster di dispositivi	432
Best practice	433
Consigli sulla sicurezza	433
Le migliori pratiche per la gestione delle risorse	434
Raccomandazioni sulle prestazioni di trasferimento dei dati	434
Miglioramento della velocità di trasferimento dei dati	436

Sicurezza	438
Protezione dei dati	439
Protezione dei dati nel cloud	440
Protezione dei dati sul tuo dispositivo	444
Identity and Access Management	447
Controllo degli accessi per console e lavori	447
Registrazione e monitoraggio	490
Convalida della conformità	490
Resilienza	491
Sicurezza dell'infrastruttura	492
Convalida dei dati	493
Inventario locale dei file	493
Cause comuni degli errori di convalida dei dati con Snowball Edge	493
Convalida manuale dei dati dopo l'importazione in Amazon S3	494
Notifiche	496
In che modo Snowball Edge utilizza Amazon SNS	496
Crittografia degli argomenti SNS per le modifiche allo stato del lavoro	496
Impostazione di una politica chiave KMS gestita dal cliente	497
Esempi di notifiche SNS	498
Registrazione con AWS CloudTrail	511
AWS Snowball Edge informazioni in CloudTrail	511
Comprensione delle voci dei file di log di	512
Quote	514
Disponibilità regionale per AWS Snowball Edge	514
Limitazioni per i lavori AWS Snowball Edge	515
Limiti di velocità su AWS Snowball Edge	516
Limite di connessione dell'adattatore Amazon Snow S3	516
Limitazioni al trasferimento di dati locali	516
Quote per le istanze di calcolo	517
Calcolo delle quote di storage delle risorse su Snowball Edge	517
Limitazioni delle risorse di elaborazione condivise su Snowball Edge	520
Limitazioni di spedizione	521
Limitazioni all'elaborazione dei dispositivi restituiti per i lavori di importazione	521
Risoluzione dei problemi	523
Identifica un dispositivo	524
Risoluzione dei problemi di avvio	525

Risoluzione dei problemi relativi allo schermo LCD durante l'avvio	526
Risoluzione dei problemi relativi al display E Ink durante l'avvio	528
Risoluzione dei problemi di connessione	528
Risoluzione dei problemi relativi ai unlock-device comandi	529
Risoluzione dei problemi relativi ai file manifest	529
Risoluzione dei problemi relativi alle credenziali	530
Risoluzione dei problemi: impossibile individuare le credenziali AWS CLI	530
Messaggio di errore per la risoluzione dei problemi: verifica la chiave di accesso segreta e la firma	530
Risoluzione dei problemi relativi al trasferimento dei dati	531
Risoluzione dei problemi relativi ai processi di importazione	531
Risoluzione dei problemi relativi ai processi di esportazione	532
Risoluzione dei problemi relativi all'interfaccia NFS	533
Errore di accesso negato dall'interfaccia S3	534
Errore 403 proibito dall'interfaccia S3	537
Risoluzione dei problemi AWS CLI	542
Messaggio AWS CLI di errore per la risoluzione dei problemi: «Il profilo non può essere nullo»	542
Risoluzione dell'errore null pointer durante il trasferimento di dati con AWS CLI	542
Risoluzione dei problemi relativi alle istanze di calcolo	543
Interfaccia di rete virtuale con indirizzo IP 0.0.0.0	543
Il dispositivo Snowball Edge smette di rispondere all'avvio di un'istanza di calcolo di grandi dimensioni	543
La mia istanza su Snowball Edge ha un volume root	544
Errore nel file con chiave privata non protetto	544
Cronologia dei documenti	545
.....	dliii

Che cos'è Snowball Edge?

Snowball Edge è un dispositivo con storage integrato e potenza di calcolo per funzionalità selezionate. AWS Snowball Edge è in grado di elaborare i dati localmente, eseguire carichi di lavoro di edge computing e trasferire dati da o verso. Cloud AWS

Ogni dispositivo Snowball Edge può trasportare dati a velocità superiori a quelle di Internet. Il trasporto viene effettuato spedendo i dati nei dispositivi attraverso un corriere regionale. Gli elettrodomestici sono robusti e completi di etichette di spedizione E Ink.

I dispositivi Snowball Edge offrono due opzioni di configurazione dei dispositivi: Storage Optimized 210 TB e Compute Optimized. Quando questa guida si riferisce ai dispositivi Snowball Edge, si riferisce a tutte le opzioni del dispositivo. Quando informazioni specifiche si riferiscono solo a una o più configurazioni opzionali di dispositivi, vengono richiamate specificamente. Per ulteriori informazioni, consulta [Configurazioni dei dispositivi Snowball Edge](#).

Argomenti

- [Caratteristiche di Snowball Edge](#)
- [Servizi correlati a Snowball Edge](#)
- [Accesso al servizio Snowball Edge](#)
- [Prezzi dello Snowball Edge](#)
- [AWS monitoraggio di Snowball Edge](#)
- [Risorse per utenti alle prime armi AWS Snowball Edge](#)
- [AWS Snowball Edge informazioni sull'hardware del dispositivo](#)
- [Prerequisiti per l'utilizzo di Snowball Edge](#)

Caratteristiche di Snowball Edge

I dispositivi Snowball Edge hanno le seguenti caratteristiche:

- Grandi capacità di archiviazione o funzionalità di elaborazione per i dispositivi. Dipende dalle opzioni scelte al momento della creazione del lavoro.
- Adattatori di rete con velocità di trasferimento fino a 100 Gbit/secondo.
- La crittografia viene applicata, proteggendo i dati inattivi e in transito fisico.

- Puoi importare o esportare dati tra i tuoi ambienti locali e Amazon S3 e trasportare fisicamente i dati con uno o più dispositivi senza utilizzare Internet.
- I dispositivi Snowball Edge sono robusti a sé stanti. Il display E Ink integrato cambia per mostrare l'etichetta di spedizione quando il dispositivo è pronto per la spedizione.
- I dispositivi Snowball Edge sono dotati di un display LCD integrato che può essere utilizzato per gestire le connessioni di rete e ottenere informazioni sullo stato del servizio.
- Puoi raggruppare i dispositivi Snowball Edge per processi di archiviazione ed elaborazione locali per ottenere la durabilità dei dati su 3-16 dispositivi e aumentare o ridurre localmente lo storage su richiesta.
- Puoi usare Amazon EKS Anywhere sui dispositivi Snowball Edge per carichi di lavoro Kubernetes.
- I dispositivi Snowball Edge dispongono di endpoint compatibili con Amazon S3 e EC2 Amazon, che consentono casi d'uso programmatici.
- I dispositivi Snowball Edge supportano i nuovi tipi di sbe-g istanza sbe1sbe-c, e, che puoi utilizzare per eseguire istanze di calcolo sul dispositivo utilizzando Amazon Machine Images (). AMIs
- Snowball Edge supporta i seguenti protocolli di trasferimento dati per la migrazione dei dati:
 - NFSv3
 - NFSv4
 - NFSv4.1.
 - Amazon S3 su HTTP o HTTPS (tramite API compatibile con la versione AWS CLI 1.16.14 e precedenti)

Servizi correlati a Snowball Edge

È possibile utilizzare un AWS Snowball Edge dispositivo con i seguenti AWS servizi correlati:

- Adattatore Amazon S3: da utilizzare per il trasferimento programmatico di dati in entrata e in uscita AWS utilizzando l'API Amazon S3 per Snowball Edge, che supporta un sottoinsieme di operazioni API di Amazon S3. In questo ruolo, i dati vengono trasferiti al dispositivo Snow per tuo AWS conto e il dispositivo ti viene spedito (per un lavoro di esportazione), oppure ti AWS spedisce un dispositivo Snow vuoto e tu trasferisci i dati dalle tue fonti locali al dispositivo e li rispedisci a AWS (per un processo di importazione)»
- Storage compatibile con Amazon S3 su Snowball Edge: utilizzalo per supportare le esigenze di dati di servizi di elaborazione come Amazon, Amazon EKS EC2 Anywhere on Snow e altri. Questa

funzionalità è disponibile sui dispositivi Snowball Edge e offre un set di API Amazon S3 esteso e funzionalità come una maggiore resilienza con configurazione flessibile del cluster da 3 a 16 nodi, gestione locale dei bucket e notifiche locali.

- Amazon EC2: esegui istanze di calcolo su un dispositivo Snowball Edge utilizzando l'endpoint EC2 compatibile con Amazon, che supporta un sottoinsieme delle operazioni dell'API Amazon. EC2 Per ulteriori informazioni sull'utilizzo di Amazon EC2 in AWS, consulta [Guida introduttiva alle istanze Amazon EC2 Linux](#).
- Amazon EKS Anywhere on Snow: crea e gestisci cluster Kubernetes su dispositivi Snowball Edge. Consultare [Utilizzo di Amazon EKS Anywhere sulla AWS neve](#).
- AWS Lambda con tecnologia AWS IoT Greengrass: richiama le funzioni Lambda basate sullo storage compatibile con Amazon S3 sulle azioni di storage Snowball Edge eseguite su un dispositivo. AWS Snowball Edge Per ulteriori informazioni sull'uso di Lambda, consulta la Guida per [Utilizzo AWS Lambda con un AWS Snowball Edge](#) gli [AWS Lambda sviluppatori](#).
- Amazon Elastic Block Store (Amazon EBS): fornisce volumi di storage a livello di blocco da utilizzare con istanze compatibili. EC2 Per ulteriori informazioni, consulta la sezione relativa ad [Amazon Elastic Block Store \(Amazon EBS\)](#).
- AWS Identity and Access Management (IAM): utilizza questo servizio per controllare in modo sicuro l'accesso alle risorse. AWS Per ulteriori informazioni, consulta [Cos'è IAM?](#)
- AWS Security Token Service (AWS STS) — Richiedi credenziali temporanee con privilegi limitati per gli utenti IAM o per gli utenti autenticati (utenti federati). Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).
- Amazon EC2 Systems Manager: utilizza questo servizio per visualizzare e controllare la tua infrastruttura su AWS. Per ulteriori informazioni, vedere [Cos'è AWS Systems Manager?](#)

Accesso al servizio Snowball Edge

Puoi utilizzare [Console di gestione della famiglia di servizi AWS Snow](#) o l'API di gestione dei lavori per creare e gestire i lavori. Per ulteriori informazioni sull'uso di [Console di gestione della famiglia di servizi AWS Snow](#), consulta [Guida introduttiva a Snowball Edge](#). Per informazioni sull'API per la gestione dei job, consulta [Job Management API Reference per Snowball Edge](#).

Accedere a un dispositivo AWS Snowball Edge

Una volta che il dispositivo Snowball Edge è sul posto, puoi configurarlo con un indirizzo IP utilizzando lo schermo LCD, quindi puoi sbloccarlo utilizzando il client Snowball Edge oppure.

AWS OpsHub Quindi, puoi eseguire operazioni di trasferimento dati o edge computing. Per ulteriori informazioni, vedere [Ricezione di Snowball Edge](#).

Prezzi dello Snowball Edge

Per informazioni sui prezzi e le tariffe associati al servizio e ai relativi dispositivi, consulta la pagina [AWS Snowball Edge Prezzi](#).

AWS monitoraggio di Snowball Edge

AWS monitorerà il dispositivo Snow e potrebbe raccogliere metriche e informazioni sull'utilizzo quando il dispositivo Snow è collegato a un Regione AWS. Se il dispositivo Snow non è collegato a Regione AWS, non AWS monitorerà il dispositivo Snow.

Se AWS rileva un problema irreparabile ed è necessario sostituire l'attrezzatura fisica, AWS ti avviserà. Potrai quindi inserire un lavoro sostitutivo che spediremo al tuo sito. Non è previsto alcun costo aggiuntivo, poiché il monitoraggio dei dispositivi Snow è incluso nel costo del servizio dei dispositivi Snow.

Risorse per utenti alle prime armi AWS Snowball Edge

Se utilizzi per la prima volta il servizio AWS Snowball Edge, ti consigliamo di leggere le seguenti sezioni nell'ordine:

1. Per informazioni sui tipi e le opzioni dei dispositivi, consulta [AWS Snowball Edge informazioni sull'hardware del dispositivo](#)
2. Per ulteriori informazioni sui vari tipi di processi, consulta [Informazioni sui job di Snowball Edge](#).
3. Per una end-to-end panoramica su come utilizzare un AWS Snowball Edge dispositivo, vedere [Come AWS Snowball Edge funziona](#).
4. Quando è tutto pronto per iniziare, consulta [Guida introduttiva a Snowball Edge](#).
5. Per informazioni sull'utilizzo di istanze di calcolo su un dispositivo, consulta [Utilizzo di istanze EC2 di calcolo compatibili con Amazon su Snowball Edge](#).

AWS Snowball Edge informazioni sull'hardware del dispositivo

Tutti i dispositivi Snowball Edge condividono caratteristiche fisiche, come dimensioni e peso, ma contengono diversi tipi di hardware in base all'uso previsto. I dispositivi progettati per il trasferimento

dei dati sono configurati con più spazio di archiviazione e i dispositivi progettati per l'elaborazione sono configurati con più memoria virtuale CPUs . Questa sezione fornisce informazioni sulle caratteristiche fisiche dei dispositivi Snowball Edge e sulle relative specifiche di elaborazione e archiviazione.

Argomenti

- [Configurazioni dei dispositivi Snowball Edge](#)
- [AWS Snowball Edge specifiche del dispositivo](#)
- [Hardware di rete supportato da Snowball Edge](#)

Configurazioni dei dispositivi Snowball Edge

I dispositivi Snowball Edge offrono le seguenti opzioni per le configurazioni dei dispositivi:

- 210 TB ottimizzati per lo storage Snowball Edge: questo dispositivo opzionale Snowball Edge offre 210 TB di capacità di storage utilizzabile.
- Snowball Edge ottimizzato per il calcolo: questo dispositivo Snowball Edge (con AMD EPYC Gen2) offre la massima funzionalità di elaborazione, con un massimo di 104 vCPUs, 416 GB di memoria e 28 TB di SSD dedicato per le istanze di calcolo. NVMe

Note

Quando si utilizza uno storage compatibile con Amazon S3 su Snowball Edge su questi dispositivi, lo storage utilizzabile può variare. Vedi [Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge per la capacità di storage con lo storage compatibile con Amazon S3 su Snowball Edge](#).

Per ulteriori informazioni sulle funzionalità di calcolo di queste tre opzioni, consulta [Utilizzo di istanze EC2 di calcolo compatibili con Amazon su Snowball Edge](#). [La creazione di Job e le differenze di capacità del disco in terabyte sono descritte qui](#).

Note

Quando ci riferiamo ai dispositivi Snowball Edge, ciò include tutte le varianti opzionali del dispositivo. Quando le informazioni si riferiscono a una o più configurazioni opzionali specifiche, ne facciamo esplicita menzione.

Nella tabella seguente vengono riepilogate le differenze tra le varie opzioni del dispositivo. Per informazioni sulle specifiche hardware, consulta [AWS Snowball Edge specifiche del dispositivo](#).

	210 TB ottimizzati per lo storage con Snowball Edge	Snowball Edge ottimizzato per il calcolo con AMD EPYC Gen2 e NVME
CPU	AMD Rome, 64 core, 2 GHz	AMD Rome, 64 core, 2 GHz
v CPUs	104	104
Memoria utilizzabile	416 GB	416 GB
Scheda di sicurezza	Sì	Sì
SSD	210 TB NVMe	28 TB NVMe
HDD utilizzabile	Non applicabile	Non applicabile
Interfacce di rete	• 2x 10 Gbit — RJ45 (uno utilizzabile) • 1 x 25 Gbit — SFP28 • 1 x 100 Gbit — QSFP28	• 2x 10 Gbit — RJ45 (uno utilizzabile) • 1 x 25 Gbit — SFP28 • 1 x 100 Gbit — QSFP28
Caratteristiche di sicurezza fisica	• Viti magnetiche nascoste • Switch anti-intrusione • Tag NFC • Inserti anti-manomissione • App Android per il rilevamento di manomissioni	• Viti magnetiche nascoste • Switch anti-intrusione • Tag NFC • Inserti anti-manomissione • App Android per il rilevamento di manomissioni

	210 TB ottimizzati per lo storage con Snowball Edge	Snowball Edge ottimizzato per il calcolo con AMD EPYC Gen2 e NVME
	• Rivestimento conforme	• Rivestimento conforme

AWS Snowball Edge specifiche del dispositivo

In questa sezione, puoi trovare le specifiche per i tipi di AWS Snowball Edge dispositivi e l'hardware.

Argomenti

- [Specifiche di Snowball Edge Storage Optimized da 210 TB](#)
- [Specifiche del dispositivo Snowball Edge Compute Optimized](#)

Specifiche di Snowball Edge Storage Optimized da 210 TB

La tabella seguente contiene le specifiche hardware per i dispositivi Snowball Edge Storage Optimized da 210 TB.

Elemento	Specifiche di Snowball Edge Storage Optimized da 210 TB
Specifiche di calcolo e memoria	
CPU	104 v CPUs
RAM	416 GB
Specifiche di archiviazione	
Capacità di archiviazione NVME	210 TB utilizzabili (per il trasferimento di oggetti e dati NFS)
Capacità di archiviazione SSD	Nessuno

Elemento	Specifiche di Snowball Edge Storage Optimized da 210 TB
Specifiche dell'alimentatore	
Alimentazione	Regioni AWS Negli Stati Uniti: NEMA 5—15p 100—220 volt. In tutte le regioni, è incluso un cavo di alimentazione AWS
Consumo energetico	304 watt per un caso d'uso medio, sebbene l'alimentatore abbia una potenza nominale di 1200 watt
Tensione	100 – 240 V CA
Frequenza	47/63 Hz
Connessione dati e di rete	2x 10 Gbit — RJ45 (uno utilizzabile) 1 x 25 Gbit — SFP28 1 x 100 Gbit — QSFP28
Cavi	Ogni AWS Snowball Edge dispositivo viene fornito con cavi di alimentazione specifici per ogni paese. Non vengono forniti altri cavi o ottiche. Per ulteriori informazioni, consulta Hardware di rete supportato da Snowball Edge .
Requisiti termici	AWS Snowball Edge i dispositivi sono progettati per le operazioni d'ufficio e sono ideali per le operazioni dei data center.
Rumorosità	In media, un AWS Snowball Edge dispositivo produce 68 decibel di suono, in genere più basso rispetto a un aspirapolvere o alla musica in salotto.
Specifiche di dimensioni e peso	
Weight	22,54 Kg (49.7 libbre)
Altezza	394 mm (15,5 pollici)

Elemento	Specifiche di Snowball Edge Storage Optimized da 210 TB
Larghezza	265 mm (10,6 pollici)
Lunghezza	718 mm (28,3 pollici)
Specifiche ambientali	
Vibrazione	Uso non operativo equivalente a ASTM D4169 Truck level I 0,73 GRMS
Scossa	Uso operativo equivalente a 70G (MIL-S-901)
	Uso non operativo equivalente a 50G (ISTA-3A)
Altitude (Altitudine)	Uso operativo equivalente a 0—3.000 metri (0—10.000 piedi)
	Uso non operativo equivalente a 0—12.000 metri
Intervallo di temperatura	0—30 °C (operativo)

Specifiche del dispositivo Snowball Edge Compute Optimized

Elemento	Specifiche ottimizzate per Snowball Edge Compute
Specifiche di calcolo e memoria	
CPU	104 v CPUs
RAM	512 GB di RAM (fino a 416 GB di RAM - utilizzabile dal cliente)
Specifiche di archiviazione	
Capacità di archiviazione SSD	SSD DA 28 TB NVMe
Specifiche dell'alimentatore	

Elemento	Specifiche ottimizzate per Snowball Edge Compute
Alimentazione	Regioni AWS Negli Stati Uniti: NEMA 5—15p 100—220 volt. In tutte le regioni, è incluso un cavo di alimentazione AWS
Consumo energetico	304 watt per un caso d'uso medio, sebbene l'alimentatore abbia una potenza nominale di 1200 watt
Tensione	100 – 240 V CA
Frequenza	47/63 Hz
Connessione dati e di rete	2x 10 Gbit — RJ45 (uno utilizzabile) 1 x 25 Gbit — SFP28 1 x 100 Gbit — QSFP28
Cavi	Ogni AWS Snowball Edge dispositivo viene fornito con cavi di alimentazione specifici per ogni paese. Non vengono forniti altri cavi o ottiche. Per ulteriori informazioni, consulta Hardware di rete supportato da Snowball Edge .
Requisiti termici	AWS Snowball Edge i dispositivi sono progettati per le operazioni d'ufficio e sono ideali per le operazioni dei data center.
Rumorosità	In media, un AWS Snowball Edge dispositivo produce 68 decibel di suono, in genere più basso rispetto a un aspirapolvere o alla musica in salotto.
Specifiche di dimensioni e peso	
Weight	22,54 Kg (49.7 libbre)
Altezza	394 mm (15,5 pollici)
Larghezza	265 mm (10,6 pollici)

Elemento	Specifiche ottimizzate per Snowball Edge Compute
Lunghezza	718 mm (28,3 pollici)
Specifiche ambientali	
Vibrazione	Uso non operativo equivalente a ASTM D4169 Truck level I 0,73 GRMS
Scossa	Uso operativo equivalente a 70G (MIL-S-901) Uso non operativo equivalente a 50G (ISTA-3A)
Altitude (Altitudine)	Uso operativo equivalente a 0—3.000 metri (0—10.000 piedi) Uso non operativo equivalente a 0—12.000 metri
Intervallo di temperatura	0—45 °C (operativo)

Hardware di rete supportato da Snowball Edge

Per utilizzare il AWS Snowball Edge dispositivo, sono necessari cavi di rete propri. Per RJ45 i cavi, non ci sono raccomandazioni specifiche. È stata verificata la compatibilità dei cavi e dei moduli SFP+ e QSFP+ di Mellanox e Finisar con il dispositivo.

Dopo aver aperto il pannello posteriore del AWS Snowball Edge dispositivo, vengono visualizzate porte di rete simili a quelle mostrate nella schermata seguente.



È possibile utilizzare una sola interfaccia di rete sul AWS Snowball Edge dispositivo alla volta. Quindi utilizza una qualsiasi delle porte per supportare il seguente hardware di rete.

SFP

Questa porta fornisce un' SFP28 interfaccia 10G/25G compatibile con i moduli ricetrasmittitori SFP + SFP28 e i cavi in rame a collegamento diretto (DAC). Occorre fornire i propri ricetrasmittitori e cavi DAC.

- Per il funzionamento 10G, puoi utilizzare qualsiasi opzione SFP+. Esempi includono:
 - Ricetrasmittitore 10Gbase-LR (fibra monomodale)
 - Ricetrasmittitore 10Gbase-SR (fibra multi-mode)
 - Cavo DAC SFP+
- Per il funzionamento a 25G, è possibile utilizzare qualsiasi opzione. SFP28 Esempi includono:
 - Ricetrasmittitore 25Gbase-LR (fibra monomodale)
 - Ricetrasmittitore 25Gbase-SR (fibra multi-mode)
 - SFP28 Cavo DAC



QSFP

Questa porta offre un'interfaccia QSFP+40G sui dispositivi ottimizzati per lo storage e un'interfaccia QSFP+40/50/100G sui dispositivi ottimizzati per il calcolo. Entrambi compatibili con moduli transceiver QSFP+ e cavi DAC. Occorre fornire i propri ricetrasmittitori e cavi DAC. Considerare i seguenti esempi:

- Ricetrasmittitore 40Gbase- LR4 (fibra monomodale)
- Ricetrasmittitore 40Gbase- (fibra multimodale) SR4
- DAC QSFP+

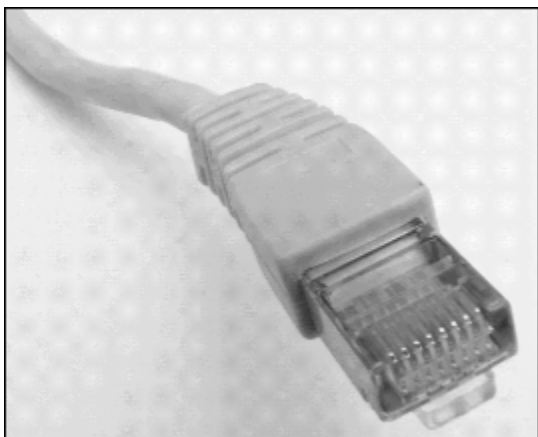


RJ45

Questa porta fornisce funzionamento 1Gbase-TX/10Gbase-TX. È collegato tramite cavo UTP terminato con un connettore. RJ45 I dispositivi Snowball Edge dispongono di due RJ45 porte. Scegli una porta da usare.

Il funzionamento 1G è indicato da una spia ambra lampeggiante. Il funzionamento 1G non è consigliato per i trasferimenti di dati su larga scala verso il dispositivo Snowball Edge, poiché aumenta notevolmente il tempo necessario per il trasferimento dei dati.

Il funzionamento 10G è indicato da una spia verde lampeggiante. Richiede un cavo Cat6A UTP con una distanza di funzionamento massima di 55 metri (180 piedi).



Prerequisiti per l'utilizzo di Snowball Edge

Prima di iniziare a usare Snowball Edge, devi creare un AWS account se non ne possiedi uno. Ti consigliamo inoltre di imparare a configurare i dati e le istanze di calcolo da utilizzare con Snowball Edge.

AWS Snowball Edge è un servizio specifico della regione. Quindi, prima di pianificare il tuo lavoro, assicurati che il servizio sia disponibile presso il tuo. Regione AWS Assicurati che la tua posizione e il bucket Amazon S3 si trovino nello stesso Regione AWS o nello stesso Paese, perché ciò influirà sulla tua possibilità di ordinare il dispositivo.

Per utilizzare lo storage compatibile con Amazon S3 su Snowball Edge con dispositivi ottimizzati per l'elaborazione per processi di edge computing e storage locali, devi fornire la capacità S3 sul dispositivo o sui dispositivi al momento dell'ordine. Lo storage compatibile con Amazon S3 su Snowball Edge supporta la gestione locale dei bucket, quindi puoi creare bucket S3 sul dispositivo o sul cluster dopo aver ricevuto il dispositivo o i dispositivi.

Come parte del processo di ordinazione, crei un ruolo AWS Identity and Access Management (IAM) e una chiave (). AWS Key Management Service AWS KMS La chiave KMS viene utilizzata per crittografare il codice di sblocco per il tuo lavoro. Per ulteriori informazioni sulla creazione di ruoli IAM e chiavi KMS, consulta [Creazione di un lavoro per ordinare un dispositivo Snowball Edge](#).

Note

In Asia Pacifico (Mumbai) il Regione AWS servizio è fornito da Amazon su Internet Services Private Limited (AISPL). Per informazioni sulla registrazione ad Amazon Web Services nell'Asia Pacifico (Mumbai) Regione AWS, consulta [Registrazione ad AISPL](#).

Argomenti

- [Registrati per un Account AWS](#)
- [Crea un utente con accesso amministrativo](#)
- [Informazioni sul tuo ambiente](#)
- [Lavorare con nomi di file che contengono caratteri speciali](#)
- [Crittografia Amazon S3 con AWS KMS](#)
- [Crittografia Amazon S3 con crittografia lato server](#)
- [Prerequisiti per l'utilizzo dell'adattatore Amazon S3 su Snowball Edge per processi di importazione ed esportazione](#)
- [Prerequisiti per l'utilizzo dello storage compatibile con Amazon S3 su Snowball Edge](#)
- [Prerequisiti per l'utilizzo delle istanze di calcolo su Snowball Edge](#)

Registrati 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.

Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene 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 [attività che richiedono l'accesso di un utente root](#).

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a <https://aws.amazon.com/> e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi [Console di gestione AWS](#) come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Signing in as the root user](#) della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta [Abilitare un dispositivo MFA virtuale per l'utente Account AWS root \(console\)](#) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

Per istruzioni, consulta [Abilitazione di AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta [Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory](#) nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta [AWS Accedere al portale di accesso](#) nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

Segui le istruzioni riportate nella pagina [Creazione di un set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

Per istruzioni, consulta [Aggiungere gruppi](#) nella Guida per l'utente di AWS IAM Identity Center .

Informazioni sul tuo ambiente

Comprendere il set di dati e la configurazione dell'ambiente locale ti aiuterà a completare il trasferimento dei dati. Considerate quanto segue prima di effettuare l'ordine.

Quali dati state trasferendo?

Il trasferimento di un gran numero di file di piccole dimensioni non funziona bene con. AWS Snowball Edge. Questo perché Snowball Edge crittografa ogni singolo oggetto. I file di piccole dimensioni includono file di dimensioni inferiori a 1 MB. Ti consigliamo di comprimerli prima di trasferirli sul AWS Snowball Edge dispositivo. Ti consigliamo inoltre di non avere più di 500.000 file o directory all'interno di ciascuna directory.

Si accederà ai dati durante il trasferimento?

È importante disporre di un set di dati statico (ovvero, nessun utente o sistema accede ai dati durante il trasferimento). In caso contrario, il trasferimento del file può fallire a causa di una mancata corrispondenza del checksum. I file non verranno trasferiti e verranno contrassegnati come. `Failed`

Per evitare di danneggiare i dati, non scollegare un AWS Snowball Edge dispositivo o modificarne le impostazioni di rete durante il trasferimento dei dati. Durante la scrittura nel dispositivo lo stato dei file deve essere statico. I file modificati durante la scrittura sul dispositivo possono causare conflitti di lettura/scrittura.

La rete supporterà il trasferimento AWS Snowball Edge dei dati?

Snowball Edge supporta gli RJ45 adattatori di rete SFP+ o QSFP+. Verifica che lo switch sia uno switch gigabit. A seconda della marca dello switch, potrebbe indicare gigabit o 10/100/1000. I dispositivi Snowball Edge non supportano uno switch da megabit o uno switch 10/100.

Lavorare con nomi di file che contengono caratteri speciali

È importante notare che se i nomi degli oggetti contengono caratteri speciali, è possibile che si verifichino degli errori. Sebbene Amazon S3 consenta caratteri speciali, ti consigliamo vivamente di evitare i seguenti caratteri:

- Barra rovesciata ("`\`")
- Parentesi graffa di apertura ("`{`")
- Parentesi graffa di chiusura ("`}`")
- Parentesi quadra di apertura ("`[`")
- Parentesi quadra di chiusura ("`]`")
- Simbolo "minore di" ("`<`")

- Simbolo 'maggiore di' (">")
- Caratteri ASCII non stampabili (caratteri decimali da 128 a 255)
- Accento circonflesso ("^")
- Carattere di percentuale ("%")
- Accento grave/apice inverso ("`")
- Virgolette
- Tilde ("~")
- Carattere "cancellato" ("#")
- Barra verticale ("|")

Se i tuoi file contengono uno o più di questi caratteri nei nomi degli oggetti, rinomina gli oggetti prima di copiarli sul AWS Snowball Edge dispositivo. Gli utenti Windows con spazi nei nomi dei file devono prestare attenzione quando copiano singoli oggetti o eseguono un comando ricorsivo. Nei comandi, racchiudi i nomi degli oggetti che includono spazi nei nomi tra virgolette. Di seguito sono riportati alcuni esempi di tali file.

Sistema operativo	Nome del file: test file.txt
Windows	"C:\Users\<username>\desktop\test file.txt"
iOS	/Users/<username>/test\ file.txt
Linux	/home/<username>/test\ file.txt

Note

Gli unici metadati dell'oggetto che vengono trasferiti sono il nome e la dimensione dell'oggetto.

Crittografia Amazon S3 con AWS KMS

Puoi utilizzare le chiavi di crittografia predefinite AWS gestite o gestite dal cliente per proteggere i dati durante l'importazione o l'esportazione dei dati.

Utilizzo della crittografia dei bucket predefinita di Amazon S3 con chiavi gestite AWS KMS

Per abilitare la crittografia AWS gestita con AWS KMS

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegli il bucket Amazon S3 che desideri crittografare.
3. Nella procedura guidata che appare sul lato destro, scegli Proprietà.
4. Nella casella Crittografia predefinita, scegli Disabilitata (questa opzione è disattivata) per abilitare la crittografia predefinita.
5. Scegli AWS-KMS come metodo di crittografia, quindi scegli la chiave KMS che desideri utilizzare. Questa chiave viene utilizzata per crittografare gli oggetti che vengono INSERITI nel bucket.
6. Scegli Save (Salva).

Dopo la creazione del job Snowball Edge e prima dell'importazione dei dati, aggiungi un'istruzione alla policy di ruolo IAM esistente. Questo è il ruolo che hai creato durante il processo di ordinazione. A seconda del tipo di lavoro, il nome del ruolo predefinito è simile a `Snowball-import-s3-only-role` o `Snowball-export-s3-only-role`.

Di seguito sono riportati alcuni esempi di tale affermazione.

Per importare dati

Se utilizzi la crittografia lato server con chiavi AWS KMS gestite (SSE-KMS) per crittografare i bucket Amazon S3 associati al tuo processo di importazione, devi anche aggiungere la seguente dichiarazione al tuo ruolo IAM.

Example Esempio di ruolo IAM di importazione Snowball

```
{
  "Effect": "Allow",
  "Action": [
    "kms: GenerateDataKey",
    "kms: Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```


Per esportare dati

Se utilizzi la crittografia lato server con chiavi AWS KMS gestite per crittografare i bucket Amazon S3 associati al tuo processo di esportazione, devi anche aggiungere la seguente dichiarazione al tuo ruolo IAM.

Example Ruolo IAM per l'esportazione di Snowball

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Utilizzo della crittografia dei bucket predefinita di S3 con chiavi cliente AWS KMS

Puoi utilizzare la crittografia dei bucket Amazon S3 predefinita con le tue chiavi KMS per proteggere i dati che stai importando ed esportando.

Per importare dati

Per abilitare la crittografia gestita dal cliente con AWS KMS

1. Accedi Console di gestione AWS e apri la console AWS Key Management Service (AWS KMS) su <https://console.aws.amazon.com/kms>.
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione a sinistra, scegli Customer managed keys, quindi scegli la chiave KMS associata ai bucket che desideri utilizzare.
4. Espandi Key Policy se non è già stato espanso.
5. Nella sezione Utenti chiave, scegli Aggiungi e cerca il ruolo IAM. Scegli il ruolo IAM, quindi scegli Aggiungi.
6. In alternativa, puoi scegliere Passa alla visualizzazione Policy per visualizzare il documento di policy chiave e aggiungere una dichiarazione alla policy chiave. Di seguito è riportato un esempio della politica.

Example di una politica per la chiave gestita dal AWS KMS cliente

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/snowball-import-s3-only-role"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

Dopo aver aggiunto questa policy alla chiave gestita AWS KMS dal cliente, è necessario aggiornare anche il ruolo IAM associato al job Snowball. Per impostazione predefinita, il ruolo è `snowball-import-s3-only-role`.

Example del ruolo IAM di importazione di Snowball

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Per ulteriori informazioni, consulta [Utilizzo di politiche basate sull'identità \(politiche IAM\) per AWS Snowball Edge](#).

La chiave KMS utilizzata ha il seguente aspetto:

`"Resource": "arn:aws:kms:region:AccountID:key/*"`

Per esportare dati

Example di una politica per la chiave gestita AWS KMS dal cliente

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/snowball-import-s3-only-role"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

Dopo aver aggiunto questa policy alla chiave gestita AWS KMS dal cliente, è necessario aggiornare anche il ruolo IAM associato al job Snowball. Per impostazione predefinita, il ruolo è simile al seguente:

snowball-export-s3-only-role

Example del ruolo IAM di Snowball export

```
{
  "Effect": "Allow",
  "Action": [
    "kms: GenerateDataKey",
    "kms: Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Dopo aver aggiunto questa policy alla chiave gestita AWS KMS dal cliente, è necessario aggiornare anche il ruolo IAM associato al job Snowball. Per impostazione predefinita, il ruolo è snowball-export-s3-only-role.

Crittografia Amazon S3 con crittografia lato server

AWS Snowball Edge supporta la crittografia lato server con chiavi di crittografia gestite di Amazon S3 (SSE-S3). La crittografia lato server serve a proteggere i dati inattivi e SSE-S3 dispone di una crittografia avanzata a più fattori per proteggere i dati archiviati in Amazon S3. Per ulteriori informazioni su SSE-S3, consulta [Protezione dei dati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 \(SSE-S3\) nella Guida per l'utente di Amazon Simple Storage Service](#).

Note

Attualmente, AWS Snowball Edge non supporta la crittografia lato server con chiavi fornite dal cliente (SSE-C). Tuttavia, è possibile usare questo tipo di SSE per proteggere i dati importati o potrebbe essere già utilizzato sui dati che si desidera esportare. In questi casi tieni a mente le seguenti considerazioni:

- Importazione: se desideri utilizzare SSE-C per crittografare gli oggetti che hai importato in S3, copia tali oggetti in un altro bucket con crittografia SSE-KMS o SSE-S3 stabilita come parte della policy del bucket.
- Esporta: se desideri esportare oggetti crittografati con SSE-C, copia prima tali oggetti in un altro bucket che non dispone di crittografia lato server o che ha SSE-KMS o SSE-S3 specificato nella policy del bucket di quel bucket.

Prerequisiti per l'utilizzo dell'adattatore Amazon S3 su Snowball Edge per processi di importazione ed esportazione

Puoi utilizzare l'adattatore S3 su Snowball Edge quando utilizzi i dispositivi per spostare dati da fonti di dati locali al cloud o dal cloud all'archiviazione dati locale. Per ulteriori informazioni, consulta [Trasferimento di file tramite l'adattatore Amazon S3 per la migrazione dei dati da o verso Snowball Edge](#).

Il bucket Amazon S3 associato al job deve utilizzare la classe di storage standard Amazon S3. Prima di creare il primo processo, tieni presente quanto segue.

Per i lavori che importano dati in Amazon S3, segui questi passaggi:

- Verifica che i file e le cartelle da trasferire siano denominati in base alle [linee guida per la denominazione delle chiavi degli oggetti](#) per Amazon S3. Tutti i file o le cartelle con nomi che non soddisfano queste linee guida non vengono importati in Amazon S3.
- Pianifica i dati che desideri importare in Amazon S3. Per ulteriori informazioni, consulta [Pianificazione di trasferimenti di grandi dimensioni con Snowball Edge](#).

Prima di esportare dati da Amazon S3, segui questi passaggi:

- Individua quali dati verranno esportati al momento della creazione di un processo. Per ulteriori informazioni, consulta [Utilizzo delle chiavi oggetto Amazon S3 per l'esportazione di dati su un dispositivo Snowball Edge](#).
- Per tutti i file con i due punti (:) nel nome del file, modifica i nomi dei file in Amazon S3 prima di creare il processo di esportazione per ottenere questi file. I file con due punti nel nome non vengono esportati in Microsoft Windows Server.

Prerequisiti per l'utilizzo dello storage compatibile con Amazon S3 su Snowball Edge

Utilizzi lo storage compatibile con Amazon S3 su Snowball Edge quando memorizzi dati sul dispositivo presso la tua edge location e utilizzi i dati per operazioni di elaborazione locali. I dati utilizzati per le operazioni di elaborazione locali non verranno importati in Amazon S3 quando il dispositivo viene restituito.

Quando ordini un dispositivo Snow per l'elaborazione e lo storage locali con storage compatibile con Amazon S3, tieni presente quanto segue.

- Fornirai la capacità di storage di Amazon S3 al momento dell'ordine del dispositivo. Considerate quindi le vostre esigenze di archiviazione prima di ordinare un dispositivo.
- Puoi creare bucket Amazon S3 sul dispositivo dopo averlo ricevuto anziché ordinando un dispositivo Snowball Edge.
- Per utilizzare lo storage compatibile con Amazon S3 su Snowball Edge, devi scaricare la versione più recente AWS CLI (v2.11.15 o AWS OpsHub successiva) del client Snowball Edge o installarla sul tuo computer.
- Dopo aver ricevuto il dispositivo, configura, avvia e utilizza lo storage compatibile con Amazon S3 su Snowball Edge in base a [Uso dello storage compatibile con Amazon S3 su Snowball Edge](#) in questa guida.

Prerequisiti per l'utilizzo delle istanze di calcolo su Snowball Edge

Puoi eseguire istanze di calcolo EC2 compatibili con Amazon ospitate su un sistema AWS Snowball Edge con i seguenti tipi sbe1 di istanze sbe-g: sbe-c

- Il tipo di sbe1 istanza funziona su dispositivi con l'opzione Snowball Edge Storage Optimized.
- Il tipo di sbe-c istanza funziona su dispositivi con l'opzione Snowball Edge Compute Optimized.

Tutti i tipi di istanze di calcolo supportati dalle opzioni dei dispositivi Snowball Edge sono specifici AWS Snowball Edge per i dispositivi. Come le loro controparti basate sul cloud, queste istanze richiedono Amazon Machine Images AMIs () per l'avvio. Scegli l'AMI come istanza prima di creare il job Snowball Edge.

Per utilizzare un'istanza di calcolo su Snowball Edge, crea un lavoro per ordinare un dispositivo Snowball Edge e specifica il tuo. AMIs È possibile eseguire questa operazione utilizzando la console di AWS Snowball Edge gestione, il AWS Command Line Interface (AWS CLI) o uno dei. AWS SDKs In genere, per utilizzare le istanze, è necessario eseguire alcuni prerequisiti di pulizia prima di creare il lavoro.

Per i lavori che utilizzano istanze di calcolo, prima di poterne aggiungere una qualsiasi AMIs al lavoro, è necessario disporre di un AMI Account AWS e deve essere un tipo di immagine supportato. Attualmente, AMIs sono supportati i seguenti sistemi operativi:

- [Amazon Linux 2](#)
- [CentOS 7 \(x86_64\) - con aggiornamenti HVM](#)
- Ubuntu 16.04 LTS - Xenial (HVM)
- [Ubuntu 20.04 LTS - Focal](#)
- [Ubuntu 22.04 LTS - Jammy](#)
- [Microsoft Windows Server 2012 R2](#)
- [Microsoft Windows Server 2016](#)
- [Microsoft Windows Server 2019](#)

 Note

Ubuntu 16.04 LTS - Le immagini Xenial (HVM) non sono più supportate in Marketplace AWS, ma sono ancora supportate per l'uso su dispositivi Snowball Edge tramite Amazon VM e in esecuzione localmente in. EC2 Import/Export AMIs

Puoi ottenere queste immagini da. [Marketplace AWS](#)

Se usi SSH per connetterti alle istanze in esecuzione su Snowball Edge, puoi usare la tua coppia di chiavi o crearne una su Snowball Edge. Per AWS OpsHub utilizzarla per creare una key pair sul dispositivo, vedere [Utilizzo di coppie di chiavi per EC2 istanze compatibili in AWS OpsHub](#). Per utilizzare la AWS CLI funzione per creare una key pair sul dispositivo, vedere create-key-pair in [Elenco dei AWS CLI comandi EC2 compatibili supportati su Snowball Edge](#). Per ulteriori informazioni sulle coppie di chiavi e Amazon Linux 2, consulta le [coppie di EC2 chiavi Amazon e le istanze Linux](#) nella Amazon EC2 User Guide.

Per informazioni specifiche per l'utilizzo di istanze di calcolo su un dispositivo, consulta [Utilizzo di istanze EC2 di calcolo compatibili con Amazon su Snowball Edge](#).

Come AWS Snowball Edge funziona

AWS Snowball Edge i dispositivi sono di AWS proprietà di e risiedono presso la tua sede locale mentre sono in uso.

Esistono tre tipi di lavoro che è possibile utilizzare con un AWS Snowball Edge dispositivo. Anche se i tipi di progetto differiscono per i casi d'uso, ogni tipo di progetto ha lo stesso flusso di lavoro per il modo in cui è possibile ordinare, ricevere e restituire i dispositivi. Indipendentemente dal tipo di lavoro, ogni lavoro segue una cancellazione dei dati dello standard 800-88 del National Institute of Standards and Technology (NIST) dopo il completamento del lavoro.

Flusso di lavoro condiviso

1. Crea il lavoro: ogni lavoro viene creato in Console di gestione della famiglia di servizi AWS Snow o in modo programmatico tramite l'API di gestione dei lavori. Lo stato di un lavoro può essere monitorato nella console o tramite l'API.
2. Un dispositivo è pronto per il tuo lavoro: prepariamo un AWS Snowball Edge dispositivo per il tuo lavoro e lo stato del tuo lavoro è ora Preparing Snowball. Questo processo di preparazione può richiedere fino a 4 settimane dalla creazione del lavoro per ordinare il dispositivo. Questa tempistica dovrebbe essere presa in considerazione nel piano di progetto per garantire una transizione senza interruzioni.
3. Un dispositivo ti viene spedito dal corriere della tua regione: il corriere subentra da qui e lo stato del tuo incarico è ora in transito verso di te. Puoi trovare il tuo numero di tracciamento e un link al sito web di tracciamento sulla console o con la gestione di progetto API. Per informazioni su chi è il corriere della tua regione, consulta [Considerazioni sulla spedizione per Snowball Edge](#).
4. Ricevi il dispositivo: alcuni giorni dopo, l'operatore della tua regione consegna il AWS Snowball Edge dispositivo all'indirizzo che hai fornito quando hai creato l'offerta e lo stato del lavoro cambia in Consegnato a te. Quando lo ricevi, noterai che non è contenuto in una scatola perché il dispositivo è di per sé un contenitore di spedizione.
5. Ottieni le tue credenziali e scarica il client Snowball Edge: preparati a iniziare a trasferire i dati ottenendo le credenziali, il job manifest e il codice di sblocco del manifest, quindi scaricando il client Snowball Edge.
 - Il client Snowball Edge è lo strumento che utilizzi per gestire il flusso di dati dal dispositivo alla destinazione dei dati locale.

Puoi scaricare e installare il client Snowball Edge dalla pagina delle [AWS Snowball Edge risorse](#).

Devi scaricare il client Snowball Edge dalla pagina [AWS Snowball Edge Risorse](#) e installarlo su una potente workstation di tua proprietà.

- Il manifest viene utilizzato per autenticare l'accesso al dispositivo ed è crittografato in modo da poter essere decrittografato solo con il codice di sblocco. Puoi ottenere il manifest dalla console o utilizzando l'API di gestione del processo quando il dispositivo si trova presso la tua sede.
 - Il codice di sblocco è un codice a 29 caratteri utilizzato per decrittografare il manifest. È possibile ottenere il codice di sblocco dalla console o con il processo di gestione API. Ti consigliamo di annotarlo e conservarlo in un posizione separata rispetto al manifest per evitare un accesso non autorizzato al dispositivo mentre si trova presso la tua struttura.
6. Posiziona l'hardware: sposta il dispositivo nel data center e aprilo seguendo le istruzioni sulla custodia. Collega il dispositivo all'alimentazione e alla rete locale.
 7. Accensione del dispositivo: quindi, accendi il dispositivo premendo il pulsante di accensione sopra il display LCD. Attendi qualche minuto finché non appare la schermata Ready (Pronto).
 8. Ottieni l'indirizzo IP del dispositivo: sul display LCD è presente la scheda CONNESSIONE. Tocca questa scheda e ottieni l'indirizzo IP del AWS Snowball Edge dispositivo.
 9. Usa il client Snowball Edge per sbloccare il dispositivo: quando utilizzi il client Snowball Edge per sbloccare il AWS Snowball Edge dispositivo, inserisci l'indirizzo IP del dispositivo, il percorso del file manifest e il codice di sblocco. Il client Snowball Edge decifra il manifesto e lo utilizza per autenticare l'accesso dell'utente al dispositivo.
 10. Usa il dispositivo: il dispositivo è attivo e funzionante. Puoi usarlo per trasferire dati con l'adattatore Amazon S3 o il punto di montaggio Network File System (NFS) o per l'elaborazione e lo storage locali con lo storage compatibile con Amazon S3 su Snowball Edge.
 11. Prepara il dispositivo per il viaggio di ritorno: dopo aver utilizzato il dispositivo nella tua postazione locale, premi il pulsante di accensione sopra il display LCD. Lo spegnimento del dispositivo richiede circa 20 secondi. Scollega il dispositivo e i cavi di alimentazione nel relativo scomparto nella parte superiore del dispositivo e chiudi tutti e tre gli sportelli del dispositivo. Il dispositivo è ora pronto per essere restituito.
 12. L'operatore della tua regione restituisce il dispositivo a AWS: quando l'operatore ha il AWS Snowball Edge dispositivo, lo stato del lavoro diventa In transito verso AWS.

 Note

Esistono passaggi aggiuntivi per i lavori di esportazione e cluster. Per ulteriori informazioni, consultare [Come funzionano i lavori di esportazione di Snowball Edge](#) e [Come funzionano i job di elaborazione e storage locali in cluster Snowball Edge](#).

Argomenti

- [Come funzionano i processi di importazione di Snowball Edge](#)
- [Come funzionano i lavori di esportazione di Snowball Edge](#)
- [Come funzionano i job di elaborazione e storage locali di Snowball Edge](#)
- [Video e blog su Snowball Edge](#)

Come funzionano i processi di importazione di Snowball Edge

Ogni processo di importazione utilizza un singolo dispositivo Snowball. Dopo aver creato un lavoro per ordinare un dispositivo Snowball Edge nella Console di gestione della famiglia di servizi AWS Snow o nell'API di gestione dei lavori, ti spediamo uno Snowball. Quando arriva tra qualche giorno, connetti il dispositivo Snowball Edge alla rete e trasferisci sul dispositivo i dati che desideri importare in Amazon S3. Al termine del trasferimento dei dati, rispediti lo Snowball AWS a e noi importeremo i tuoi dati in Amazon S3.

 Important

Il processo di importazione non può scrivere su bucket in Amazon S3 dal dispositivo Snow se hai attivato S3 Object Lock e abilitato le impostazioni di conservazione predefinite. Dopo aver abilitato Amazon S3 Object Lock, non puoi disabilitarlo o sospendere il controllo delle versioni del bucket per il bucket. Se i tuoi bucket hanno S3 Object Lock con le impostazioni di conservazione predefinite abilitate, prima di restituire Snowball Edge, disabilita l'impostazione di conservazione di S3 Object Lock. Dopo aver importato i dati dal dispositivo entro AWS, abilita nuovamente l'impostazione di conservazione sul bucket. Per ulteriori informazioni, consulta [Impostare o modificare un periodo di conservazione su un oggetto S3](#).

Inoltre, il processo di importazione non può scrivere nel bucket in Amazon S3 se le politiche IAM sul bucket impediscono la scrittura nel bucket. Per ulteriori informazioni, consulta [Identity and Access Management for Amazon S3](#).

Come funzionano i lavori di esportazione di Snowball Edge

Ogni processo di esportazione può utilizzare un numero qualsiasi di AWS Snowball Edge dispositivi. Se l'inserzione contiene più dati di quanti ne possa contenere un singolo dispositivo, ti verranno forniti più dispositivi. Ogni parte del processo include un dispositivo associato. Dopo aver creato le parti del lavoro, la prima parte del lavoro passa allo stato Preparing Snowball.

Note

L'operazione di quotazione utilizzata per suddividere il lavoro in parti è una funzione di Amazon S3 e ti viene fatturata allo stesso modo di qualsiasi operazione di Amazon S3.

Subito dopo, iniziamo a esportare i dati su un dispositivo. Il tempo necessario per esportare i dati varia in base alla natura del set di dati. Ad esempio, l'esportazione di molti file di piccole dimensioni (meno di 10 MB) richiede molto più tempo. Al termine dell'esportazione, AWS prepara il dispositivo per il ritiro da parte dell'operatore della tua regione. Quando arriva, connetti il AWS Snowball Edge dispositivo alla rete e trasferisci i dati dal dispositivo allo spazio di archiviazione sulla rete.

Al termine del trasferimento dei dati, rispedisci il dispositivo a AWS. Quando riceviamo il dispositivo destinato all'esportazione, lo cancelliamo completamente. Questa cancellazione rispetta gli standard 800-88 della National Institute of Standards and Technology (NIST). Questa fase contrassegna il completamento della particolare parte del processo.

- Per inserire i dati

Prima di esportare gli oggetti nel bucket S3, eseguiamo la scansione del bucket. Se il bucket viene modificato dopo la scansione, il processo potrebbe subire ritardi perché eseguiamo la scansione alla ricerca di oggetti mancanti o alterati.

- Per S3 Glacier Flexible Retrieval

È importante notare che AWS Snowball Edge non è possibile esportare oggetti che si trovano nella classe di archiviazione S3 Glacier. Questi oggetti devono essere ripristinati prima di AWS Snowball Edge poter esportare correttamente gli oggetti nel bucket.

Come funzionano i job di elaborazione e storage locali di Snowball Edge

Puoi utilizzare la funzionalità di calcolo e archiviazione locale di un AWS Snowball Edge dispositivo eseguendo istanze di calcolo AWS EC2 compatibili o contenitori Kubernetes in Amazon EKS Anywhere on Snow. Per quanto riguarda la funzionalità di elaborazione, lo storage dei dati viene fornito da uno storage compatibile con Amazon S3 su Snowball Edge.

Puoi creare bucket Amazon S3 sui dispositivi Snowball Edge per archiviare e recuperare oggetti in locale per applicazioni che richiedono l'accesso locale ai dati, l'elaborazione locale dei dati e la residenza dei dati. Lo storage compatibile con Amazon S3 su Snowball Edge offre una nuova classe di storage che utilizza Amazon S3 ed è progettata per archiviare i dati in modo duraturo e ridondante su più dispositivi APIs Snowball Edge. SNOW Sui bucket Snowball Edge puoi utilizzare le stesse APIs funzionalità che usi su Amazon S3, tra cui le policy del ciclo di vita dei bucket, la crittografia e l'etichettatura. Quando il dispositivo o i dispositivi vengono restituiti AWS, tutti i dati creati o archiviati nello storage compatibile con Amazon S3 su Snowball Edge vengono cancellati. Per ulteriori informazioni, consulta [Local Compute and Storage Only Jobs](#).

Per ulteriori informazioni, consulta [Informazioni sull'utilizzo dei dispositivi Snowball Edge per fornire funzionalità di elaborazione e archiviazione locali](#).

Come funzionano i job di elaborazione e storage locali in cluster Snowball Edge

Un cluster job è un tipo speciale di lavoro destinato esclusivamente all'archiviazione e all'elaborazione locali. È per quei carichi di lavoro che richiedono una maggiore durabilità dei dati e capacità di archiviazione. Per ulteriori informazioni, consulta [Informazioni sui lavori che forniscono archiviazione locale su un cluster di dispositivi Snowball Edge](#).

Note

Analogamente ai processi di elaborazione e archiviazione locali autonomi, i dati archiviati in un cluster non possono essere importati in Amazon S3 senza ordinare dispositivi aggiuntivi

come parte di processi di importazione separati. Ordinandoli, puoi trasferire i dati dal cluster ai dispositivi e importarli quando restituisci i dispositivi per i processi di importazione.

I cluster hanno da 3 a 16 AWS Snowball Edge dispositivi, chiamati nodi. Quando ricevi i nodi dal tuo operatore regionale, connetti tutti i nodi all'alimentazione e alla rete per ottenere i relativi indirizzi IP. Questi indirizzi IP vengono utilizzati per sbloccare tutti i nodi del cluster contemporaneamente con un unico comando di sblocco, utilizzando l'indirizzo IP di uno dei nodi. Per ulteriori informazioni, consulta [Configurazione e utilizzo del client Snowball Edge](#).

Puoi scrivere dati su un cluster sbloccato utilizzando o utilizzando lo storage compatibile con Amazon S3 su Snowball Edge e i dati distribuiti tra gli altri nodi.

Quando hai finito con il cluster, rispedisci tutti i nodi a AWS. Quando riceviamo il nodo del cluster, eseguiamo una cancellazione completa dello Snowball. Questa cancellazione rispetta gli standard 800-88 della National Institute of Standards and Technology (NIST).

Video e blog su Snowball Edge

- [Migrazione di file di dimensioni diverse con dispositivi snow-transfer-tool AWS Snowball Edge](#)
- [AWS Snowball Edge Migrazione dei dati](#)
- [AWS OpsHub for Snow Family](#)
- [Novetta offre IoT e machine learning all'edge per la risposta ai disastri](#)
- [Abilita migrazioni di database su larga scala con DMS e AWS Snowball Edge](#)
- [Best practice per la migrazione dei dati con AWS Snowball Edge](#)
- [AWS Snowball Edge resources](#)
- [Storage compatibile con Amazon S3 su dispositivi ottimizzati per l' AWS Snowball Edge elaborazione ora disponibile a livello generale](#)
- [Guida introduttiva allo storage compatibile con Amazon S3 su Snowball Edge su dispositivi Snowball Edge AWS](#)

Prezzi a lungo termine per i dispositivi Snowball Edge

Quando ordini un dispositivo Snowball Edge, puoi scegliere l'opzione di prezzo più adatta al tuo caso d'uso. I prezzi sono disponibili in due modi: su richiesta per ogni giorno di utilizzo del dispositivo o in modalità prepagata, prezzi a lungo termine mensili, di uno o tre anni in base al tipo di dispositivo. Puoi scegliere di rinnovare automaticamente l'opzione di prezzo a lungo termine per un periodo di uno o tre anni in modo che un nuovo periodo prepagato inizi allo scadere del periodo precedente per evitare l'interruzione dell'utilizzo del dispositivo. L'opzione di prezzo mensile a lungo termine si rinnoverà automaticamente finché il dispositivo sarà in tuo possesso. Per ulteriori informazioni sull'ordinazione di un dispositivo, consulta [Creare un lavoro per ordinare un dispositivo Snowball Edge](#) in questa guida.

Oltre alla convenienza economica, i prezzi a lungo termine consentono di sostituire i dispositivi Snowball Edge durante il periodo di prezzo, quando cambiano i requisiti operativi. Ad esempio, puoi richiedere di sostituire i dispositivi in modo che il nuovo dispositivo includa una nuova AMI o nuovi dati da Amazon S3 o di sostituire un dispositivo guasto. Consultare [Sostituzione dei dispositivi Snowball Edge durante il periodo di prezzo a lungo termine](#).

Note

Se richiedi la sostituzione o la sostituzione di un dispositivo Snowball Edge nell'ambito del piano tariffario Commit di 1 o 3 anni per qualsiasi motivo diverso da un problema hardware o software attribuito AWS al servizio Snow, ti verrà addebitata una tariffa per l'utilizzo del dispositivo. Questa tariffa per l'utilizzo del dispositivo è determinata come tariffa mensile (per Snowball Edge Compute Optimized) o tariffa per lavori su richiesta per la configurazione.

Per ulteriori informazioni sui prezzi a lungo termine, consulta [Ottimizzazione dei costi con opzioni di prezzo a lungo termine](#) per AWS Snowball Edge. Per AWS Snowball Edge i prezzi dei tuoi prodotti Regione AWS, consulta la sezione [AWS Snowball Edge Prezzi](#).

Sostituzione dei dispositivi Snowball Edge durante il periodo di prezzo a lungo termine

La sostituzione dei dispositivi Snowball Edge durante il periodo di prezzo a lungo termine prevede l'ordinazione di un nuovo dispositivo e la restituzione immediata del dispositivo attuale.

1. Crea un nuovo lavoro per il dispositivo Snowball Edge sostitutivo. Il dispositivo sostitutivo deve essere destinato allo stesso tipo di lavoro e avere le stesse opzioni di elaborazione e archiviazione del dispositivo in uso. Vedi [Creare un lavoro per ordinare un dispositivo Snowball Edge](#) in questa guida.
2. Restituisci immediatamente il dispositivo che possiedi. Vedi [Spegnimento dello Snowball Edge](#) e [Restituzione del dispositivo Snowball Edge](#). AWS gestirà la logistica di sostituzione del dispositivo e per questa sostituzione verrà applicata una commissione per il riciclaggio del dispositivo.

Considerazioni sulla spedizione per Snowball Edge

Quando crei un lavoro per ordinare un dispositivo Snowball Edge, fornisci un indirizzo di spedizione e scegli la velocità di spedizione. Tieni presente che la velocità di spedizione non indica quanto tempo puoi aspettarti di ricevere il dispositivo dal giorno in cui hai creato il lavoro. Piuttosto, indica l'ora in cui il dispositivo è in transito tra AWS e il tuo indirizzo di spedizione.

Potrebbero essere necessarie fino a 4 settimane per fornire e preparare il dispositivo per il lavoro prima che venga spedito. Questa tempistica dovrebbe essere presa in considerazione nel piano di progetto per garantire una transizione senza interruzioni. Durante AWS la preparazione del dispositivo per la spedizione, puoi monitorare lo stato del tuo lavoro tramite Console di gestione della famiglia di servizi AWS Snow. Per ulteriori informazioni, consulta [Stati delle offerte di lavoro Snowball Edge](#).

Note

La velocità di spedizione scelta si applica quando ti viene AWS inviato il dispositivo e quando lo restituisci a AWS.

I dispositivi Snowball Edge possono essere utilizzati solo per importare o esportare dati all'interno della AWS regione in cui sono ordinati i dispositivi.

Per ulteriori informazioni sulla scelta della velocità di spedizione e sull'immissione dell'indirizzo di spedizione durante la creazione di un lavoro per ordinare un dispositivo Snowball Edge, consulta [Scelta delle preferenze di sicurezza, spedizione e notifica](#). Per ulteriori informazioni sulla restituzione di un dispositivo Snowball Edge a AWS, consulta [Restituzione del dispositivo Snowball Edge](#).

Per informazioni sui costi di spedizione, consulta la sezione [AWS Snowball Edge Prezzi](#).

Restrizioni di spedizione in base alla regione per Snowball Edge

Prima di creare un lavoro per ordinare un dispositivo Snowball Edge, devi accedere alla console dagli stessi dati di Amazon S3. AWS non spedisce Snowball Edge tra paesi all'interno dello stesso, ad esempio dalla Regione AWS Asia Pacifico (India) all'Asia Pacifico (Australia).

Un'eccezione alla spedizione tra paesi è quella tra i paesi membri dell'Unione Europea (UE). Per i trasferimenti di dati AWS nelle regioni europee, spediamo i dispositivi solo nei paesi membri dell'UE elencati:

Austria, Belgio, Bulgaria, Croazia, Repubblica di Cipro, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Italia, Irlanda, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna e Svezia.

Snowball Edge può essere restituito solo nella stessa AWS regione in cui sono stati ordinati i dispositivi.

Sono consentite le spedizioni nazionali all'interno dello stesso paese. Esempi:

- Per i trasferimenti di dati nella regione del Regno Unito, spediamo i dispositivi a livello nazionale all'interno del Regno Unito.
- Per i trasferimenti di dati in Asia Pacifico (Mumbai), spediamo i dispositivi all'interno dell'India.

 Note

AWS non spedisce Snowball Edge alle caselle postali.

Guida introduttiva a Snowball Edge

Con un AWS Snowball Edge dispositivo, puoi accedere alla potenza di archiviazione e di calcolo della rete Cloud AWS locale in modo conveniente in luoghi in cui la connessione a Internet potrebbe non essere un'opzione. Puoi anche trasferire centinaia di terabyte o petabyte di dati tra i tuoi data center locali e Amazon Simple Storage Service (Amazon S3).

Di seguito, puoi trovare le istruzioni generali per creare e completare il tuo primo lavoro su un dispositivo in. AWS Snowball Edge Console di gestione della famiglia di servizi AWS Snow La console presenta i flussi di lavoro più comuni, suddivisi in tipi di processi. Puoi trovare ulteriori informazioni su componenti specifici del AWS Snowball Edge dispositivo in questa documentazione. Per una panoramica dell'intero servizio, consulta [Come AWS Snowball Edge funziona](#).

Potrebbero essere necessarie fino a 4 settimane per il rifornimento e la preparazione di Snowball Edge per il lavoro prima della spedizione. Questa tempistica dovrebbe essere presa in considerazione nel piano di progetto per garantire una transizione senza interruzioni.

Prima di iniziare, devi creare un utente Account AWS e un utente amministratore in AWS Identity and Access Management (IAM). Per informazioni, consultare [Prerequisiti per l'utilizzo di Snowball Edge](#).

Argomenti

- [Creazione di un lavoro per ordinare un dispositivo Snowball Edge](#)
- [Annullamento di un lavoro per ordinare uno Snowball Edge](#)
- [Clonazione di un lavoro per ordinare uno Snowball Edge nel Console di gestione della famiglia di servizi AWS Snow](#)
- [Ricevere lo Snowball Edge](#)
- [Connessione di uno Snowball Edge alla rete locale](#)
- [Ottenere le credenziali per accedere a Snowball Edge](#)
- [Sbloccare Snowball Edge](#)
- [Configurazione degli utenti locali su Snowball Edge](#)
- [Riavvio del dispositivo Snowball Edge](#)
- [Spegnimento dello Snowball Edge](#)
- [Restituzione del dispositivo Snowball Edge](#)
- [Spedizione di ritorno per Snowball Edge](#)

- [Monitoraggio dello stato di importazione da Snowball Edge](#)
- [Ottenimento del report e dei log di completamento del processo di trasferimento dei dati](#)

Creazione di un lavoro per ordinare un dispositivo Snowball Edge

Per ordinare un dispositivo Snowball Edge, devi creare un lavoro per ordinare un dispositivo Snowball Edge nel. Console di gestione della famiglia di servizi AWS Snow Un lavoro è un termine AWS utilizzato per descrivere il ciclo di vita dell'utilizzo di un dispositivo Snowball Edge da parte di un cliente. Un processo inizia con l'ordine di un dispositivo, continua con la AWS preparazione del dispositivo, la spedizione e l'utente lo utilizza e viene completato dopo la AWS ricezione e l'elaborazione del dispositivo dopo la restituzione. I lavori sono classificati per tipo: esportazione, importazione, elaborazione e archiviazione locali. Per ulteriori informazioni, consulta Nozioni di base sui [job di AWS Snowball Edge](#).

Dopo aver creato il lavoro per ordinare un dispositivo, puoi utilizzarlo Console di gestione della famiglia di servizi AWS Snow per visualizzare lo stato del lavoro e monitorare l'avanzamento del dispositivo ordinato durante la AWS preparazione del dispositivo alla spedizione e dopo la restituzione. Per ulteriori informazioni, consulta [Job Statuses](#). Dopo che il dispositivo è stato restituito ed elaborato da AWS, è possibile accedere a un rapporto di completamento dei lavori e accedere tramite. Console di gestione della famiglia di servizi AWS Snow Per ulteriori informazioni, vedi [Ottenere il rapporto e i registri sul completamento del lavoro sulla console](#).

Puoi anche creare e gestire i lavori utilizzando l'API di gestione dei lavori. Per ulteriori informazioni, consulta la [Documentazione di riferimento delle API di AWS Snowball Edge](#).

Argomenti

- [Scelta di un tipo di lavoro](#)
- [Scelta delle opzioni di elaborazione e archiviazione](#)
- [Scelta delle funzionalità e delle opzioni](#)
- [Scelta delle preferenze di sicurezza, spedizione e notifica](#)
- [Rivedi il riepilogo del lavoro e crea il tuo lavoro](#)

Scelta di un tipo di lavoro

Il primo passaggio per creare un lavoro consiste nel determinare il tipo di lavoro di cui hai bisogno e iniziare a pianificarlo utilizzando il Console di gestione della famiglia di servizi AWS Snow.

Per scegliere il tipo di lavoro

1. Accedi a Console di gestione AWS, e apri il [Console di gestione della famiglia di servizi AWS Snow](#). Se è la prima volta che crei un lavoro in questo campo Regione AWS, vedrai la pagina AWS Snowball Edge. Altrimenti verrà visualizzato l'elenco delle offerte di lavoro esistenti.
2. Se è la prima volta che ordini un dispositivo, scegli Ordina un dispositivo AWS Snowball Edge. Se prevedi che più processi richiedano la migrazione di oltre 500 TB di dati, scegli Crea il tuo piano di migrazione di dati di grandi dimensioni superiori a 500 TB. Altrimenti, scegli Create Job nella barra di navigazione a sinistra. Scegli Passaggio successivo per aprire la pagina Pianifica il tuo lavoro.
3. Nella sezione Job name, fornisci un nome per il tuo lavoro nella casella Job name.
4. A seconda delle tue esigenze, scegli uno dei seguenti tipi di lavoro:
 - Importazione in Amazon S3: scegli questa opzione per farti AWS spedire un dispositivo Snowball Edge vuoto. Connetti il dispositivo alla rete locale ed esegui il client Snowball Edge. Copi i dati sul dispositivo utilizzando la condivisione NFS o l'adattatore S3, li rispedisci a AWS e i dati vengono caricati su. AWS
 - Esporta da Amazon S3: scegli questa opzione per esportare i dati dal tuo bucket Amazon S3 al tuo dispositivo. AWS carica i dati sul dispositivo e te li spedisce. Connetti il dispositivo alla rete locale ed esegui il client Snowball Edge. I dati vengono copiati dal dispositivo ai server. Al termine, spedisce il dispositivo a e AWS i tuoi dati vengono cancellati dal dispositivo.
 - Solo elaborazione e archiviazione locali: esegui carichi di lavoro di elaborazione e archiviazione sul dispositivo senza trasferire dati.

Choose a job type

☒ **Import into Amazon S3** [Info](#)

AWS will ship an empty device to you for storage and compute workloads. You'll transfer your data onto it, and ship it back. After AWS gets it, your data will be moved.

☐ **Export from Amazon S3** [Info](#)

Choose what data you want to export from your S3 buckets for storage and compute workloads. AWS will load that data onto a device and ship it to you. When you're done ship the device back for erasing.

☐ **Local compute and storage only** [Info](#)

Perform local compute and storage workloads without transferring data. You can order multiple devices in a cluster for increased durability and storage capacity. Includes rugged and rack-mountable devices.

5. Seleziona Successivo per continuare.

Scelta delle opzioni di elaborazione e archiviazione

Scegli le specifiche hardware per il tuo dispositivo Snowball Edge, quali istanze EC2 compatibili con Amazon includere, come verranno archiviati i dati e i prezzi.

Per scegliere le opzioni di elaborazione e archiviazione del dispositivo

1. Nella sezione Dispositivi Snow, scegli il dispositivo Snowball Edge da ordinare.

Note

Alcuni Snowball Edge potrebbero non essere disponibili a seconda del Regione AWS tipo di ordine e del tipo di lavoro scelto.

2. Nella sezione Scegli la tua opzione di prezzo, dal menu Scegli la tua opzione di prezzo, scegli il tipo di prezzo da candidarti a questa offerta di lavoro. Se scegli l'abbonamento anticipato per 1 anno o per 3 anni, in Rinnovo automatico scegli Attivo per rinnovare automaticamente i prezzi al termine del periodo corrente o Disattivato per non rinnovare automaticamente il prezzo al termine del periodo corrente. Per ulteriori informazioni sulle opzioni di prezzo a lungo termine per i dispositivi Snowball Edge, consulta [Prezzi a lungo termine per i dispositivi Snowball Edge](#)

in questa guida. [Per i prezzi dei tuoi dispositivi Regione AWS, consulta AWS Snowball Edge Prezzi.](#)

3. Nella sezione Seleziona il tipo di archiviazione, fai una scelta in base alle tue esigenze:

- Adattatore S3: utilizza l'adattatore S3 per trasferire dati a livello di codice da e verso Snowball Edge utilizzando le azioni dell'API REST di Amazon S3.
- Storage compatibile con Amazon S3: utilizza lo storage compatibile con Amazon S3 per distribuire uno storage di oggetti durevole e scalabile compatibile con S3 su un singolo dispositivo Snowball Edge o in un cluster multidispositivo.
- Trasferimento dati basato su NFS: utilizza il trasferimento dati basato su Network File System (NFS) per trascinare i file dal computer ai bucket Amazon S3 su Snowball Edge.

 Warning

Il trasferimento dati basato su NFS non supporta l'adattatore S3. Se si procede con il trasferimento di dati basato su NFS, è necessario montare la condivisione NFS per trasferire oggetti. L'utilizzo di AWS CLI per trasferire oggetti avrà esito negativo. Per ulteriori informazioni, consulta [Using NFS for Offline Data Transfer](#) nella AWS Snowball Edge Developer Guide.

 Note

Le opzioni di archiviazione disponibili dipendono dal tipo di lavoro e dal dispositivo Snow che hai scelto.

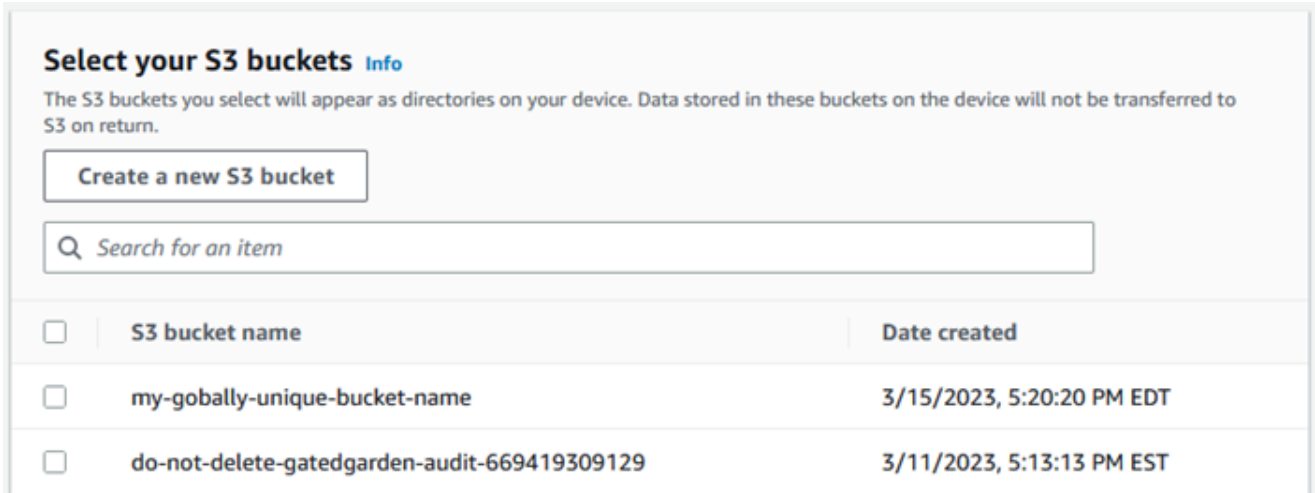
4.

Se hai selezionato S3 Adapter come tipo di archiviazione o se hai selezionato un dispositivo che supporta lo storage a blocchi, procedi come segue per selezionare uno o più bucket S3 da includere nel dispositivo:

- Nella sezione Seleziona i tuoi bucket S3, esegui una o più delle seguenti operazioni per selezionare uno o più bucket S3:
 1. Scegli il bucket S3 che desideri utilizzare nell'elenco dei nomi dei bucket S3.
 2. Nel campo Cerca un elemento, inserisci il nome completo o parziale del bucket per filtrare l'elenco dei bucket disponibili in base alla tua voce, quindi scegli il bucket.

3. Scegli Crea un nuovo bucket S3 per creare un nuovo bucket S3. Il nuovo nome del bucket viene visualizzato nell'elenco dei nomi del bucket. Sceglilo.

Puoi includere uno o più bucket S3. Questi bucket vengono visualizzati sul dispositivo come bucket S3 locali.



Select your S3 buckets [Info](#)

The S3 buckets you select will appear as directories on your device. Data stored in these buckets on the device will not be transferred to S3 on return.

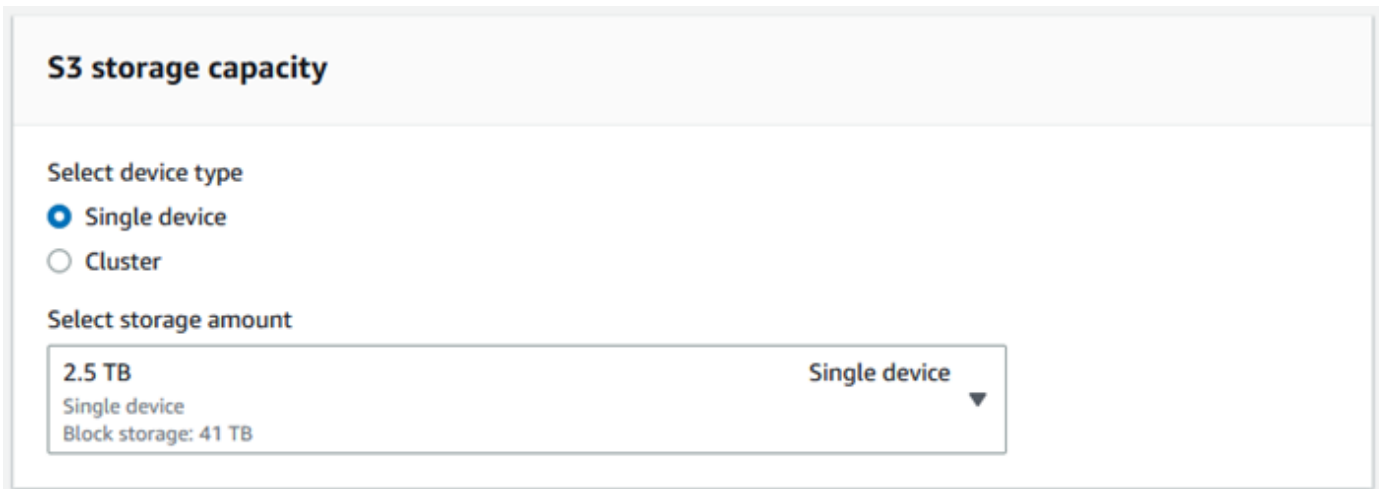
[Create a new S3 bucket](#)

☐	S3 bucket name	Date created
☐	my-gobally-unique-bucket-name	3/15/2023, 5:20:20 PM EDT
☐	do-not-delete-gatedgarden-audit-669419309129	3/11/2023, 5:13:13 PM EST

5. Se hai selezionato lo storage compatibile con Amazon S3 come tipo di storage, nella sezione Capacità di storage S3, procedi come segue:
 - a. Scegli di utilizzare lo storage compatibile con Amazon S3 su Snowball Edge su un singolo dispositivo o su un cluster di dispositivi. Vedi [Utilizzo di un AWS Snowball Edge cluster](#) in questa guida.
 - b. Seleziona la quantità di storage del dispositivo da utilizzare per lo storage compatibile con Amazon S3 su Snowball Edge.

Note

Se utilizzi uno storage compatibile con Amazon S3 su Snowball Edge, puoi gestire e creare bucket Amazon S3 dopo aver ricevuto il dispositivo, in modo da non doverli scegliere al momento dell'ordine. Scopri lo [storage compatibile con Amazon S3 su Snowball Edge](#) in questa guida.



The screenshot shows a configuration window titled "S3 storage capacity". It contains two sections: "Select device type" with radio buttons for "Single device" (selected) and "Cluster", and "Select storage amount" with a dropdown menu. The dropdown menu is open, showing "2.5 TB" as the selected option, with subtext "Single device" and "Block storage: 41 TB". To the right of the dropdown is a label "Single device" with a downward arrow.

6. Se hai selezionato il trasferimento dati basato su NFS come tipo di archiviazione, nella sezione Seleziona i tuoi bucket S3, esegui una o più delle seguenti operazioni per selezionare uno o più bucket S3:
- Scegli il bucket S3 che desideri utilizzare nell'elenco dei nomi dei bucket S3.
 - Nel campo Cerca un elemento, inserisci il nome completo o parziale del bucket per filtrare l'elenco dei bucket disponibili in base alla tua voce, quindi scegli il bucket.
 - Scegli Crea un nuovo bucket S3 per creare un nuovo bucket S3. Il nuovo nome del bucket viene visualizzato nell'elenco dei nomi del bucket. Sceglilo.
 - Dopo aver scelto i bucket S3 da utilizzare con il trasferimento dati NFS, scegli anche un bucket S3 da utilizzare come storage a blocchi. AMIs Scopri i passaggi per scegliere un bucket. [S3](#)

Puoi includere uno o più bucket S3. Questi bucket vengono visualizzati sul dispositivo come bucket S3 locali.

Choose your NFS storage

These S3 buckets will appear on directories on your device. You can transfer data onto these buckets using NFS.

 Only data stored in these directories will be ingested to your S3 buckets in the cloud.

The NFS storage limit is 80 TB

Create a new S3 bucket

 Search for an item

☐	S3 bucket name	Date created
☐	this-unique-bucket-name	6/14/2023, 12:20:08 PM EDT

- Nella sezione Compute using EC2 -compatible instances - optional, scegli Amazon EC2 - compatible AMIs dal tuo account da includere nel dispositivo. Oppure, nel campo di ricerca, inserisci in tutto o in parte il nome di un AMI per filtrare l'elenco di quelli AMIs disponibili nella tua voce, quindi scegli l'AMI.

Per maggiori informazioni sulla configurazione di un'AMI per Secure Shell (SSH), vedi [Configurazione di un'AMI per Snowball Edge e SSH](#)

Per ulteriori informazioni, consulta [Aggiungere un AMI quando si ordina il dispositivo](#) in questa guida.

Questa funzionalità comporta costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di AWS Snowball Edge](#).

- Scegliere il pulsante Next (Avanti).

Scelta delle funzionalità e delle opzioni

Scegli le funzionalità e le opzioni da includere nel processo del dispositivo AWS Snowball Edge, tra cui Amazon EKS Anywhere for Snow, un' AWS IoT Greengrass istanza e la funzionalità di gestione remota dei dispositivi.

Per scegliere le funzionalità e le opzioni

- Nella sezione Amazon EKS Anywhere on AWS Snow, per includere Amazon EKS Anywhere on AWS Snow, seleziona Includi Amazon EKS Anywhere on Snow e procedi come segue.

 Note

Ti consigliamo di creare il tuo cluster Kubernetes con l'ultima versione di Kubernetes disponibile supportata da Amazon EKS Anywhere. Per ulteriori informazioni, consulta [Amazon EKS-Anywhere Versioning](#). Se la tua applicazione richiede una versione specifica di Kubernetes, utilizza qualsiasi versione di Kubernetes offerta con supporto standard o esteso da Amazon EKS. Considera le date di rilascio e supporto delle versioni di Kubernetes quando pianifichi il ciclo di vita della tua implementazione. Questo ti aiuterà a evitare la potenziale perdita del supporto per la versione di Kubernetes che intendi utilizzare. Per ulteriori informazioni, consulta il calendario delle release di [Amazon EKS Kubernetes](#).

- a. Nella sezione Crea la tua AMI, scegli quella AMIs che hai creato per Amazon EKS Anywhere. Consultare [Azioni da completare prima di ordinare un dispositivo Snowball Edge per Amazon EKS Anywhere on Snow AWS](#).
- b. Nella sezione Alta disponibilità, per gestire i cluster Amazon EKS Anywhere su più dispositivi Snowball Edge, scegli il numero di dispositivi da includere nel tuo ordine.
2. Nella sezione AWS IoT Greengrass on Snow, per includere un'AMI convalidata per carichi di lavoro IoT, seleziona Installa AMI AWS IoT Greengrass convalidata sul mio dispositivo Snow.
3. Per abilitare la gestione remota del dispositivo Snowball Edge tramite o AWS OpsHub Snowball Edge Client, seleziona Gestisci il tuo dispositivo Snow da remoto con AWS OpsHub o Snowball Edge Client.
4. Seleziona il pulsante Avanti.

Scelta delle preferenze di sicurezza, spedizione e notifica

Argomenti

- [Scegli le preferenze di sicurezza per Snowball Edge](#)
- [Scegli le tue preferenze di spedizione per la ricezione e la restituzione di Snowball Edge](#)
- [Scegli le preferenze per le notifiche relative al job Snowball Edge](#)

Scegli le preferenze di sicurezza per Snowball Edge

L'impostazione della sicurezza aggiunge le autorizzazioni e le impostazioni di crittografia per il job AWS Snowball Edge per proteggere i dati durante il transito.

Per impostare la sicurezza per il tuo lavoro

1. Nella sezione Crittografia, scegli la chiave KMS che desideri utilizzare.
 - Se desideri utilizzare la chiave default AWS Key Management Service (AWS KMS), scegli AWS/importexport (default). Questa è la chiave predefinita che protegge i processi di importazione ed esportazione quando non viene definita nessun'altra chiave.
 - Se desideri fornire la tua AWS KMS chiave, scegli Inserisci una chiave ARN, fornisci Amazon Resource Name (ARN) nella casella ARN della chiave e scegli Usa questa chiave KMS. La chiave ARN verrà aggiunta all'elenco.
2. Nella sezione Scegli il tipo di accesso al servizio, esegui una delle seguenti operazioni:
 - La console Choose Snow creerà e utilizzerà un ruolo collegato al servizio per accedere alle AWS risorse per tuo conto. per concedere a AWS Snowball Edge le autorizzazioni per utilizzare Amazon S3 e Amazon Simple Notification Service (Amazon SNS) per tuo conto. Il ruolo garantisce la fiducia del AWS Security Token Service (AWS STS) AssumeRole al servizio Snow
 - Scegli Aggiungi un ruolo di servizio esistente da utilizzare, per specificare l'ARN del ruolo che desideri, oppure puoi utilizzare il ruolo predefinito.
3. Scegli Next (Successivo).

Scegli le tue preferenze di spedizione per la ricezione e la restituzione di Snowball Edge

La ricezione e la restituzione di un dispositivo Snowball Edge comportano la spedizione del dispositivo avanti e indietro, quindi è importante fornire informazioni di spedizione accurate.

Per fornire i dettagli di spedizione

1. Nella sezione Indirizzo di spedizione, scegli un indirizzo esistente o aggiungi un nuovo indirizzo.
 - Se scegli Usa indirizzo recente, vengono visualizzati gli indirizzi in archivio. Scegli con attenzione l'indirizzo che desideri dall'elenco.

- Se scegli Aggiungi un nuovo indirizzo, fornisci le informazioni sull'indirizzo richieste. Console di gestione della famiglia di servizi AWS Snow Salva le tue nuove informazioni di spedizione.

Note

Il paese fornito nell'indirizzo deve corrispondere al paese di destinazione del dispositivo e deve essere valido per quel paese.

2. Nella sezione Velocità di spedizione, scegli una velocità di spedizione per il lavoro. La velocità di spedizione non indica quanto presto puoi aspettarti di ricevere il dispositivo dal giorno in cui hai creato il lavoro. Piuttosto, indica l'ora in cui il dispositivo è in transito tra AWS e il tuo indirizzo di spedizione.

Potrebbero essere necessarie fino a 4 settimane per fornire e preparare il dispositivo per il lavoro prima che venga spedito. Questa tempistica dovrebbe essere presa in considerazione nel piano di progetto per garantire una transizione senza interruzioni.

Le velocità di spedizione che puoi scegliere sono:

- Spedizione in un giorno (1 giorno lavorativo)
- Spedizione in due giorni (2 giorni lavorativi)

Scegli le preferenze per le notifiche relative al job Snowball Edge

Le notifiche ti aggiornano sullo stato più recente dei tuoi lavori in AWS Snowball Edge. Crei un argomento SNS e ricevi e-mail da Amazon Simple Notification Service (Amazon SNS) man mano che lo stato del tuo lavoro cambia.

Per configurare le notifiche

- Nella sezione Imposta notifiche, esegui una delle seguenti operazioni:
 - Se desideri utilizzare un argomento SNS esistente, scegli Usa un argomento SNS esistente e scegli l'argomento Amazon Resource Name (ARN) dall'elenco.
 - Se desideri creare un nuovo argomento SNS, scegli Crea un nuovo argomento SNS. Inserisci un nome per l'argomento e fornisci un indirizzo email.

 Note

I lavori su ordinazione dei dispositivi Snow creati nelle regioni Stati Uniti occidentali (California settentrionale) e Stati Uniti occidentali (Oregon) vengono inoltrati attraverso la regione Stati Uniti orientali (Virginia settentrionale). Per questo motivo, le chiamate di servizio come Amazon SNS vengono dirette anche attraverso gli Stati Uniti orientali (Virginia settentrionale). Per un'esperienza ottimale, consigliamo di creare nuovi argomenti SNS nella regione Stati Uniti orientali (Virginia settentrionale).

Le notifiche riguarderanno uno dei seguenti stati del tuo lavoro:

- Job created (Processo creato)
- Preparazione dispositivo
- Preparing shipment (Preparazione spedizione)
- In transit to you (In transito verso l'utente)
- Delivered to you (Consegnato all'utente)
- In transito verso AWS
- Al centro di smistamento
- In AWS
- Importing (Importazione)
- Completato
- Annullato

Per ulteriori informazioni sulle notifiche di modifica dello stato del lavoro e sugli argomenti relativi ai SNS crittografati, consulta [Notifiche per Snowball](#) Edge in questa guida.

Seleziona Avanti.

Rivedi il riepilogo del lavoro e crea il tuo lavoro

Dopo aver fornito tutte le informazioni necessarie per il job AWS Snowball Edge, esaminatelo e createlo. Dopo aver creato il lavoro, AWS inizieremo a preparare lo Snowball Edge per la spedizione.

Le offerte di lavoro sono soggette alle leggi sul controllo delle esportazioni in determinati paesi e potrebbero richiedere una licenza di esportazione. Si applicano anche le leggi statunitensi in materia di esportazione e riesportazione. È vietata la deroga alle leggi e ai regolamenti nazionali e statunitensi.

1. Nella pagina di riepilogo del lavoro, rivedi tutte le sezioni prima di creare il lavoro. Se desideri apportare modifiche, scegli Modifica per la sezione appropriata e modifica le informazioni.
2. Al termine della revisione e della modifica, scegli Crea lavoro.

Note

Dopo aver creato un lavoro per ordinare un dispositivo Snowball Edge, puoi annullarlo mentre si trova nello stato di creazione del lavoro senza incorrere in alcun addebito. Per ulteriori informazioni, consulta [Annullamento di un lavoro tramite](#) Console di gestione della famiglia di servizi AWS Snow

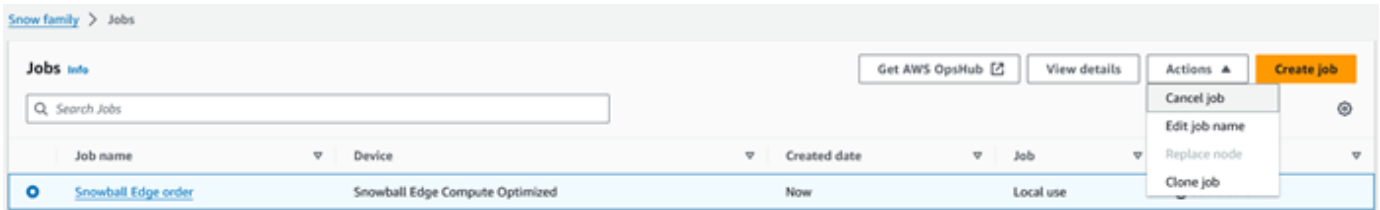
Dopo aver creato il lavoro, puoi visualizzarne lo stato nella sezione Stato del lavoro.

Annullamento di un lavoro per ordinare uno Snowball Edge

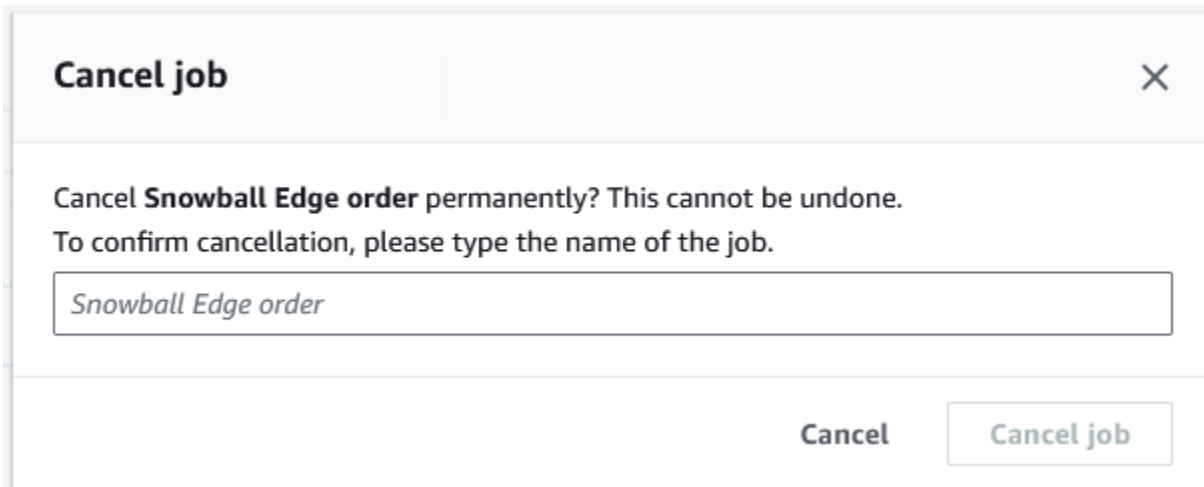
Dopo aver creato un lavoro per ordinare un dispositivo Snowball Edge, puoi annullare il lavoro tramite Console di gestione della famiglia di servizi AWS Snow. Se annulli il lavoro, non riceverai il dispositivo ordinato. È possibile annullare il lavoro solo quando lo stato del lavoro è Job creato. Dopo che il lavoro ha superato questo stato, non è possibile annullarlo. Per ulteriori informazioni, consulta [Job Statuses](#).

Quando annulli un lavoro mentre è nello stato Job creato, non ti verrà addebitato alcun costo per il dispositivo Snowball Edge. La fatturazione inizia solo dopo che il dispositivo è stato preparato e spedito.

1. Accedi al [Console di gestione della famiglia di servizi AWS Snow](#).
2. Scegli il lavoro da annullare.
3. Scegli Azioni. Dal menu visualizzato, scegli Annulla lavoro.



4. Viene visualizzata la finestra Annulla lavoro. Per confermare l'annullamento del lavoro, inserisci **job name** e scegli Annulla lavoro. Nell'elenco dei lavori, Annullato appare nella colonna Stato.



Clonazione di un lavoro per ordinare uno Snowball Edge nel Console di gestione della famiglia di servizi AWS Snow

Quando crei per la prima volta un processo di importazione o un processo di elaborazione e archiviazione locale, potresti scoprire di aver bisogno di più di un AWS Snowball Edge dispositivo. Poiché i processi di importazione e quelli di storage ed elaborazione locale sono associati a un singolo dispositivo, se sono necessari più dispositivi occorre creare più di un processo. Quando si creano processi aggiuntivi puoi eseguire nuovamente la procedura guidata di creazione del processo nella console o clonare un processo esistente.

Note

La clonazione di un processo è un collegamento disponibile nella console per semplificare la creazione di ulteriori processi. Se crei un processo con l'API di gestione processi, è sufficiente eseguire nuovamente il comando di creazione del processo.

Clonare un lavoro significa ricrearlo esattamente, ad eccezione di un nome modificato automaticamente. La clonazione è un processo semplice.

Per clonare di un processo nella console

1. In Console di gestione della famiglia di servizi AWS Snow, scegli il tuo lavoro dalla tabella.
2. Per Actions (Operazioni) scegliere Clone job (Clona processo).

La procedura guidata Create job (Crea processo) visualizza l'ultima pagina Step 6: Review (Fase 6: Verifica).

3. Verificare le informazioni e apportare le modifiche necessarie selezionando il pulsante Edit (Modifica) appropriato.
4. Per creare il processo clonato scegliere Create job (Crea processo).

I lavori clonati sono denominati nel formato **Job Name**-clone -. **number** Il numero viene automaticamente aggiunto al nome del processo e indica quante volte il processo è stato clonato dopo la prima clonazione. Ad esempio, AprilFinanceReports-clone rappresenta il primo lavoro clonato del lavoro e DataCenterMigration-clone-42 rappresenta il clone di AprilFinanceReportsquaranta secondi del lavoro. DataCenterMigration

Ricevere lo Snowball Edge

Quando ricevi il AWS Snowball Edge dispositivo, potresti notare che non viene fornito in una confezione. Il dispositivo è di per se un contenitore di spedizione fisicamente robusto. La prima volta che ricevi il dispositivo, controlla se risulta danneggiato o manomesso in modo evidente. Se noti qualcosa di sospetto sul dispositivo, non connetterlo alla rete interna. Invece, contattati [Supporto AWS](#) e informali del problema in modo che possa esserti spedito un nuovo dispositivo.

Important

Il AWS Snowball Edge dispositivo è di proprietà di AWS. La manomissione di un AWS Snowball Edge dispositivo è una violazione della Politica di utilizzo AWS accettabile. Per ulteriori informazioni, consulta la Politica di [utilizzo AWS accettabile](#).

Il dispositivo ha un aspetto simile all'immagine seguente.



Se sei pronto per collegare il dispositivo alla rete interna, consulta la sezione successiva.

Successivo: [Connessione di uno Snowball Edge alla rete locale](#)

Connessione di uno Snowball Edge alla rete locale

Utilizzando la procedura seguente, si connette il AWS Snowball Edge dispositivo alla rete locale. Non è necessario connettere il dispositivo a Internet. Il dispositivo è dotato di tre porte: una anteriore, una posteriore e una superiore.

Per connettere il dispositivo alla rete

1. Aprire gli sportelli anteriore e posteriore, facendoli scorrere all'interno della relativa fessura. In questo modo è possibile accedere al touch screen sul display LCD incorporato nel lato anteriore del dispositivo e alle porte di alimentazione e di rete nella parte posteriore.

Note

Non chiudere le porte anteriori e posteriori mentre usi il dispositivo Snowball Edge. Le porte aperte consentono all'aria di raffreddare il dispositivo. La chiusura delle porte durante l'utilizzo del dispositivo può causare lo spegnimento del dispositivo per evitare il surriscaldamento.

2. Aprire lo sportello superiore e rimuovere il cavo di alimentazione fornito dal relativo gancio, quindi collegare il dispositivo all'alimentazione.
3. Scegli uno dei tuoi RJ45 cavi di rete SFP+ o QSFP+ e collega il dispositivo alla rete. La porte di rete si trovano sulla parte posteriore del dispositivo.
4. Accendi il AWS Snowball Edge dispositivo premendo il pulsante di accensione sopra il display LCD.
5. Quando il dispositivo è pronto, sul display LCD viene riprodotto un breve video prima dell'avvio del dispositivo. Dopo circa dieci minuti, il dispositivo è pronto per essere sbloccato.
6. (Facoltativo) Modificare le impostazioni di rete predefinite tramite il display LCD scegliendo CONNECTION (CONNESSIONE).

Puoi modificare l'indirizzo IP in un indirizzo statico diverso, che puoi fornire utilizzando la seguente procedura.

Per risolvere i problemi di avvio, vedere. [Risoluzione dei problemi di avvio con Snowball Edge](#)

Per modificare l'indirizzo IP di un dispositivo AWS Snowball Edge

1. Sul display LCD, seleziona CONNECTION (CONNESSIONE).

Viene visualizzata una schermata che mostra le impostazioni di rete correnti del AWS Snowball Edge dispositivo. L'indirizzo IP sotto la casella a discesa viene aggiornato automaticamente in base all'indirizzo DHCP richiesto dal AWS Snowball Edge dispositivo.

2. (Opzionale) Cambiare l'indirizzo IP in un indirizzo IP statico. Puoi mantenerlo così come è.

Il dispositivo è ora connesso alla rete.

 Important

Per evitare di danneggiare i dati, non scollegare il AWS Snowball Edge dispositivo o modificarne le impostazioni di connessione mentre è in uso.

Successivo: [Ottenere le credenziali per accedere a Snowball Edge](#)

Ottenere le credenziali per accedere a Snowball Edge

A ogni job è associato un set di credenziali che devi ottenere dall'API Console di gestione della famiglia di servizi AWS Snow o dall'API di gestione dei lavori per autenticare l'accesso a Snowball Edge. Queste credenziali sono un file manifesto crittografato e un codice di sblocco associato. Il file manifest contiene informazioni importanti sul processo e le autorizzazioni a esso associate.

 Note

Ottieni le tue credenziali dopo che il dispositivo è in transito verso di te. Puoi vedere lo stato del tuo lavoro in Console di gestione della famiglia di servizi AWS Snow Per ulteriori informazioni, consulta [Stati delle offerte di lavoro Snowball Edge](#).

Per ottenere le tue credenziali utilizzando la console

1. Accedi a Console di gestione AWS e apri il [Console di gestione della famiglia di servizi AWS Snow](#).
2. Sulla console, cerca nella tabella il lavoro specifico per cui scaricare il manifesto del lavoro, quindi scegli quel lavoro.
3. Espandi il riquadro di stato del lavoro e scegli Visualizza dettagli del lavoro.
4. Nel riquadro dei dettagli visualizzato, espandere Credentials (Credenziali), quindi eseguire le seguenti operazioni:
 - Prendi nota del codice di sblocco (inclusi i trattini), perché devi fornire tutti i 29 caratteri per sbloccare il dispositivo.
 - Nella finestra di dialogo, scegliete Scarica manifesto e seguite le istruzioni per scaricare il file del manifesto del lavoro sul computer. Il nome del file manifest include il Job ID (ID processo).

 Note

Ti consigliamo di non salvare una copia del codice di sblocco nella stessa posizione sul computer del manifesto del lavoro. Per ulteriori informazioni, consulta [Procedure consigliate per l'utilizzo di un dispositivo Snowball Edge](#).

Ora che hai le tue credenziali, il passaggio successivo consiste nel scaricare il client Snowball Edge, che viene utilizzato per sbloccare AWS Snowball Edge il dispositivo.

Successivo: [Scaricamento e installazione del client Snowball Edge](#)

Sbloccare Snowball Edge

Questa sezione descrive come sbloccare il dispositivo Snowball Edge utilizzando il client Snowball Edge.

Prima di utilizzare un dispositivo Snowball Edge per trasferire dati o eseguire attività di edge computing, è necessario sbloccare il dispositivo. Quando sblocchi il dispositivo, autentichi la tua capacità di accedervi fornendo due tipi di credenziali: un codice di sblocco a 29 cifre e un file manifest. Dopo aver sbloccato il dispositivo, puoi configurarlo ulteriormente, spostare dati da o verso il dispositivo, configurare e utilizzare istanze EC2 compatibili con Amazon e altro ancora.

Prima di sbloccare un dispositivo, è necessario collegarlo all'alimentazione e alla rete, accenderlo e assegnargli un indirizzo IP. Vedi le [Connessione di uno Snowball Edge alla rete locale](#). Sono necessarie le seguenti informazioni sul dispositivo Snowball Edge:

- Scarica e installa il client Snowball Edge. Per ulteriori informazioni, consulta [Scaricamento e installazione del client Snowball Edge](#).
- Ottieni le credenziali da. Console di gestione della famiglia di servizi AWS Snow Per uno o più dispositivi autonomi, i codici di sblocco e il file manifest per ogni Snowball Edge. Per un cluster di dispositivi Snowball Edge, un unico codice di sblocco e un file manifest per il cluster. Per ulteriori informazioni sul download delle credenziali, consulta. [Ottenere le credenziali per accedere a Snowball Edge](#)
- Accendi ogni dispositivo e connettilo alla rete. Per ulteriori informazioni, consulta [Connessione di uno Snowball Edge alla rete locale](#).

Per sbloccare un dispositivo autonomo con il client Snowball Edge

1. Individua l'indirizzo IP del AWS Snowball Edge dispositivo sul display LCD del AWS Snowball Edge dispositivo, nella scheda Connessioni. Prendere nota di tale indirizzo IP.
2. Utilizza il `unlock-device` comando per autenticare l'accesso a Snowball Edge con l'indirizzo IP di Snowball Edge e le tue credenziali, come segue.

```
snowballEdge unlock-device --endpoint https://ip-address-of-device --manifest-file /Path/to/manifest/file.bin --unlock-code 29-character-unlock-code
```

Il dispositivo indica che è stato sbloccato correttamente con il seguente messaggio.

```
Your Snowball Edge device is unlocking. You may determine the unlock state of your device using the describe-device command. Your Snowball Edge device will be available for use when it is in the UNLOCKED state.
```

Se il comando ritorna `connection refused`, vedi [Risoluzione dei problemi relativi allo sblocco di Snowball Edge](#).

Example del **unlock-device** comando

In questo esempio, l'indirizzo IP del dispositivo è `192.0.2.0`, il nome del file manifest è `JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin` e il codice di sblocco di 29 caratteri è `12345-abcde-12345-ABCDE-12345`

```
snowballEdge unlock-device --endpoint https://192.0.2.0 --manifest-file /Downloads/JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin /--unlock-code 12345-abcde-12345-ABCDE-12345
```

Per sbloccare un cluster di dispositivi Snowball Edge con il client Snowball Edge

1. Trova l'indirizzo IP di ogni dispositivo del cluster sul display LCD di ogni AWS Snowball Edge dispositivo, nella scheda Connessioni. Annotare gli indirizzi IP.

2. Utilizza il `snowballEdge unlock-cluster` comando per autenticare l'accesso al cluster di AWS Snowball Edge dispositivi con l'indirizzo IP di uno dei dispositivi del cluster, le tue credenziali e gli indirizzi IP di tutti i dispositivi del cluster, come segue.

```
snowballEdge unlock-cluster --endpoint https://ip-address-of-device --manifest-  
file Path/to/manifest/file.bin --unlock-code 29-character-unlock-code --device-ip-  
addresses ip-address-of-cluster-device-1 ip-address-of-cluster-device-2 ip-address-  
of-cluster-device-3
```

Il cluster di dispositivi indica che è stato sbloccato correttamente con il seguente messaggio.

```
Your Snowball Edge Cluster is unlocking. You may determine the unlock state of your  
cluster using the describe-cluster command. Your Snowball Edge Cluster will be  
available for use when your Snowball Edge devices are in the UNLOCKED state.
```

Se il comando ritorna `connection refused`, vedi [Risoluzione dei problemi relativi allo sblocco di Snowball Edge](#).

Example del **unlock-cluster** comando

In questo esempio per un cluster di cinque dispositivi, l'indirizzo IP di uno dei dispositivi del cluster è `192.0.2.0`, il nome del file manifest è `JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin` e il codice di sblocco di 29 caratteri è `12345-abcde-12345-ABCDE-12345`

```
snowballEdge unlock-cluster --endpoint https://192.0.2.0 --manifest-file /  
Downloads/JID2EXAMPLE-0c40-49a7-9f53-916aEXAMPLE81-manifest.bin /
```

```
--unlock-code 12345-abcde-12345-ABCDE-12345 --device-ip-addresses 192.0.2.0  
192.0.2.1 192.0.2.2 192.0.2.3 192.0.2.4
```

Risoluzione dei problemi relativi allo sblocco di Snowball Edge

Se il `unlock-device` comando viene restituito `connection refused`, è possibile che la sintassi del comando sia stata digitata in modo errato oppure la configurazione del computer o della rete potrebbe impedire al comando di raggiungere il dispositivo Snow. Esegui queste azioni per risolvere la situazione:

1. Assicurati che il comando sia stato inserito correttamente.
 - a. Utilizzate lo schermo LCD del dispositivo per verificare che l'indirizzo IP utilizzato nel comando sia corretto.
 - b. Assicuratevi che il percorso del file manifesto utilizzato nel comando sia corretto, incluso il nome del file.
 - c. Usa la [console di gestione AWS Snowball Edge](#) per verificare che il codice di sblocco utilizzato nel comando sia corretto.
2. Assicurati che il computer che stai utilizzando sia sulla stessa rete e sottorete del dispositivo Snow.
3. Assicurati che il computer che stai utilizzando e la rete siano configurati per consentire l'accesso al dispositivo Snow. Usa il `ping` comando del tuo sistema operativo per determinare se il computer è in grado di raggiungere il dispositivo Snow tramite la rete. Controlla le configurazioni del software antivirus, della configurazione del firewall, della rete privata virtuale (VPN) o altre configurazioni del computer e della rete.

Ora puoi iniziare a usare Snowball Edge.

Successivo: [Configurazione degli utenti locali su Snowball Edge](#)

Configurazione degli utenti locali su Snowball Edge

Di seguito sono riportati i passaggi per configurare un amministratore locale sul AWS Snowball Edge dispositivo.

1. Recupera le credenziali utente root

Utilizzare `snowballEdge list-access-keys` e `snowballEdge get-secret-access-key` per ottenere le credenziali locali. Per ulteriori informazioni, consulta [Ottenere le credenziali per uno Snowball Edge](#).

2. Configurare le credenziali utente root utilizzando **aws configure**

Fornire AWS Access Key ID, AWS Secret Access Key e Default region name. Il nome della regione deve essere `snow`. Facoltativamente fornire un Default output format. Per ulteriori informazioni sulla configurazione di AWS CLI, vedere [Configurazione](#) di AWS CLI nella Guida per l'AWS Command Line Interface utente.

3. Crea uno o più utenti locali sul tuo dispositivo

Utilizzare il comando `create-user` per aggiungere utenti al dispositivo.

```
aws iam create-user --endpoint endpointIPAddress:6078 --region snow --user-name UserName --profile ProfileID
```

Dopo aver aggiunto gli utenti in base alle esigenze aziendali, è possibile archiviare le credenziali AWS root in un luogo sicuro e utilizzarle solo per attività di gestione degli account e dei servizi. Per ulteriori informazioni sulla creazione di utenti IAM, consulta [Creating an IAM user in your Account AWS nella](#) IAM User Guide.

4. Crea una chiave di accesso per l'utente

Warning

Questo scenario richiede agli utenti IAM un accesso programmatico e credenziali a lungo termine, il che presenta 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. Le chiavi di accesso possono essere aggiornate se necessario. Per ulteriori informazioni, consulta [Update access keys](#) nella IAM User Guide.

Utilizzare il comando `create-access-key` per creare una chiave di accesso per l'utente.


```
aws iam create-access-key --endpoint endpointIPAddress:6078 --region snow --user-name UserName --profile ProfileID
```

Salva le informazioni chiave di accesso in un file e distribuiscilo agli utenti.

5. Creazione di un access point

È possibile che utenti diversi abbiano diversi livelli di accesso alle funzionalità sul dispositivo. Nell'esempio seguente viene creato un documento dei criteri denominato s3-only-policy e allegato a un utente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

```
aws iam create-policy --endpoint endpointIPAddress:6078 --region snow --policy-name s3-only-policy --policy-document file://s3-only-policy --profile ProfileID
```

6. Associare la policy all'utente

Utilizzare attach-user-policy per allegare il criterio s3-only-a un utente.

```
aws iam attach-user-policy --endpoint endpointIPAddress:6078 --region snow --user-name UserName --policy-arn arn:aws:iam::AccountID:policy/POLICYNAME --profile ProfileID
```

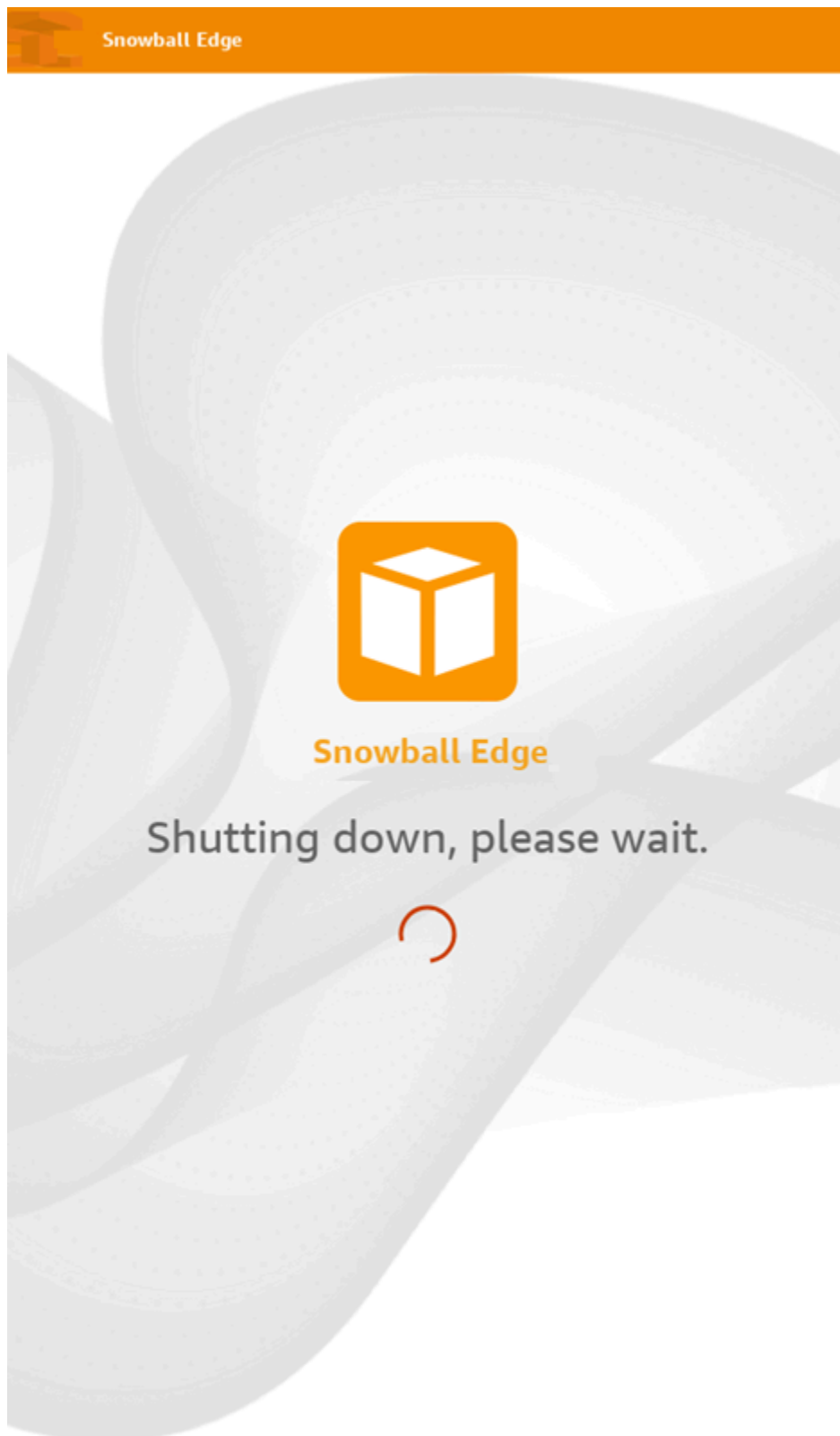
Per ulteriori informazioni sull'utilizzo locale di IAM, consulta [Utilizzo di IAM localmente su Snowball Edge](#).

Riavvio del dispositivo Snowball Edge

Prima di riavviare un dispositivo Snowball Edge, assicurati che il trasferimento di tutti i dati verso il dispositivo sia stato interrotto.

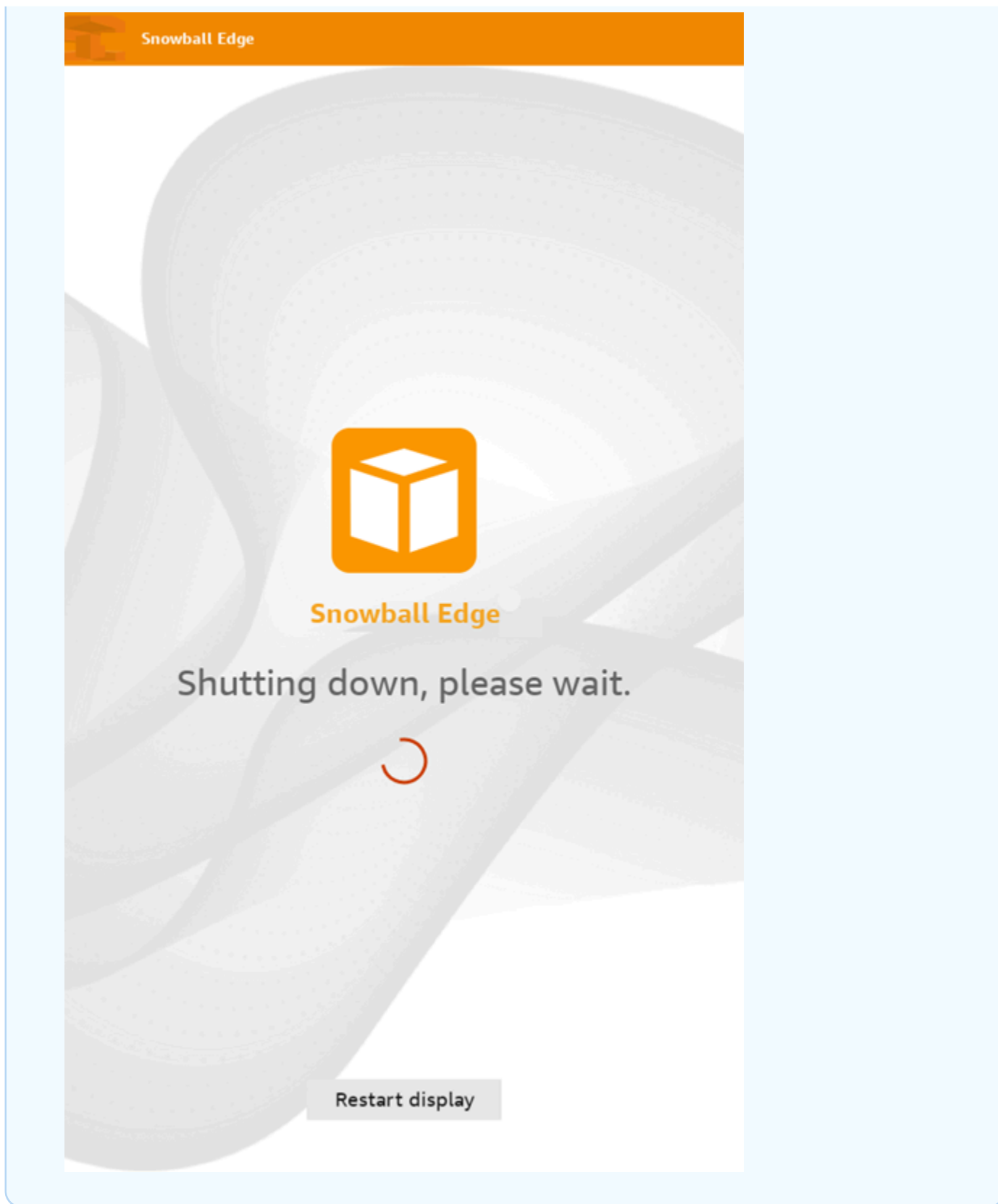
Per riavviare il dispositivo utilizzando il pulsante di accensione:

1. Quando tutte le comunicazioni con il dispositivo sono terminate, spegnilo premendo il pulsante di accensione situato sopra lo schermo LCD. Lo spegnimento del dispositivo richiede circa 20 secondi. Durante lo spegnimento del dispositivo, sullo schermo LCD viene visualizzato un messaggio che indica che il dispositivo si sta spegnendo.



 Note

Se sullo schermo LCD viene visualizzato il messaggio di spegnimento quando il dispositivo non è effettivamente spento, premere il pulsante Riavvia lo schermo per ripristinare il normale funzionamento dello schermo.



2. Premere il pulsante di accensione. Quando il dispositivo è pronto, sul display LCD viene riprodotto un breve video prima dell'avvio del dispositivo. Dopo circa dieci minuti, il dispositivo è pronto per essere sbloccato.
3. Sbloccare il dispositivo. Consultare [Sbloccare Snowball Edge](#).

Per riavviare il dispositivo utilizzando il client Snowball Edge:

1. Quando tutte le comunicazioni con il dispositivo sono terminate, usa il `reboot-device` comando per riavviarlo. Quando il dispositivo è pronto, sul display LCD viene riprodotto un breve video prima dell'avvio del dispositivo. Dopo circa dieci minuti, il dispositivo è pronto per essere sbloccato.

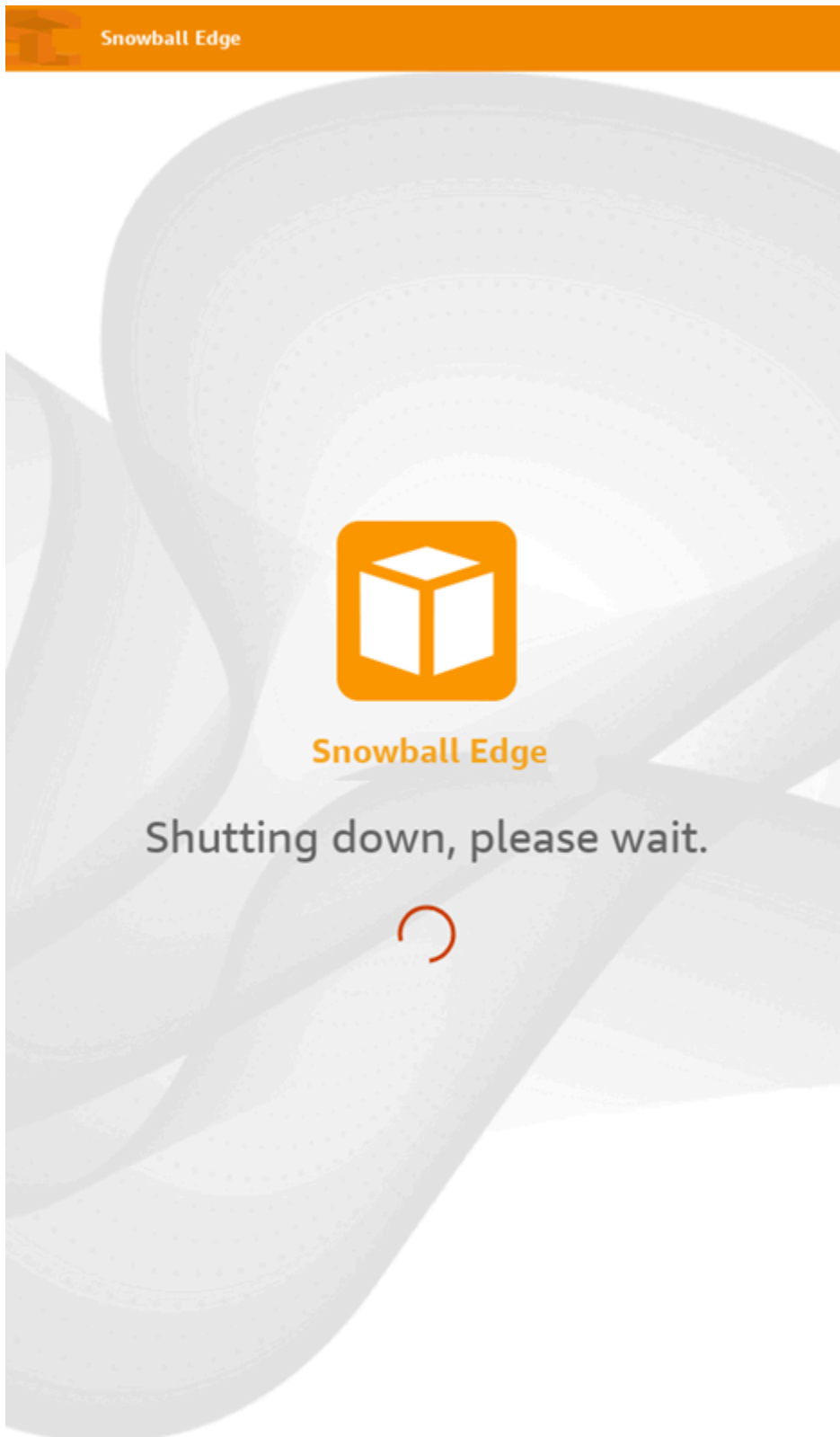
```
snowballEdge reboot-device --profile profile-name
```

2. Sbloccare il dispositivo. Consultare [Sbloccare Snowball Edge](#).

Spegnimento dello Snowball Edge

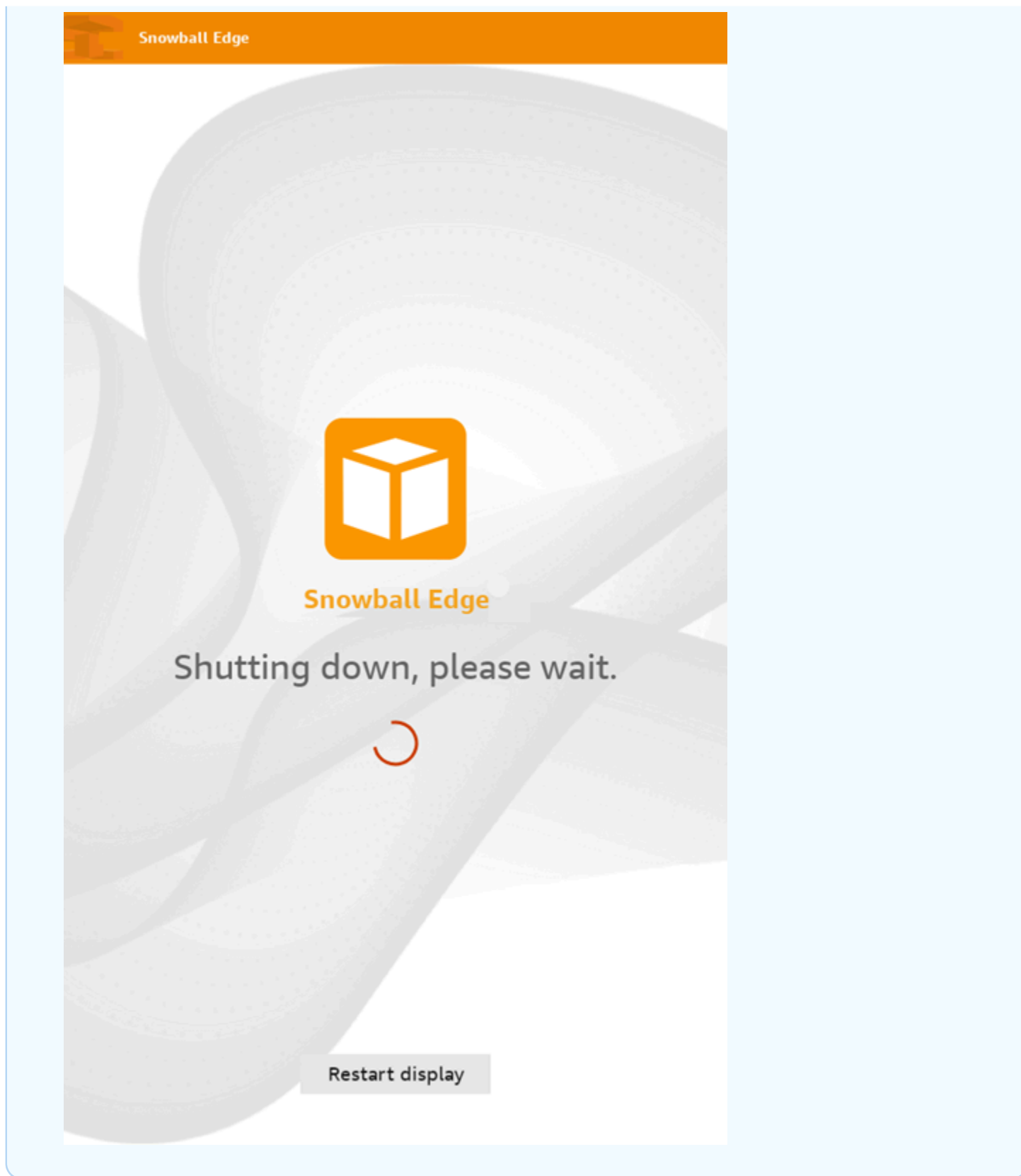
Una volta terminato il trasferimento dei dati sul AWS Snowball Edge dispositivo, preparalo per il viaggio di ritorno a AWS. Prima di continuare, assicurati che tutti i trasferimenti dati al dispositivo siano stati interrotti. Se stavi usando l'interfaccia NFS per trasferire dati, disattivala prima di spegnere il dispositivo. Per ulteriori informazioni, vedere [Gestione dell'interfaccia NFS](#).

Quando tutte le comunicazioni con il dispositivo sono terminate, spegnilo premendo il pulsante di accensione situato sopra lo schermo LCD. Lo spegnimento del dispositivo richiede circa 20 secondi. Durante lo spegnimento del dispositivo, sullo schermo LCD viene visualizzato un messaggio che indica che il dispositivo si sta spegnendo.



 Note

Se sullo schermo LCD viene visualizzato il messaggio di spegnimento quando il dispositivo non è effettivamente spento, premere il pulsante Riavvia lo schermo per ripristinare il normale funzionamento dello schermo.



Dopo lo spegnimento del dispositivo, le informazioni di spedizione vengono visualizzate sul display E Ink. Se le informazioni sulla spedizione del reso non vengono visualizzate sul display di E Ink, contatta Supporto.

Successivo: [Restituzione del dispositivo Snowball Edge](#)

Restituzione del dispositivo Snowball Edge

Dopo aver finito di utilizzare Snowball Edge e averlo spento, un corriere lo restituirà a AWS. Il corriere fornisce automaticamente un numero di tracciamento per la spedizione del dispositivo. Il numero di tracciamento appare nel Console di gestione della famiglia di servizi AWS Snow. Puoi accedere al numero di tracciamento e a un link al sito web di tracciamento del corriere visualizzando i dettagli sullo stato dell'offerta nella console. Per ulteriori informazioni, consulta [Spedizione di reso per i dispositivi Snowball Edge](#).

Il corriere consegna il dispositivo a un centro di AWS smistamento e il dispositivo viene inoltrato al data center. AWS Al data center, AWS si assicurerà che il dispositivo non sia stato manomesso durante la spedizione e che sia integro. Se il dispositivo contiene dati da importare in Amazon S3, AWS inizierà l'importazione. In caso contrario, i dati sul dispositivo verranno cancellati in modo sicuro. È possibile tenere traccia delle modifiche di stato durante l'AWS elaborazione del dispositivo in Console di gestione della famiglia di servizi AWS Snow. Riceverai notifiche Amazon SNS sulle modifiche allo stato se hai selezionato tale opzione quando hai creato il lavoro per ordinare il dispositivo. Per ulteriori informazioni, consulta [Monitoraggio dello stato dell'importazione](#).

I valori dello stato finale includono quando il AWS Snowball Edge dispositivo è stato ricevuto da AWS, quando inizia l'importazione dei dati e quando il processo è completato.

Note

Se il dispositivo contiene dati che intendevi importare in Amazon S3 e non desideri che i dati sul dispositivo vengano importati, contatta Supporto per richiedere l'annullamento del job Snow. Se annulli il processo, salteremo il trasferimento dei dati e cancelleremo il dispositivo in modo sicuro seguendo i processi stabiliti. Non siamo in grado di tenere un dispositivo contenente i tuoi dati presso le nostre strutture a causa della nostra rigida catena di custodia e procedure operative.

Per preparare un AWS Snowball Edge dispositivo per la spedizione di ritorno

1. Spegnerne il dispositivo. Per ulteriori informazioni, consulta [Spegnimento dello Snowball Edge](#).
2. Scollegare tutti i cavi di rete collegati al dispositivo.
3. Scollegare il cavo di alimentazione. Riponilo nell'apposito passacavi sulla parte superiore del dispositivo. AWS Snowball Edge
4. Chiudi le porte sul retro, sulla parte superiore e anteriore del AWS Snowball Edge dispositivo. Premi ogni porta finché non senti e senti un clic.

Successivo: [Spedizione di ritorno per Snowball Edge](#)

Spedizione di ritorno per Snowball Edge

Il AWS Snowball Edge dispositivo viene spedito e consegnato a un AWS data center. Le informazioni sulla spedizione prepagata nella schermata E Ink del dispositivo includono l'indirizzo per la restituzione del AWS Snowball Edge dispositivo. La velocità di spedizione per il reso corrisponde alla velocità di spedizione originale al momento della ricezione del dispositivo. Puoi tenere traccia delle modifiche allo stato utilizzando e monitorare l'avanzamento del pacco tramite il corriere della tua regione. Console di gestione della famiglia di servizi AWS Snow

Per ulteriori informazioni su come restituire il AWS Snowball Edge dispositivo, consulta [Corrieri di spedizione per Snowball Edge](#).

Important

Salvo diversa indicazione AWS, non apporre mai un'etichetta di spedizione separata sul AWS Snowball Edge dispositivo. Utilizza sempre le informazioni di spedizione visualizzate sul display E Ink del AWS Snowball Edge dispositivo.

Corrieri di spedizione per Snowball Edge

Quando crei un lavoro per ordinare un dispositivo Snowball Edge, fornisci l'indirizzo a cui spedire il AWS Snowball Edge dispositivo. Il corriere che supporta la tua regione gestisce la spedizione dei dispositivi AWS da e verso AWS te. Puoi visualizzare le informazioni sulla spedizione in uscita quando il tuo lavoro raggiunge lo stato Preparazione della spedizione.

Esiste un numero di tracciamento per ogni AWS Snowball Edge dispositivo spedito. Puoi trovare il numero di tracciamento e un link al sito web di tracciamento utilizzando la dashboard dei [Console di gestione della famiglia di servizi AWS Snow](#) lavori o l'API di gestione dei lavori.

Questi operatori sono supportati per AWS Snowball Edge i dispositivi:

- Per l'India, Blue Dart è il corriere.
- Per Corea, Giappone, Australia e Indonesia, Kuehne + Nagel è il corriere.
- Per la Cina e Hong Kong, S.F. Express è il corriere.
- Per tutte le altre regioni, il corriere è [UPS](#).

Argomenti

- [Prelievi UPS Snowball Edge in UE, Stati Uniti, Regno Unito, Sud Africa e Canada](#)
- [Pickup Snowball Edge nel Regno Unito](#)
- [Pickup Snowball Edge in Brasile](#)
- [Pickup Snowball Edge in Australia](#)
- [Pickup Snowball Edge in India](#)
- [Pickup Snowball Edge in Corea](#)
- [Pickup Snowball Edge a Hong Kong](#)
- [Pickup Snowball Edge a Singapore, Giappone e Indonesia](#)
- [Snowball Edge ricevimento e restituzione a Dubai, Emirati Arabi Uniti](#)
- [Velocità di spedizione per Snowball Edge](#)

Prelievi UPS Snowball Edge in UE, Stati Uniti, Regno Unito, Sud Africa e Canada

UPS può spesso ritirare il dispositivo nell'UE, negli Stati Uniti, nel Regno Unito, in Sudafrica e in Canada. Ecco alcune linee guida utili:

- Pianifica un ritiro direttamente con UPS o porta il AWS Snowball Edge dispositivo presso un centro di consegna dei pacchi UPS per la spedizione. AWS
- L'etichetta di spedizione UPS prepagata sul display E Ink contiene l'indirizzo di restituzione del dispositivo. AWS Snowball Edge
- Il AWS Snowball Edge dispositivo viene consegnato a un centro di AWS smistamento e inoltrato a un data center. AWS UPS ti fornisce un numero di tracciamento.

 Important

Salvo diversa indicazione AWS, non apporre mai un'etichetta di spedizione separata sul AWS Snowball Edge dispositivo. Utilizza sempre le informazioni di spedizione visualizzate sul display E Ink del dispositivo.

UPS spedisce i dispositivi Snowball Edge nei seguenti paesi membri dell'UE: Austria, Belgio, Bulgaria, Croazia, Repubblica di Cipro, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Italia, Irlanda, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna e Svezia.

 Note

Gli ordini tra il Regno Unito e i paesi dell'Unione Europea sono ora considerati internazionali e richiedono l'approvazione attraverso uno speciale processo internazionale. Se devi spedire il tuo dispositivo tra il Regno Unito e l'UE, inviaci un'e-mail all'<indirizzo snowball-shipping@amazon.com> per richiedere una fattura commerciale prima di organizzare il ritiro o la riconsegna con UPS.

I servizi UPS per i prodotti Snowball Edge sono nazionali solo all'interno di un Paese.

Pickup Snowball Edge nel Regno Unito

Nel Regno Unito, tenete a mente le seguenti informazioni per consentire a UPS di ritirare uno Snowball Edge:

- Puoi far ritirare il AWS Snowball Edge dispositivo da UPS programmando un ritiro direttamente con UPS oppure portalo a un centro di riconsegna UPS per la spedizione. AWS Snowball Edge AWS
- L'etichetta di spedizione UPS prepagata sul display E Ink contiene l'indirizzo corretto a cui restituire il dispositivo. AWS Snowball Edge
- Il AWS Snowball Edge dispositivo viene consegnato a un centro di AWS smistamento e inoltrato al data center. AWS UPS restituisce automaticamente un numero di tracciamento per il processo.

 Important

Salvo diversa indicazione personale AWS, non apporre mai un'etichetta di spedizione separata sul dispositivo. AWS Snowball Edge Utilizza sempre le informazioni di spedizione visualizzate sul display E Ink del dispositivo.

I servizi UPS per i prodotti Snowball Edge sono nazionali solo all'interno di un Paese.

 Note

Da gennaio 2021, il Regno Unito non fa più parte dell'UE. Gli ordini tra il Regno Unito e altri paesi dell'UE sono ordini internazionali, un processo di disponibilità non generale approvato solo attraverso una speciale procedura internazionale. Se un cliente è stato approvato e sta restituendo un dispositivo da un paese dell'UE a LHR o dal Regno Unito a un paese dell'UE, deve prima richiedere un reso a <snowball-shipping@amazon.com> in modo da poter fornire una fattura commerciale prima di organizzare il ritiro con UPS. up/drop

Pickup Snowball Edge in Brasile

Ecco alcune linee guida con cui UPS può ritirare un dispositivo Snowball Edge in Brasile:

- Quando sei pronto a restituire un dispositivo Snowball Edge, chiama il numero 0800-770-9035 per fissare un ritiro con UPS.
- Snowball Edge Edge è disponibile a livello nazionale in Brasile, che include 26 stati e il Distrito Federal.
- Se si dispone di un codice fiscale Nacional de Cadastro Pessoa Juridica (CNPJ), accertarsi di conoscerlo prima di creare il processo.
- È necessario emettere il documento appropriato per restituire il dispositivo Snowball Edge. Verifica con il tuo ufficio fiscale quale dei seguenti documenti è richiesto nel tuo stato, in base alla tua registrazione all'Imposto sobre Circulação de Mercadorias e Serviços (ICMS):
 - A San Paolo: di solito sono richieste una dichiarazione non ICMS e una fattura fiscale elettronica (NF-e).
 - Fuori San Paolo — Di solito sono richiesti:
 - Una dichiarazione non ICMS

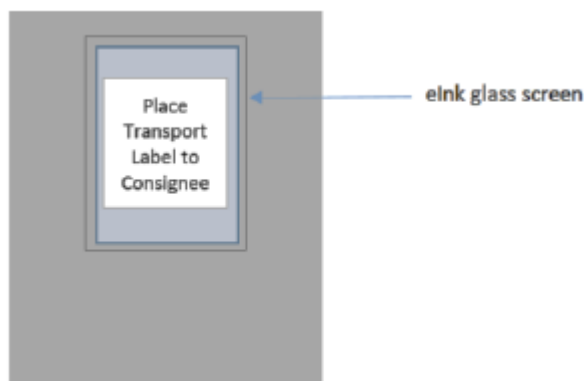
- Una nota fiscal avulsa
- Una Electronic Tax Invoice (NF-e)

Note

Per le dichiarazioni dei contribuenti non conformi all'ICMS, consigliamo di generare quattro copie della dichiarazione: una per i registri e le altre tre per il trasporto.

Pickup Snowball Edge in Australia

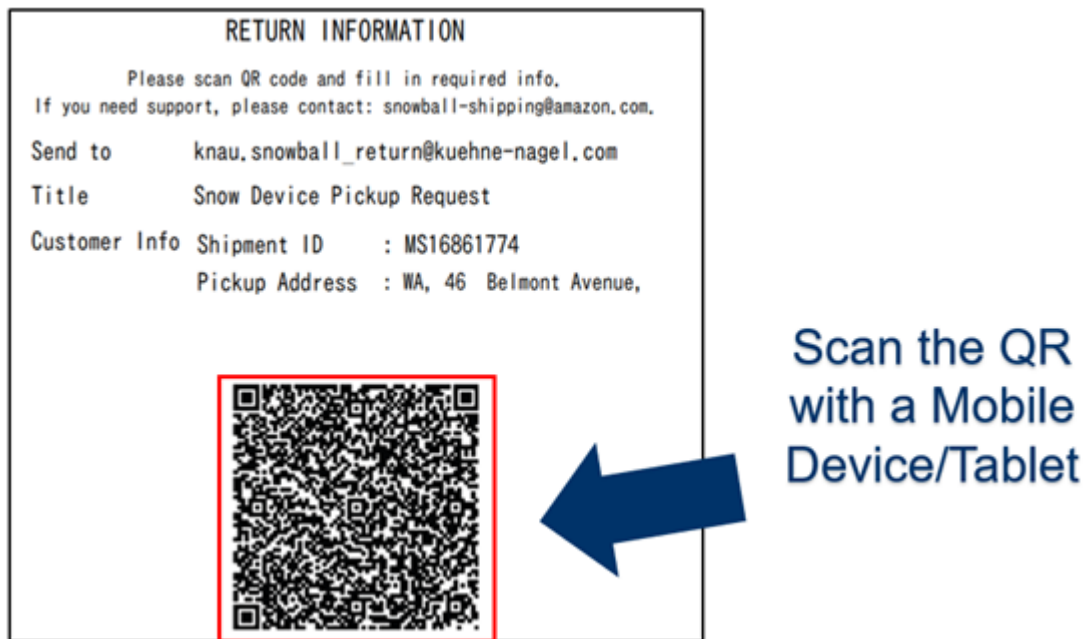
In Australia, se rispedisci un AWS Snowball Edge dispositivo a AWS, posiziona l'etichetta di trasporto per il reso (che si trova nella busta contenente queste istruzioni) sull'etichetta E Ink del dispositivo Snow.



Note

Se non hai ricevuto un'etichetta di reso con il tuo dispositivo, invia un'e-mail a knau.snowball_return@kuehne-nagel.com con il numero di serie del dispositivo o il numero di riferimento.

Per organizzare la restituzione di Snowball Edge, scansiona il codice QR riportato nelle istruzioni per la restituzione con il tuo dispositivo mobile. Sul dispositivo viene visualizzato un collegamento ipertestuale a un messaggio e-mail. Il messaggio contiene informazioni quali indirizzo e-mail, oggetto e numero di controllo o numero di spedizione. Inserisci la data di ritiro, il nome e i dettagli di contatto o fornisci un nuovo indirizzo di ritiro in caso di modifiche.



Pickup Snowball Edge in India

In India, Blue Dart rileva il dispositivo Snowball. Quando sei pronto a restituire il dispositivo Snowball, spegnilo e preparalo per la spedizione del reso. Per pianificare il ritiro, invia un'e-mail all'indirizzo snowball-pickup@amazon.com con Snowball Pickup Request nell'oggetto. Nell'e-mail, includi le seguenti informazioni:

- Job ID: l'ID del lavoro associato allo Snowball a cui desideri restituire. AWS
- Account AWS ID: l'ID dell' AWS account che ha creato il lavoro.
- Data richiesta: il giorno in cui desideri che il dispositivo Snowball venga ritirato.
- Prima ora di ritiro (ora locale): la prima ora del giorno in cui si desidera che lo Snowball venga ritirato.
- Ultimo orario di ritiro (ora locale): l'ultima ora del giorno in cui desideri che lo Snowball venga ritirato.
- Istruzioni speciali (facoltative): tutte le istruzioni speciali per il ritiro dello Snowball, compresi i dati di contatto per coordinare il ritiro.

Il team di Snowball Edge organizza il ritiro con Blue Dart e ti invia un'email di conferma. Blue Dart fornisce un'etichetta di spedizione cartacea e preleva il dispositivo Snowball Edge.

Important

- Quando usi uno Snowball in India, ricordati di presentare tutti i documenti fiscali pertinenti al tuo stato.
- AWS richiede un preavviso di almeno 72 ore per elaborare le richieste di spedizione di reso in India. AWS non può rimborsare alcuna tariffa giornaliera per le richieste di spedizione di reso ricevute con meno di 72 ore di anticipo.

Pickup Snowball Edge in Corea

In Corea, Kuehne+Nagel gestisce i ritiri. Quando desideri restituire il tuo dispositivo, invia un messaggio e-mail all'indirizzo snowball-shipping@amazon.com con Snowball Pickup Request nell'oggetto in modo da poter pianificare il ritiro. Nel corpo del messaggio e-mail, includi le seguenti informazioni:

- Job ID: l'ID del lavoro associato allo Snowball a cui desideri restituire. AWS
- Indirizzo di ritiro: l'indirizzo presso il quale viene ritirato il dispositivo.
- Data di ritiro: il primo giorno in cui desideri che il dispositivo venga ritirato.
- Dati del punto di contatto: nome, indirizzo e-mail e numero di telefono locale che Kuehne + Nagel può utilizzare per contattarti in caso di necessità.

Presto, riceverai un'e-mail di follow-up dal team di Snowball con informazioni riguardanti il ritiro del dispositivo all'indirizzo che hai fornito. Spegni e riaccendi il dispositivo e preparati per il ritiro di solito tra 1300 e 1500.

Pickup Snowball Edge a Hong Kong

A Hong Kong, S.F. Express gestisce i tuoi pickup. Quando sei pronto a restituire il dispositivo, invia un'e-mail a snowball-shipping-ap-east-1@amazon.com indicando come oggetto Snowball Pickup Request, così potremo programmare il ritiro per te. Nel corpo del messaggio e-mail, includi le seguenti informazioni:

- Job ID
- Account AWS ID
- Nome del contatto

- Numero di telefono del contatto
- Indirizzo e-mail del contatto
- Giorno desiderato per il ritiro del dispositivo
- Primo orario di ritiro
- Ultimo orario di ritiro
- Indirizzo di ritiro

Una volta pianificata una data di ritiro con S.F. Express, non è possibile riprogrammarla.

Il dispositivo verrà consegnato AWS da S.F. Express. Il numero di tracciamento S.F. Express per la spedizione di reso indica quando è stato recapitato.

Pickup Snowball Edge a Singapore, Giappone e Indonesia

A Singapore, Giappone e Indonesia, quando sei pronto a restituire il tuo dispositivo, scansiona il codice QR visualizzato sull'etichetta di reso E Ink con il tuo telefono cellulare. Verrai indirizzato direttamente a un modello di email. Compila i dati di ritiro date/time e di contatto.

RETURN

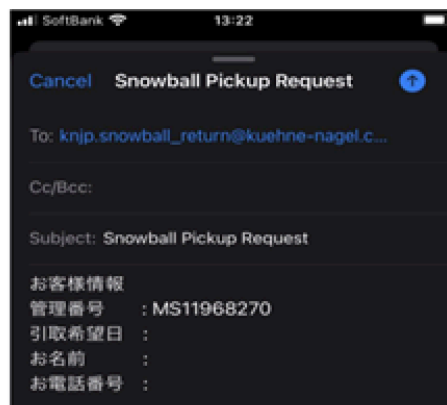
AMS Jobs ID QF6LNZGKTZPF
 シリアル番号 2R 207138750022
 管理番号 MS14003547



返送のご案内

“以下のQRコードをスキャンし情報を入力の上、メールにてご連絡をお願い致します。”

送信先アドレス knjp.snowball_return@kuehne-nagel.com
 件名 Snow Ball Pickup Request
 お客様情報
 管理番号 : MS14003547
 引取希望日 : 要記入
 お名前 : 要記入
 お電話番号 : 要記入



 Note

Se il tuo indirizzo di ritiro è diverso da quello a cui è stato consegnato il dispositivo, aggiungi il nuovo indirizzo nel corpo dell'e-mail in modo che il corriere incaricato possa essere informato.

 Note

In Giappone, la compagnia di spedizioni addebita una tassa di spedizione di 120,00 USD. La descrizione della tariffa indica Snowball Edge, ma la tariffa si applica alla spedizione di tutti gli Snowball Edge.

Snowball Edge ricevimento e restituzione a Dubai, Emirati Arabi Uniti

Ecco alcune linee guida da seguire quando si riceve o si restituisce un AWS Snowball Edge dispositivo a Dubai.

Ricezione di un dispositivo Snowball Edge

Quando ricevete un dispositivo Snowball Edge in una zona franca e ricevete una notifica da UPS che il pacco è pronto per la consegna, richiedete, ottenete e condividete il gate pass per la vostra zona franca.

Se ti trovi in una zona franca o nel continente, firma la prova di consegna (POD) quando ricevi il dispositivo.

Restituzione di un dispositivo Snowball Edge

Quando restituisci un dispositivo Snowball Edge, chiedi a UPS di ritirare il dispositivo programmando un ritiro con UPS direttamente al numero 600 544 743 o tramite il sito Web UPS. Assicurati che le informazioni sulla spedizione del reso siano visualizzate sul display E Ink prima del ritiro del dispositivo. Consultare [Restituzione del dispositivo Snowball Edge](#). In una zona franca, quando ti viene comunicato che è stato assegnato un autista UPS per il ritiro del dispositivo, richiedi, ottieni e condividi il Gate Pass per la tua zona franca.

Le informazioni di spedizione UPS prepagate sul display E Ink contengono l'indirizzo corretto per la restituzione del dispositivo Snowball Edge.

Il dispositivo Snowball Edge viene consegnato a un centro di AWS smistamento e inoltrato al data center. AWS UPS fornisce automaticamente un numero di tracciamento per il tuo lavoro.

 Important

Salvo diversa indicazione personale AWS, non apporre mai un'etichetta di spedizione separata sul dispositivo Snowball Edge. Usa sempre l'etichetta di spedizione visualizzata sul display E Ink del dispositivo.

I servizi UPS per i prodotti Snowball Edge sono nazionali solo all'interno di un Paese.

Velocità di spedizione per Snowball Edge

Ogni paese dispone di velocità di spedizione diverse. Queste velocità di spedizione dipendono dal paese in cui spedisce un AWS Snowball Edge dispositivo. Le velocità di spedizione sono riportate di seguito:

- Australia, Giappone, Singapore, Indonesia, Corea del Sud - Quando spedisce in questi paesi, hai accesso alla velocità di spedizione standard di 1-3 giorni.
- Brasile — Quando spedisce in Brasile, hai accesso alla spedizione UPS Domestic Express Saver, che consegna entro due giorni lavorativi durante l'orario commerciale. Le velocità di spedizione possono essere influenzate da ritardi dovuti a frontiere interstatali.
- Unione Europea (UE) — Quando spedisce in uno qualsiasi dei paesi dell'UE, hai accesso alla spedizione espressa. In genere, AWS Snowball Edge i dispositivi spediti con corriere espresso vengono consegnati in circa un giorno. Inoltre, la maggior parte dei paesi UE possono usufruire di una spedizione standard, che richiede meno di una settimana per la sola andata.
- Hong Kong — Quando spedisce all'interno di Hong Kong, hai accesso alla spedizione espressa.
- India: per le spedizioni in India, i dispositivi Snowball Edge vengono spediti entro 7 giorni lavorativi dalla AWS ricezione di tutti i documenti fiscali correlati.
- Dubai, Emirati Arabi Uniti - Hai accesso alla spedizione Courier Express Saver.
- Regno Unito (UK) - Quando spedisce all'interno del Regno Unito, hai accesso alla spedizione espressa. In genere, i dispositivi Snowball Edge spediti con corriere espresso vengono consegnati in circa un giorno. Inoltre, hai accesso alla spedizione standard, che in genere richiede meno di una settimana, solo andata.
- Stati Uniti d'America (USA) e Canada - Durante le spedizioni negli Stati Uniti o in Canada, puoi usufruire della spedizione di un solo giorno e della spedizione in due giorni.

Monitoraggio dello stato di importazione da Snowball Edge

Per monitorare lo stato del processo di importazione nella console, accedi al sito [Console di gestione della famiglia di servizi AWS Snow](#) in Regione AWS cui è stato creato il lavoro. Scegli il processo che desideri tracciare dalla tabella o cercalo in base ai parametri scelti nella barra di ricerca sopra la tabella. Dopo aver selezionato il lavoro, nella tabella vengono visualizzate informazioni dettagliate sul lavoro, inclusa una barra che mostra lo stato in tempo reale del lavoro.

Note

Se non siamo in grado di importare dati dal dispositivo Snow nei nostri data center a causa di un problema con le autorizzazioni di accesso che hai configurato, tenteremo di avvisarti e avrai 30 giorni di tempo dalla data di invio della notifica per risolvere il problema. Se il problema persiste, possiamo annullare il job Snowball Edge dell'utente ed eliminare i dati dal dispositivo.

Una volta che il dispositivo arriva a AWS, lo stato del processo cambia da In transit AWS a At AWS. In media, l'importazione dei dati in Amazon S3 richiede un giorno. All'avvio, lo stato del processo cambia in Importing (Importazione). L'importazione dei dati da Snowball Edge richiederà AWS all'incirca lo stesso tempo impiegato per spostarli su Snowball Edge. Dopo l'importazione dei dati, lo stato del lavoro passa allo stato Completato.

Ora il tuo primo processo di importazione dei dati in Amazon S3 con Amazon S3 AWS Snowball Edge è completo. Puoi ottenere un rapporto sul trasferimento dati dalla console. Per accedere a questo rapporto dalla console, seleziona il processo dalla tabella ed espandilo per rivelare le informazioni dettagliate del processo. Seleziona Get report (Ottieni rapporto) per scaricare il rapporto di completamento del processo come un file PDF. Per ulteriori informazioni, consulta [Ottenimento del report e dei log di completamento del processo di trasferimento dei dati](#).

Successivo: [Ottenimento del report e dei log di completamento del processo di trasferimento dei dati](#)

Ottenimento del report e dei log di completamento del processo di trasferimento dei dati

Quando usi Snowball Edge per importare o esportare dati da Amazon S3, ottieni un report di lavoro in formato PDF scaricabile. Per processi di importazione, questo rapporto diventa disponibile alla

fine del processo di importazione. Per i lavori di esportazione, il rapporto di lavoro in genere diventa disponibile mentre il AWS Snowball Edge dispositivo per il componente relativo al lavoro viene consegnato. I report sul completamento dei lavori non sono disponibili solo per i lavori di elaborazione e archiviazione locali.

Il job report fornisce informazioni sullo stato del trasferimento di dati in Amazon S3. Il rapporto include i dettagli sul processo o la parte del processo per i record. Il report sul lavoro include anche una tabella che fornisce una panoramica di alto livello del numero totale di oggetti e byte trasferiti tra il dispositivo e Amazon S3.

Per una maggiore visibilità dello stato degli oggetti trasferiti, puoi esaminare i due registri associati: un log di completamento e un log di errori. I log vengono salvati in un formato con valori separati da virgole e il nome di ogni log include l'ID del processo o la parte di processo descritto dal log.

Puoi scaricare il rapporto e i log da Console di gestione della famiglia di servizi AWS Snow. Di seguito è riportato un report di esempio.

Snow Family Job Completion Report



Region: us-gov-east-1(OSU)

Job ID: JIDd6d95004-fe1a-42d3-895d-684f357ef840

Snow Device Serial ID: 207117851234

Job type: IMPORT

Device type: Snowball Edge Storage Optimized

Storage type: S3

Job creation date: 2022-06-02 19:32:27.831 GMT

Job state: Completed

Customer address:

123 Any Street
Any Town, USA

Transfer details:

Transfer type	Total	Success	Failed
Objects	2,635	2,635	0
Bytes	32.2 TB	32.2 TB	0 B

Job state transition details:

The job was created on 2022-06-02 19:32:27.831 GMT
The snowball got allocated on 2022-06-06 19:10:43.670 GMT
The snowball was shipped on 2022-06-07 21:59:50.937 GMT
The snowball was at customer on 2022-06-08 14:04:45.856 GMT
The snowball was shipped to AWS on 2022-06-28 20:57:42.246 GMT
The snowball was at our sorting facility on 2022-06-29 14:06:20.737 GMT
The snowball was at AWS on 2022-06-30 23:12:45.017 GMT
The data transfer started on 2022-06-30 23:21:34.805 GMT
The data transfer was completed on +54473-09-10 22:23:46 GMT

Please review your job's status from the console.

For Snow job details, please see: <https://docs.aws.amazon.com/snowball/>

Per ottenere il rapporto del processo e i log

1. Accedi a Console di gestione AWS e apri il [Console di gestione della famiglia di servizi AWS Snow](#).
2. Scegli il lavoro o la parte del lavoro dalla tabella ed espandi il riquadro di stato.

Vengono visualizzate tre opzioni per ottenere il rapporto del processo e i log: Get job report (Ottieni rapporto del processo), Download success log (Scarica log di completamento) e Download failure log (Scarica log di errore).

3. Scegliere il log da scaricare.

Nell'elenco seguente vengono descritti i valori possibili per il rapporto:

- Completato: il trasferimento è stato completato con successo. Puoi trovare altre informazioni dettagliate nel log di completamento.
- Completato con errori: alcuni o tutti i dati non sono stati trasferiti. Puoi trovare altre informazioni dettagliate nel log di errore.

Migrazione di grandi quantità di dati con Snowball Edge

La migrazione di grandi quantità di dati da sedi locali richiede un'attenta pianificazione, orchestrazione ed esecuzione per garantire la corretta migrazione dei dati verso AWS.

Ti consigliamo di adottare una strategia di migrazione dei dati prima di iniziare la migrazione per evitare il rischio di mancato rispetto delle scadenze, superamento del budget e errori di migrazione. AWS I servizi Snow ti aiutano a posizionare, ordinare e tenere traccia dei tuoi progetti di migrazione di dati di grandi dimensioni tramite la funzionalità Snowball Edge Large Data Migration Manager (LDMM) di. Console di gestione della famiglia di servizi AWS Snow

Gli argomenti [Pianificazione di trasferimenti di grandi dimensioni con Snowball Edge](#) [Calibrazione di un trasferimento di grandi dimensioni con Snowball Edge](#) descrivono un processo di migrazione manuale dei dati. Puoi semplificare i passaggi manuali utilizzando il piano di migrazione LDMM Snowball Edge.

Argomenti

- [Pianificazione di trasferimenti di grandi dimensioni con Snowball Edge](#)
- [Calibrazione di un trasferimento di grandi dimensioni con Snowball Edge](#)
- [Creazione di un piano di migrazione dei dati di grandi dimensioni con Snowball Edge](#)
- [Utilizzo del piano di migrazione dei dati di grandi dimensioni con Snowball Edge](#)

Pianificazione di trasferimenti di grandi dimensioni con Snowball Edge

Ti consigliamo di pianificare e calibrare trasferimenti di dati di grandi dimensioni tra i AWS Snowball Edge dispositivi presenti in loco e i server utilizzando le linee guida riportate nelle sezioni seguenti.

Argomenti

- [Passaggio 1: scopri cosa stai trasferendo sul cloud](#)
- [Fase 2: Calcola la velocità di trasferimento desiderata](#)
- [Fase 3: Stabilisci quanti Snowball Edge ti servono](#)
- [Fase 4: Crea le tue offerte di lavoro](#)
- [Passaggio 5: Separa i dati in segmenti di trasferimento](#)

Passaggio 1: scopri cosa stai trasferendo sul cloud

Prima di creare il primo lavoro utilizzando il Console di gestione della famiglia di servizi AWS Snow, assicurati di valutare il volume di dati che devi trasferire, dove sono attualmente archiviati e la destinazione verso cui desideri trasferirli. Per i trasferimenti di dati di dimensioni pari o superiori a un petabyte, questa gestione amministrativa semplifica notevolmente l'arrivo di Snowball Edge.

Se stai migrando i dati in the Cloud AWS per la prima volta, ti consigliamo di progettare un modello di migrazione al cloud. La migrazione al cloud non avviene dall'oggi al domani. Richiede un attento processo di pianificazione per garantire che tutti i sistemi funzionino come previsto.

Al termine di questa fase, conoscerai la quantità totale di dati che vengono spostati nel cloud.

Fase 2: Calcola la velocità di trasferimento desiderata

È importante stimare la velocità con cui è possibile trasferire i dati allo Snowball Edge collegato a ciascuno dei server. Questa velocità stimata in MB/sec determina la velocità con cui è possibile trasferire i dati dalla sorgente dati ai dispositivi Snowball Edge utilizzando l'infrastruttura di rete locale.

Note

Per trasferimenti di dati di grandi dimensioni, consigliamo di utilizzare il metodo di trasferimento dati Amazon S3. È necessario selezionare questa opzione quando si ordinano dispositivi in. Console di gestione della famiglia di servizi AWS Snow

Per determinare una velocità di trasferimento di base, trasferisci un piccolo sottoinsieme di dati sul dispositivo Snowball Edge oppure trasferisci un file di esempio da 10 GB e osserva la velocità effettiva.

Nel determinare la velocità di trasferimento desiderata, tenete presente che potete migliorare la velocità di trasmissione ottimizzando l'ambiente, inclusa la configurazione di rete, modificando la velocità di rete, la dimensione dei file trasferiti e la velocità di lettura dei dati dai server locali. L'adattatore Amazon S3 copia i dati su Snowball Edge non appena le condizioni lo consentono.

Fase 3: Stabilisci quanti Snowball Edge ti servono

Utilizzando la quantità totale di dati che intendi trasferire nel cloud, la velocità di trasferimento stimata e il numero di giorni in cui desideri consentire lo spostamento dei dati AWS, determina la quantità di Snowball Edge necessaria per la migrazione dei dati su larga scala. A seconda del

tipo di dispositivo, i dispositivi Snowball Edge dispongono di circa 39,5 TB o 210 TB di spazio di archiviazione utilizzabile. Ad esempio, se desideri trasferire 300 TB di dati in AWS più di 10 giorni e hai una velocità di trasferimento di 250 MB/s, hai bisogno di 2 dispositivi Snowball Edge con 210 TB di spazio di archiviazione.

Note

Snowball Edge LDMM fornisce una procedura guidata per stimare il numero di Snowball Edge che possono essere supportati contemporaneamente. Per ulteriori informazioni, consulta [Creazione di un piano di migrazione dei dati di grandi dimensioni con Snowball Edge](#).

Fase 4: Crea le tue offerte di lavoro

Dopo aver stabilito la quantità di Snowball Edge necessaria, è necessario creare un processo di importazione per ogni dispositivo. La creazione di più lavori è semplificata dallo Snowball Edge LDMM. Per ulteriori informazioni, consulta [Effettuare il tuo prossimo ordine di lavoro](#).

Note

Puoi effettuare il tuo prossimo ordine di lavoro e aggiungerlo automaticamente al tuo piano direttamente dalla pianificazione degli ordini di lavoro consigliata. Per ulteriori informazioni, consulta [Pianificazione degli ordini di lavoro consigliata](#).

Passaggio 5: Separa i dati in segmenti di trasferimento

Come best practice per trasferimenti di dati di grandi dimensioni che coinvolgono più processi, consigliamo di suddividere logicamente i dati in una serie di set di dati più piccoli e più gestibili. Ciò consente di trasferire ogni partizione alla volta o più partizioni in parallelo. Quando pianifichi le partizioni, assicurati che i dati delle partizioni combinate corrispondano a Snowball Edge per il lavoro. Ad esempio, puoi separare il trasferimento in partizioni in uno dei seguenti modi:

- Puoi creare 10 partizioni da 20 TB ciascuna da utilizzare con un dispositivo Snowball Edge con 210 TB di spazio di archiviazione, ad esempio.
- Per file di grandi dimensioni, ogni file può essere una singola partizione fino al limite di dimensione di 5 TB per gli oggetti in Amazon S3.

- Ogni partizione può avere dimensioni diverse e ogni singola partizione può essere composta dallo stesso tipo di dati, ad esempio file di piccole dimensioni in una partizione, archivi compressi in un'altra, file di grandi dimensioni in un'altra partizione e così via. Questo approccio può aiutarvi a determinare la velocità di trasferimento media per diversi tipi di file.

Note

Le operazioni sui metadati vengono eseguite per ogni file trasferito. Indipendentemente dalle dimensioni di un file, questo overhead rimane invariato. Pertanto, è possibile ottenere prestazioni più elevate comprimendo file di piccole dimensioni in un pacchetto più grande, raggruppando i file in batch o trasferendo singoli file più grandi.

La creazione di segmenti per il trasferimento dei dati può semplificare la risoluzione rapida dei problemi di trasferimento, poiché cercare di risolvere un trasferimento di grandi dimensioni ed eterogeneo dopo un giorno o più può essere complesso.

Quando hai finito di pianificare il trasferimento di dati su scala petabyte, ti consigliamo di trasferire alcuni segmenti sul dispositivo Snowball Edge dal server per calibrare la velocità e il tempo di trasferimento totale.

Calibrazione di un trasferimento di grandi dimensioni con Snowball Edge

È possibile calibrare le prestazioni di trasferimento trasferendo un set rappresentativo di partizioni di dati. Scegliete più partizioni che avete definito e trasferitele su un dispositivo Snowball Edge. Registra la velocità di trasferimento e il tempo totale di trasferimento per ogni operazione. Se i risultati della calibrazione sono inferiori alla velocità di trasferimento target, potresti riuscire a copiare più parti del trasferimento di dati contemporaneamente. In questo caso, ripeti la calibrazione con le partizioni aggiuntive del set di dati.

Continuate ad aggiungere operazioni di copia parallela durante la calibrazione finché non vedrete rendimenti decrescenti nella somma della velocità di trasferimento di tutte le istanze che attualmente trasferiscono dati. Termina l'ultima istanza attiva e prendi nota della nuova velocità di trasferimento target.

È possibile trasferire i dati più velocemente su Snowball Edge trasferendoli in parallelo utilizzando uno dei seguenti scenari:

- Utilizzo di più sessioni dell'adattatore S3 su una workstation contro un singolo dispositivo Snowball Edge.
- Utilizzo di più sessioni dell'adattatore S3 su più workstation su un singolo dispositivo Snowball Edge.
- Utilizzo di più sessioni dell'interfaccia S3 (utilizzando una o più workstation) destinate a più Snowball Edge.

Una volta completati questi passaggi, dovresti sapere quanto velocemente puoi trasferire i dati su un dispositivo Snowball Edge.

Creazione di un piano di migrazione dei dati di grandi dimensioni con Snowball Edge

La funzionalità del piano di migrazione dei dati di grandi dimensioni di Snowball Edge consente di pianificare, tracciare, monitorare e gestire migrazioni di dati di grandi dimensioni da 500 TB a più petabyte utilizzando più prodotti di servizio Snowball Edge.

Utilizza la funzionalità del piano di migrazione dei dati di grandi dimensioni per raccogliere informazioni sugli obiettivi di migrazione dei dati, come la dimensione dei dati verso cui passare AWS e il numero di Snowball Edge necessari per migrare i dati contemporaneamente. Utilizza il piano per creare una pianificazione prevista per il tuo progetto di migrazione dei dati e la pianificazione degli ordini di lavoro consigliata per raggiungere i tuoi obiettivi.

Note

Attualmente, il piano di migrazione dei dati è disponibile per i lavori di importazione superiori a 500 TB.

Argomenti

- [Passaggio 1: scegli i dettagli della migrazione](#)
- [Passaggio 2: scegli le tue preferenze di spedizione, sicurezza e notifica](#)

- [Fase 3: Rivedi e crea il tuo piano](#)

Passaggio 1: scegli i dettagli della migrazione

Note

È disponibile un ampio piano di migrazione dei dati per migrazioni di dati superiori a 500 TB. Crea ordini di lavoro singolarmente su Snowball Edge per i tuoi progetti di trasferimento dati di dimensioni inferiori a 500 TB. Per ulteriori informazioni, consulta [Creare un lavoro per ordinare un dispositivo Snowball Edge](#) in questa guida.

1. Accedi alla [Console di gestione della famiglia di servizi AWS Snow](#). Se è la prima volta che usi Console di gestione della famiglia di servizi AWS Snow in this Regione AWS, viene visualizzata la pagina Snowball Edge. Altrimenti, viene visualizzato l'elenco dei lavori esistenti.
2. Se questo è il tuo primo piano di migrazione dei dati, scegli Crea un piano di migrazione dei dati di grandi dimensioni dalla pagina principale. Altrimenti, scegli un piano di migrazione dei dati di grandi dimensioni. Scegli Crea piano di migrazione dei dati per aprire la procedura guidata di creazione del piano.
3. In Assegna un nome al tuo piano di migrazione dei dati, fornisci un nome per il piano di migrazione dei dati. Il nome del piano può contenere fino a 64 caratteri. I caratteri validi sono A-Z, a-z, 0-9 e - (trattino). Il nome di un piano non deve iniziare con. **aws** :
4. Per i dati totali verso cui migrare AWS, inserisci la quantità di dati verso cui desideri migrare. AWS
5. Nei dispositivi Snow, scegli un dispositivo Snowball Edge.

Note

Le opzioni dei dispositivi supportati possono variare in base alla disponibilità di alcuni Regioni AWS dispositivi.

6. Per i dispositivi Concurrent, inserisci il numero di Snowball Edge su cui puoi copiare contemporaneamente i dati nella tua posizione. Se non sei sicuro, vai alla sezione successiva per informazioni sull'utilizzo della procedura guidata di stima dei dispositivi concorrenti per determinarlo.
7. Scegli Next (Successivo).

Utilizzo della procedura guidata di stima dei dispositivi concorrenti

La procedura guidata di stima dei dispositivi simultanei consente di determinare il numero di dispositivi simultanei che è possibile utilizzare durante migrazioni di dati di grandi dimensioni.

Prerequisiti:

- Hai eseguito una prova di fattibilità per testare la metodologia di trasferimento dei dati e misurato le prestazioni con un dispositivo Snowball Edge nel tuo ambiente.
- Conosci la rete e la connessione allo storage back-end.

Passaggio 1: Immettere le informazioni sulla fonte dei dati

Innanzitutto, determina la velocità teorica massima per la copia dei dati dalla fonte di archiviazione.

1. Per i dati totali da migrare, inserisci la quantità di dati che intendi migrare.

Per Unità, scegli l'unità di misura (GB o TB) per la quantità di dati che intendi migrare.

2. Per Numero di interfacce di rete attive, inserisci il numero di interfacce di rete attive disponibili per la migrazione dei dati dalla fonte di archiviazione.

Number of active network interfaces [Info](#)
The number of network interfaces that can be used for migrations

Number of active network interfaces used for data migration

3. Per Velocità dell'interfaccia di rete, scegli la velocità dell'interfaccia di rete per la fonte di archiviazione. Le velocità di rete sono espresse in Gb/s.

Network interface speed [Info](#)
The speed of the network interfaces used for migrations

Network interface speed (Gb/s)

4. In Throughput di rete massimo, immettete il throughput di rete massimo testato per la sorgente di archiviazione determinato durante la dimostrazione del concetto. La velocità effettiva è espressa in MB/S.

Maximum network throughput [Info](#)
The maximum sustainable throughput for the data source

Maximum tested throughput of data source (MB/s)

5. Per l'utilizzo della rete di storage back-end, indica se la sorgente di archiviazione condivide una rete con lo storage back-end.
- Scegli Sì se la rete non è condivisa. Non è necessario inserire la velocità dell'interconnessione di archiviazione per un singolo flusso.
 - Scegli No se la rete è condivisa. Immettete la velocità dell'interconnessione di archiviazione per un singolo flusso in MB/s.

In base alla scelta, la procedura guidata aggiorna il valore della velocità effettiva di migrazione massima per l'origine dati (MB/s) nella parte inferiore della pagina.

Storage backend network usage [Info](#)

Network shared with storage backend traffic?
Is the network used for migration being shared with your storage backend?

Yes ▼

Speed of storage interconnection for single stream (MB/s)
This is a single connection throughput that can be sustained from source to destination

6. Scegli Next (Successivo).

Fase 2: Inserimento dei parametri della workstation di migrazione

Puoi connettere Snowball Edge direttamente alla tua fonte di archiviazione (ad esempio un server Microsoft Windows). Puoi invece scegliere di connettere Snowball Edge a una o più workstation per copiare i dati dalla fonte di archiviazione.

1. Per l'utilizzo della workstation di migrazione, indica la scelta di utilizzo della workstation.
 - Scegli Nessuno: utilizza direttamente l'origine dati per trasferire i dati direttamente da un'origine dati senza utilizzare una workstation, quindi scegli Avanti.
 - Scegli Altro - Usa una o più postazioni di copia per utilizzare una o più workstation per il trasferimento dei dati.

Migration workstation usage [Info](#)

Type of migration source used

Other - Use copy workstation(s) ▼

2. Per Numero di interfacce di rete attive, inserisci il numero di porte da utilizzare per la migrazione dei dati.

Number of active network interfaces [Info](#)

The number of network interfaces that can be used for migrations

Number of active network interfaces on the migration workstation

1

3. Per Velocità dell'interfaccia di rete, scegli la velocità in Gb/s delle interfacce di rete.

Network interface speed [Info](#)

Your workstations Network card speeds

Network interface speed (Gb/s)

10 ▼

4. In Utilizzo della rete di back-end di archiviazione, indica se la rete su cui si trovano le workstation è condivisa con lo storage back-end.
 - Scegli Sì se è condiviso.
 - Scegli No se non è condiviso. Inserisci la velocità dell'interconnessione di archiviazione per un singolo flusso in MB/s.

Storage backend network usage [Info](#)

Network shared with storage backend traffic?
Is the network used for migration being shared with your storage backend?

Yes ▼

Speed of storage interconnection for single stream (MB/s)
This is a single connection throughput that can be sustained from source to destination

In base ai dati forniti, la procedura guidata visualizza un suggerimento in Numero di workstation di migrazione. È possibile modificare manualmente il numero se non si è d'accordo con il consiglio. Questo numero verrà visualizzato in Dispositivi concorrenti nel piano di migrazione dei dati di grandi dimensioni.

Number of migration workstations [Info](#)

Recommended number of migration workstations used

0

Fase 3: Inserimento della velocità di trasferimento media di Snowball Edge

1. Nel campo Velocità di trasferimento media del dispositivo Snow, inserisci la velocità di trasferimento in MB/s che hai visto durante il proof of concept.

Average Snow device transfer throughput [Info](#)

This is the throughput from your migration workstation to the Snow device you saw during the proof of concept

Average Snow device transfer throughput (MB/s)

In base al throughput medio, la procedura guidata aggiorna il numero consigliato di dispositivi Snow simultanei e il numero massimo di dispositivi simultanei nei dettagli del piano di migrazione.

2. Scegli Usa questo numero per continuare e tornare a scegliere i dettagli della migrazione. Scegli Avanti e vai al passaggio successivo ([Passaggio 2: scegli le tue preferenze di spedizione, sicurezza e notifica](#)).

Note

Puoi utilizzare fino a 5 dispositivi Snow simultanei.

Passaggio 2: scegli le tue preferenze di spedizione, sicurezza e notifica

1. Nella sezione Indirizzo di spedizione, scegli un indirizzo esistente o creane uno nuovo.

Note

Il paese indicato nell'indirizzo deve corrispondere al paese di destinazione del dispositivo e deve essere valido per quel paese.

2. In Scegli il tipo di accesso al servizio, esegui una delle seguenti operazioni:
 - Consenti a Snowball Edge di creare per te un nuovo ruolo collegato ai servizi con tutte le autorizzazioni necessarie per pubblicare metriche CloudWatch e notifiche Amazon SNS per i tuoi job Snowball Edge.
 - Aggiungi un ruolo di servizio esistente con le autorizzazioni necessarie. Per un esempio di come impostare questo ruolo, vedi [Esempio 4: Autorizzazioni previste per i ruoli e politica di attendibilità](#).

3. Per Invia notifiche, scegli se inviare notifiche. Tieni presente che se scegli Non inviare notifiche sui piani di migrazione dei dati, non riceverai notifiche da questo piano, ma riceverai comunque notifiche di lavoro.
4. Per Imposta notifiche,
 - scegli Usa un argomento SNS esistente
 - o Crea un nuovo argomento SNS.

Fase 3: Rivedi e crea il tuo piano

1. Controlla le tue informazioni in Dettagli del piano e Preferenze di spedizione, sicurezza e notifica e modificalle se necessario.
2. Scegli Crea piano di migrazione dei dati per creare il piano.

Utilizzo del piano di migrazione dei dati di grandi dimensioni con Snowball Edge

Dopo aver creato il piano di migrazione dei dati di grandi dimensioni, puoi utilizzare la pianificazione e la dashboard risultanti per guidarti nel resto del processo di migrazione.

Pianificazione degli ordini di lavoro consigliata

Dopo aver creato un piano di migrazione di grandi dimensioni per Snowball Edge, puoi utilizzare la pianificazione degli ordini di lavoro consigliata per creare nuovi lavori.

Note

Gli aggiornamenti manuali apportati alla dimensione dei dati o al numero di dispositivi simultanei modificano la pianificazione. La pianificazione viene modificata automaticamente se un lavoro non è stato ordinato entro la data dell'ordine consigliata o è stato ordinato prima della data dell'ordine consigliata. Se un lavoro viene restituito prima della data dell'ordine consigliata, la pianificazione viene modificata automaticamente.

Recommended job ordering scheduleJobs ordered

Recommended job ordering schedule

This list provides an estimated schedule to place Snow jobs in order to achieve your data migration goals. The estimated ordering schedule is automatically adjusted based on your data migration speed.

Filter by a date and time range

Hide Ordered

<1>

	Recommended date to order	Number of devices to order	Number of ordered devices	Device type	Status
☐	Thu Mar 23 2023	2	-	Snowball Edge Storage Optimized with 210TB	Not Ordered
☐	Fri Mar 31 2023	2	-	Snowball Edge Storage Optimized with 210TB	Not Ordered
☐	Sat Apr 08 2023	2	-	Snowball Edge Storage Optimized with 210TB	Not Ordered
☐	Sun Apr 16 2023	2	-	Snowball Edge Storage Optimized with 80TB	Not Ordered
☐	Mon Apr 24 2023	2	-	Snowball Edge Storage Optimized with 80TB	Not Ordered
☐	Tue May 02 2023	2	-	Snowball Edge Storage Optimized with 80TB	Not Ordered
☐	Wed May 10 2023	2	-	Snowball Edge Storage Optimized with 80TB	Not Ordered
☐	Thu May 18 2023	2	-	Snowball Edge Storage Optimized with 80TB	Not Ordered
☐	Fri May 26 2023	1	-	Snowball Edge Storage Optimized with 80TB	Not Ordered
☐	Fri May 26 2023	1	-	Snowcone SSD	Not Ordered

Effettuare il tuo prossimo ordine di lavoro

Per effettuare il prossimo ordine, invece di creare manualmente un lavoro e poi aggiungerlo al piano, hai la possibilità di clonare un lavoro ordinato in precedenza o crearne uno precompilato.

Per clonare un lavoro:

1. Scegli l'ordine successivo (il primo consiglio con lo stato Non ordinato) dalla pianificazione degli ordini di lavoro consigliati, quindi scegli Clone Job dal menu Azioni. Viene visualizzata la finestra Clone Job.
2. Nella finestra Clone Job, nella sezione Job ordinati, scegli il lavoro da clonare.
3. Nella sezione Dettagli sui nuovi lavori, scegli i dispositivi che desideri ordinare. Per ogni dispositivo scelto, il nome del Job verrà compilato automaticamente in base al lavoro scelto. È possibile sovrascrivere il nome del lavoro.
4. Scegli Conferma per effettuare l'ordine di lavoro per i dispositivi scelti. Il sistema clona il lavoro per ogni dispositivo.

Per creare nuovi posti di lavoro:

1. Scegli l'ordine successivo (il primo consiglio con lo stato Non ordinato) dalla pianificazione degli ordini di lavoro consigliati, quindi scegli Crea nuovi lavori dal menu Azioni. Viene visualizzata la finestra Crea nuovi lavori.

Recommended job ordering schedule					
Jobs ordered					
Recommended job ordering schedule					
This list provides an estimated schedule to place Snow jobs in order to achieve your data migration goals. The estimated ordering schedule is automatically adjusted based on your data migration speed.					
Filter by a date and time range 🔄 ☒ Hide Ordered					
Recommended date to order	Number of devices to order	Number of ordered devices	Device type	Status	
☒ Thu Mar 23 2023	2	-	Snowball Edge Storage Optimized with 210TB	⊗ Not Ordered	
☐ Fri Mar 31 2023	2	-	Snowball Edge Storage Optimized with 210TB	⊗ Not Ordered	
☐ Sat Apr 08 2023	2	-	Snowball Edge Storage Optimized with 210TB	⊗ Not Ordered	
☐ Sun Apr 16 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Mon Apr 24 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Tue May 02 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Wed May 10 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Thu May 18 2023	2	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Fri May 26 2023	1	-	Snowball Edge Storage Optimized with 80TB	⊗ Not Ordered	
☐ Fri May 26 2023	1	-	Snowcone SSD	⊗ Not Ordered	

- Nella sezione Selezione del dispositivo, scegli i dispositivi che desideri ordinare. Scegli Continua.

Create New Jobs

Device Selection (2/2)

Select which devices you would like to order

☒ Device type

☒ Snowball Edge Storage Optimized with 210TB
 ☒ Snowball Edge Storage Optimized with 210TB

- Viene visualizzata la pagina Crea nuovo. La maggior parte dei parametri, come il tipo di lavoro, l'indirizzo di spedizione e il tipo di dispositivo, sono impostati in base al piano. Il sistema crea il lavoro per ogni dispositivo.

Puoi vedere se il lavoro o i lavori sono stati creati correttamente o meno. I lavori creati con successo vengono aggiunti automaticamente al piano.

Elenco dei lavori ordinati

Ogni piano mostra un elenco di lavori ordinati. All'inizio è vuoto. Quando inizi a ordinare lavori, puoi aggiungere lavori al tuo piano selezionando **Aggiungi lavoro** dal menu **Azioni**. I lavori che aggiungi qui vengono tracciati nella dashboard di monitoraggio.

Allo stesso modo, puoi rimuovere il lavoro dall'elenco dei lavori ordinati selezionando **Rimuovi lavoro** dal menu **Azioni**.

Ti consigliamo di utilizzare la pianificazione degli ordini di lavoro fornita nel piano per una migrazione dei dati senza problemi.

Dashboard di monitoraggio

Dopo aver aggiunto i lavori al tuo piano, puoi visualizzare le metriche sulla dashboard man mano che i lavori tornano a essere AWS inseriti. Queste metriche possono aiutarti a tenere traccia dei tuoi progressi:

- **Dati migrati a AWS:** la quantità di dati verso cui è stata effettuata la migrazione finora.. AWS
- **Dati migrati in media per processo:** la quantità media di dati per processo, espressa in terabyte.
- **Totale lavori sulla neve:** il numero di lavori Snowball Edge ordinati rispetto ai lavori rimanenti da ordinare.
- **Durata media di un processo di migrazione:** la durata media di un lavoro in giorni.
- **Snow Job Status:** il numero di lavori in ogni stato.

Utilizzo AWS OpsHub per gestire i dispositivi

Snowball Edge ora offre uno strumento intuitivo che puoi utilizzare per gestire i tuoi dispositivi e i servizi locali. AWS OpsHub AWS Si utilizza AWS OpsHub su un computer client per eseguire attività come lo sblocco e la configurazione di dispositivi singoli o in cluster, il trasferimento di file e l'avvio e la gestione di istanze in esecuzione su Snowball Edge. Puoi utilizzarlo AWS OpsHub per gestire i tipi di dispositivi Storage Optimized e Compute Optimized Snow. L' AWS OpsHub applicazione è disponibile senza costi aggiuntivi per l'utente.

AWS OpsHub prende tutte le operazioni esistenti disponibili nell'API Snowball e le presenta come interfaccia utente grafica. Questa interfaccia consente di migrare rapidamente i dati verso Cloud AWS e distribuire applicazioni di edge computing su Snowball Edge.

AWS OpsHub fornisce una visione unificata dei AWS servizi in esecuzione su Snowball Edge e automatizza le attività operative tramite. AWS Systems Manager Inoltre AWS OpsHub, gli utenti con diversi livelli di esperienza tecnica possono gestire un gran numero di Snowball Edge. Con pochi clic, puoi sbloccare dispositivi, trasferire file, gestire istanze EC2 compatibili con Amazon e monitorare i parametri dei dispositivi.

Quando il dispositivo Snow arriva al tuo sito, scarica, installa e avvia l'applicazione AWS OpsHub su un computer client, ad esempio un laptop. Dopo l'installazione, puoi sbloccare il dispositivo e iniziare a gestirlo e utilizzare i servizi supportati localmente. AWS AWS OpsHub fornisce una dashboard che riassume le metriche chiave come la capacità di archiviazione e le istanze attive sul dispositivo. Fornisce inoltre una selezione di AWS servizi supportati da Snowball Edge. In pochi minuti, è possibile iniziare a trasferire i file sul dispositivo.

Argomenti

- [Download AWS OpsHub per Snowball Edge](#)
- [Sblocco di un dispositivo Snowball Edge con AWS OpsHub](#)
- [Verifica della firma PGP di AWS OpsHub \(opzionale\)](#)
- [Gestione dei AWS servizi su Snowball Edge con AWS OpsHub](#)
- [Riavvio del dispositivo con AWS OpsHub](#)
- [Gestione dei profili con AWS OpsHub](#)
- [Spegnimento del dispositivo con AWS OpsHub](#)
- [Modifica dell'alias del dispositivo con AWS OpsHub](#)
- [Gestione dei certificati a chiave pubblica tramite OpsHub](#)

- [Ricevere aggiornamenti per Snowball Edge](#)
- [Aggiornamento dell' AWS OpsHub applicazione](#)
- [Automatizzazione delle attività di gestione con AWS OpsHub](#)
- [Impostazione dei time server NTP per il dispositivo con AWS OpsHub](#)

Download AWS OpsHub per Snowball Edge

Da scaricare AWS OpsHub

1. Vai al sito Web dedicato alle [risorse di AWS Snowball](#).

The screenshot shows the AWS OpsHub website interface. On the left is a sidebar with navigation links: 'What's New', 'OpsHub' (highlighted), 'Snowball Edge Client', 'Featured Content', 'Documentation', 'Webinars', 'Videos', 'Blog Posts', and 'Free Training'. The main content area is titled 'OpsHub' and contains a description: 'OpsHub is a graphical user interface you can use to manage Snowball devices. OpsHub makes it easy to setup and manage Snowball devices enabling you to rapidly deploy edge computing workloads and simplify data migration to the cloud. With just a few clicks in OpsHub, you have the full functionality of the Snow Family of devices at your fingertips; you can unlock and configure devices, drag-and-drop data to devices, launch applications, and monitor device metrics.' Below this is a link to 'OpsHub documentation'. At the bottom, there is a table with download links for different operating systems:

	OpsHub
Windows 7 or higher	Download
Mac OS X 10.10 or higher	Download
Linux (Ubuntu version 14 or higher, and Fedora version 24 or higher)	Download
	(Signature)

2. Nella AWS OpsHub sezione, scegli Scarica per il tuo sistema operativo e segui i passaggi di installazione.

Sblocco di un dispositivo Snowball Edge con AWS OpsHub

Quando il dispositivo arriva sul sito, il primo passo è connetterlo e sbloccarlo. AWS OpsHub consente di accedere, sbloccare e gestire i dispositivi utilizzando i seguenti metodi:

- Localmente: per accedere a un dispositivo localmente, è necessario accendere il dispositivo e collegarlo alla rete locale. Fornisci quindi un codice di sblocco e un file manifesto.

- Da remoto: per accedere a un dispositivo in remoto, è necessario accendere il dispositivo e assicurarsi che possa connettersi *device-order-region*.amazonaws.com tramite la rete. Fornisci quindi le credenziali AWS Identity and Access Management (IAM) (chiave di accesso e chiave segreta) per Account AWS il dispositivo collegato al dispositivo.

Per informazioni sull'attivazione della gestione remota e sulla creazione di un account associato, consulta [Attivazione della gestione dei dispositivi Snowball Edge su Snowball Edge](#).

Argomenti

- [Sblocco locale di un dispositivo Snowball Edge con AWS OpsHub](#)
- [Sblocco remoto di un dispositivo Snowball Edge con AWS OpsHub](#)

Sblocco locale di un dispositivo Snowball Edge con AWS OpsHub

Per connettere e sbloccare il dispositivo localmente

1. Apri lo sportello del dispositivo, individua il cavo di alimentazione e collegalo a una fonte di alimentazione.
2. Connect il dispositivo alla rete utilizzando un cavo di rete (in genere un RJ45 cavo Ethernet), quindi apri il pannello anteriore e accendete il dispositivo.
3. Apri l' AWS OpsHub applicazione. Se sei un utente alle prime armi, ti viene richiesto di scegliere una lingua. Quindi scegli Successivo.
4. Nella OpsHub pagina Guida introduttiva, scegli Accedi ai dispositivi locali, quindi scegli Accedi.



Get started with OpsHub

☒ Sign into local devices
You'll need an unlock code and
manifest file

☐ Sign into remote devices
You'll need an access key & secret
key

Sign in

5. Nella pagina Accedi ai dispositivi locali, scegli il tipo di Snowball Edge, quindi scegli Accedi.
6. Nella pagina di accesso, inserisci l'indirizzo IP del dispositivo e il codice di sblocco. Per selezionare il manifesto del dispositivo, scegli Scegli file, quindi scegli Accedi.



Sign into your Snowball Edge

Sign in with an unlock code and manifest file

Device IP address

Eg 12.34.45.678

Unlock code

7c0e1-bab84-f7675-0a2b6-bfcc3

Manifest file

 Choose file

No file chosen

Back

Sign in

7. (Facoltativo) Salva le credenziali del dispositivo come profilo. Assegna un nome al profilo e scegli Salva nome profilo. Per ulteriori informazioni sui profili, consulta [Gestione dei profili con AWS OpsHub](#).
8. Nella scheda Dispositivi locali, scegli un dispositivo per visualizzarne i dettagli, come le interfacce di rete e AWS i servizi in esecuzione sul dispositivo. Puoi anche visualizzare i dettagli dei cluster da questa scheda o gestire i tuoi dispositivi proprio come fai con AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consulta [Gestione dei AWS servizi su Snowball Edge con AWS OpsHub](#).

Per i dispositivi AWS Snowball Edge Device Management installati, puoi scegliere Abilita gestione remota per attivare la funzionalità. Per ulteriori informazioni, consulta [Utilizzo AWS Snowball Edge Device Management per gestire Snowball Edge](#).

Sblocco remoto di un dispositivo Snowball Edge con AWS OpsHub

Non sbloccare uno Snowball Edge

Per connettere e sbloccare il dispositivo da remoto

1. Apri lo sportello del dispositivo, individua il cavo di alimentazione e collegalo a una fonte di alimentazione.
2. Connect il dispositivo alla rete utilizzando un cavo Ethernet (in genere un RJ45 cavo), quindi apri il pannello anteriore e accendete il dispositivo.

Note

Per essere sbloccato da remoto, il dispositivo deve essere in grado di connettersi a *device-order-region*.amazonaws.com

3. Apri l'applicazione. AWS OpsHub Se sei un utente alle prime armi, ti viene richiesto di scegliere una lingua. Quindi scegli Successivo.
4. Nella OpsHub pagina Guida introduttiva, scegli Accedi ai dispositivi remoti, quindi scegli Accedi.



Get started with OpsHub

☐ Sign into local
devices
You'll need an unlock
code and manifest file

☒ Sign into remote
devices
You'll need an access key
& secret key

Sign in

5. Nella pagina Accedi ai dispositivi remoti, inserisci le credenziali AWS Identity and Access Management (IAM) (chiave di accesso e chiave segreta) per il Account AWS dispositivo collegato al tuo dispositivo, quindi scegli Accedi.



Sign into remote devices

Sign in with an access key and secret key

Access key

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

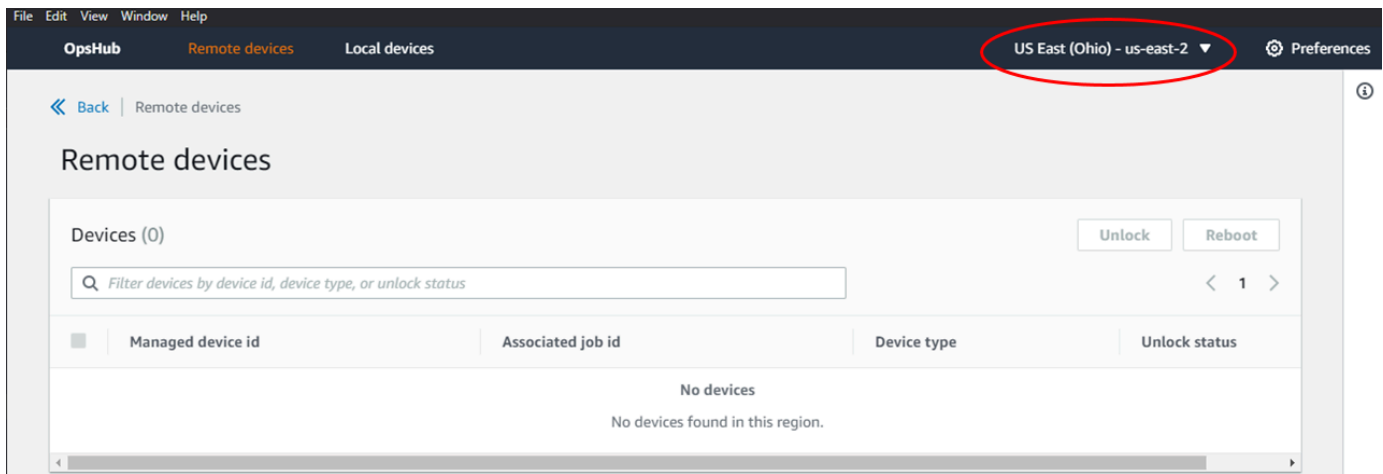
Secret key

.....

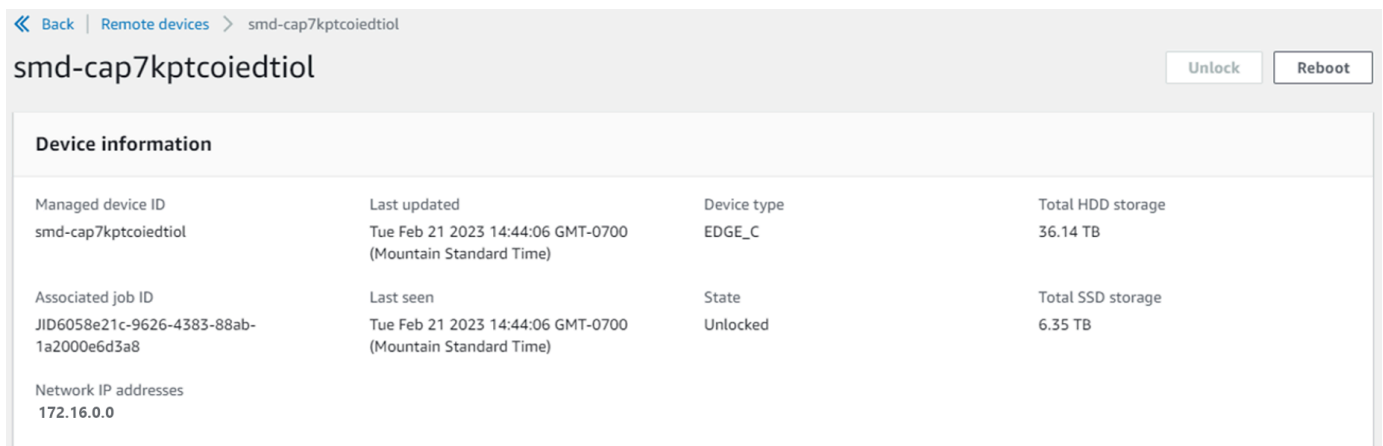
Back

Sign in

6. Nella parte superiore della scheda Dispositivi remoti, scegli la regione del dispositivo Snow da sbloccare da remoto.



7. Nella scheda Dispositivi remoti, scegli il dispositivo per visualizzarne i dettagli, come lo stato e le interfacce di rete. Quindi scegli Sblocca per sbloccare il dispositivo.



Dalla pagina dei dettagli del dispositivo remoto, puoi anche riavviare i dispositivi e gestirli proprio come fai con AWS Command Line Interface (AWS CLI). Per visualizzare i dispositivi remoti in diversi modi Regioni AWS, scegli la regione corrente sulla barra di navigazione, quindi scegli la regione che desideri visualizzare. Per ulteriori informazioni, consulta [Gestione dei AWS servizi su Snowball Edge con AWS OpsHub](#).

Verifica della firma PGP di AWS OpsHub (opzionale)

Il pacchetto di installazione AWS OpsHub dell'applicazione per il sistema operativo Linux è firmato crittograficamente. È possibile utilizzare una chiave pubblica per verificare che il pacchetto di installazione sia originale e non modificato. Se i file sono danneggiati o alterati, la verifica fallisce. È possibile verificare la firma del pacchetto di installazione utilizzando GNU Privacy Guard (GPG).

Questa verifica è facoltativa. Se scegli di verificare la firma della domanda, puoi farlo in qualsiasi momento.

È possibile scaricare il file SIGNATURE per il programma di installazione del sistema operativo Linux da [AWS Snowball Edge Resources](#) o [Snowball](#) Edge Resources.

Per verificare il pacchetto di AWS OpsHub installazione per il sistema operativo Linux

1. Copia la seguente chiave pubblica, salvala in un file e assegna un nome al file. Ad esempio, `opshub-public-key.pgp`.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
xsFNBF/hGf8BEAC9HCDV8uljDX02Jxspi6kmPu4xqf4ZZLQsSqJcHU61oL/c
/zAN+mUqJT9aJ1rr0QFGVD1bMogecUPf1TWlDkEEpG8ZbX5P8vR+EE10/rW/
WtqizSudy6qy59ZRK+YVSDx7DZyuJmI07j00UADCL+95ZQN9vqwHNjBHsgfQ
l/1Tqhy81ozTZXCi/+u+99YLaugJIP6ZYIEdfpxnghqyVtaappBFTAyfG67Y
N/5mea1VqJzd8liFpIFQnl+X7U2x6emDbM01yJWV3aMmPwhtQ7iBdt5a4x82
EF5bZJ8HSRMvANDILD/9VTN8VfUQGKFjFY2GdX9ERwvfTb47bbv9Z28V1284
4lw2w1B1007Fo02v/Y0ukrN3VHCpmJQS1IiqZbYRa0DVK6UR5QNvUlj5fwWs
4qW9UDPhT/HDuaMrMFcejEn/7wvRUrGVtzCT9F56Al/dwRSxBejQQEb1AC8j
uuyi7gJaPdyNntR0EFTD7i02L6X2jB4YLfvGxP7Xeq1Y37t8NKF8CYTp0ry/
Wvw0iKZFbo4AkiI0aLyBCK9HBXhUKa9x06g0nhh1UFQrPGrk60RPQKqL76HA
E2ewzGDa90w1RBuAt2nRQpyNYjoASBvz/cAr3e0nuWsIzopZienrxI5ffcjY
f6UWA/OK3ITHtYHewVhseDyEqTQ4MUIWQS4NAwARAQABzTlBV1MgT3BzSHVi
IGZvciBTbm93IEZhbWlseSA8YXdzLW9wc2h1Yi1zaWduZXJAYW1hem9uLmNv
bT7CwY0EEAEIACAFAl/hGf8GCwkHCAMCBUIcGIEFgIBAAIZAQIbAwIeAQAh
CRAHgc9adPNF8RYhBDcvpelIaY930b0vqiGBz1p080XxGbcP+gPZX7LzKc1Y
w9CT3UHgkAIawOSXYktujzoYVxAz8/j3jEkCY0dKnfyqvWZDiJAXnzmXWwbg
cxg1g0GXNXCM4lAd68CmbA0LoLTaWSQX30ZbswzhbtX2ADAlOpV8RLBik7fm
bS9FyuubDRhfYRQq0fpjUGXFiEgwg6aMFxsrGLlv4QD7t+6ftFie/mxLbjR4
iMgtr8FIPXbgn05YYY/LeF4NIgX4iLEqRbAnfWjPzqQ1spFWAotIzDmZqby+
WdWThrH4K1rwtYM8sDhqRnMnqJrGFZzk7aDhVPwF+FOVMmPeEN5JRazEeUr1
VZaSw6mu0n4FMGSXuwGgdvmkqnMe6I5/xLdU4IOPNhp0UmakDW0q/a1dREDE
ZLMQDMINphmeQno4inGmwbRo63gitD4ZNR5sWwfuwty251o8Ekv7jkkp3mSv
pdxn5tptttnPaSPcSIX/4ED119Tu0i7aup+v30t7eikYDSZG6g9+jHB3Va9e
/VWShFSgy8Jm2+qq/ujUQDAGTCfSuY9jg1ITsog6ayEza/2upDJ1m+40HK4p
8DrEzP/3jTahT8q5ofFWSRDL17d31TSU+JBmPE3mz311FNXgi08w+taY320z
+irHtb3iSiiukbjS8s0maVgzszRqS9mhaEn4LL0zoqrUicmXgTyFB7n2LuYv
07vxM05xxhGQwsF2BBABCAAJBQJf4RoCAhsDACEJEBFVzT/tDi5FiEEi+09
V+UAYN9Gnw36EVm/NP+00LnnEQ/+J4C0Mn8j0AebXrwBiFs83sQo2q+WHL1S
MRc1g5gRFDXs6h1Gv+TGXRen7j1oeaddWvg0tUBxqmC0jr+8AKH00tiBWSu0
lsS8JU5rindEsKUrKTwcG2wyZFoe1z1E8xPkLRSRN5ZbbgKsTz1611HgCCId
Do+WJdDkWGwXmtDvzjM32EI/PVBd108ga9aPwXdhLw0dKAjZ4JrJXLUQJjRI
```

```

IVDSyM0bEH0UM6a/+mWNZazNfo0LSGwqGva6Xn5WJWlwR1S78vPNf03BQYU0
YRjaVQR+kPtB9aSAZni5sWfk6NrRNd1Q78d067uhhejsjRt7Mja2fEL4Kb1X
nK4U/ps7X103o/VjblneZ0hJK6kAKU172tnPJTJ31Jb0xX73wsMWDYZRZVcK
9X9+GFrpwhKHKKPjpM0t/FRxNepvqR172TkgBPqGH2TM0FdB1f/uQprvqge
PBbS0JrmBIH9/anIqgtMdtcNQB/0erLdCDqI5af0uD10LcLwdJwG9/bSrfwT
TVEE3WbXmJ8pZgMzlHUIZE6V2DSadV/YItk50I0jJR0VH0Hv1FMwGCEAIFzf
9P/pNi8hpEmLRphRi0VVcdQ30bH0M0gPHu5V9f1IhyCL1zU3LjYTHkq0yJD5
YDA1x01MYq3DcSM5130VBbLmuVS2GpcsTCYqlgQA6h/zzMwz+/70wU0EX+EZ
/wEQA0AY8ULmcJIQWIr14V0jylpJeD3qw7wd+QsBzJ+mOp0B/3ZFAhQiN01
9yCDlHeiZeAmWYX90IXrNiIdcHy+WTAp4G+NaMpqE52qhbDjz+IbvLp11yDH
bYEHpJnTHXEy21bvKAJ0Kkw/2RcQ0i4dodGnq5icyYj+9gcuHvnVwbrQ96Ia
0D7c+b5T+bzFqk90nIcztMRuhDLJnJpi70jpvQwfq/TkkZA+mzupxfSkq/Y
N9qXNEToT/VI2gn/LS0X4Ar112KxBjzNESQkwGSiWSYtMA5J+Tj5ED0uZ/qe
omNblAlD4bm7Na8NAoLxCtAiDq/f3To9Xb18lHsnd0mFLCb/BVgP4edQKTii
C/OZHy9QJ1fmN0aq7JVLQAuvQNEL88RKW6YZBqkPd3P6zdc7sWDLTMXM0d3I
e6NUvU7pW0E9NyRfUF+oT4s9wAJhAodinAi8Zi9rEfhK1VCJ76j7bcQqYZe0
jXD3IJ7T+X2XA8M/BmypoMw0Soljzhwh044RAasr/fAzpKNPB318JwcQunIz
u2N3CeJ+zrsomjcPxzehwsSVq1lzaL2ureJBL0KkBgYxUJYXpbS01ax1TsFG
091dAN0s9Ej8CND37GsNnuygj0gWXB6MNgbvPs3H3zi/AbMunQ1VB1w07JX
zdM1hBQZh6w+NeiEsK1T6wHi7IhxABEBAAHCwXYEGAEIAAkFAl/hGf8CGwwA
IQkQIYHPWnTzRfEWIQQ3L6XpSGmPd9Gzr6ohgc9adPNF8TMBD/9TbU/+PVbF
ywKvwi3GL0lpY7BXn8lQaHyunMGUavm080faRR0ynkH0ZqLHCp6bIajF0fvF
b7c0Jamzx8Hg+SIId16yRpRY+fA4RQ6PNnmT93ZgWW3EbjPyJGlm0/rt03SR
+0yn4/ldlg2KfBX4pqMoPCMKUdWxGmDETXsGihwZ0gmCZqXe8lK122PYkSN
JQQ+LlfjKvCaxfPKEjXYTbIbfyyhCR6NzA0VZxCrzSz2xDrYwP/V002K1xda
0ix6r2aEHf+xYEUh0aBt80HY5nXTuRReCVU789MUVtCMqD2u6amdo4BR0kWA
QNg4yavKwV+LVtyYh2Iju9VSyv4xL1Q4xKHvcAUrSH73bHG7b7jkUJckD0f4
twhjJk/Lfwe6RdnVo2WoeTvE93w+NAq2FXmvbiG7eltl0XfQecvQU3QNbRvH
U8B96W0w8UXJdvTKg4f0NbjSw7iJ3x5naixQ+rA8hLV8x0gn2LX6wvxT/SEu
mn20KX+fPtJELK7v/NheFLX1jsKLXYo4jHrkfIXNsNUhg/x2E71kAjbET3s+
t9kCtxt2iXDDZvpIbmG04QkvLFvOR0aSmN6+8fupe3e+e2yN0e6xGTuE60gX
I2+X1p1g9IduDYPoI20XleHyyMqGEEIb4g0iisloTp5oi3EuAYRGf1XuqAT
VA19bKnpkBsJ0A==
=tD2T
-----END PGP PUBLIC KEY BLOCK-----

```

2. Usa una suite software crittografica come GNU Privacy Guard per importare la chiave pubblica nel tuo portachiavi e annota il valore della chiave restituito.

```
gpg --import opshub-public-key.gpg
```

Example output del comando

```
gpg: key 1655BBDE2B770256: public key "AWS OpsHub for Snowball Edge <aws-opshub-signer@amazon.com>" imported
gpg: Total number processed: 1
gpg:             imported: 1
```

3. Verifica dell'impronta digitale. Assicurati di sostituirlo *key-value* con il valore del passaggio precedente. Ti consigliamo di utilizzare GPG per verificare l'impronta digitale.

```
gpg --fingerprint key-value
```

Questo comando restituisce un output simile al seguente.

```
pub  rsa4096 2020-12-21 [SC]
      372F A5E9 4869 8F77 D1B3  AFAA 2181 CF5A 74F3 45F1
uid          [ unknown] AWS OpsHub for Snowball Edge <aws-opshub-signer@amazon.com>
sub  rsa4096 2020-12-21 [E]
```

L'impronta digitale deve corrispondere alla seguente:

372F A5E9 4869 8F77 D1B3 AFAA 2181 CF5A 74F3 45F1

Se l'impronta digitale non corrisponde, non installare l' AWS OpsHub applicazione. Contattare Supporto.

4. Verifica il pacchetto di installazione e scarica il file SIGNATURE in base all'architettura e al sistema operativo dell'istanza, se non l'hai già fatto.
5. Verificare la firma del pacchetto di installazione. Assicurati di sostituire *signature-filename* e *OpsHub-download-filename* con i valori specificati durante il download del file SIGNATURE e AWS OpsHub dell'applicazione.

GPG

```
gpg --verify signature-filename OpsHub-download-filename
```

Questo comando restituisce un output simile al seguente.

GPG

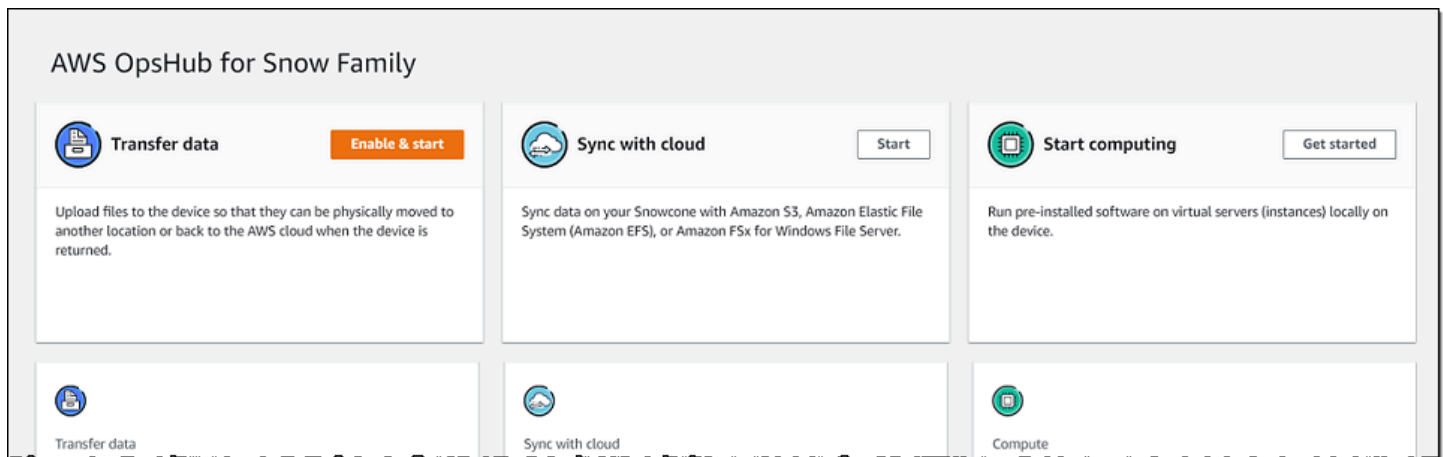
```
gpg: Signature made Mon Dec 21 13:44:47 2020 PST
gpg:                using RSA key 1655BBDE2B770256
gpg: Good signature from "AWS OpsHub for Snowball Edge <aws-opshub-
signer@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:                There is no indication that the signature belongs to the owner.
Primary key fingerprint: 9C93 4C3B 61F8 C434 9F94 5CA0 1655 BBDE 2B77 0256
```

Quando usate GPG, se l'output include la frase `BAD signature`, controllate se la procedura è stata eseguita correttamente. Se continui a ricevere questa risposta, contatta l'agente Supporto e non installarlo. Il messaggio di avviso sulla fiducia non significa che la firma non sia valida, ma solo che non hai verificato la chiave pubblica. Una chiave è considerata attendibile solo se è stata firmata dall'utente o da un firmatario fidato.

Gestione dei AWS servizi su Snowball Edge con AWS OpsHub

Con AWS OpsHub, puoi utilizzare e gestire i AWS servizi su Snowball Edge. Attualmente, AWS OpsHub supporta le seguenti risorse:

- Istanze Amazon Elastic Compute Cloud (Amazon EC2): utilizza istanze EC2 compatibili con Amazon per eseguire il software installato su un server virtuale senza inviarlo al server per l'elaborazione. Cloud AWS
- Network File System (NFS): utilizza le condivisioni di file per spostare i dati sul dispositivo. Puoi spedire il dispositivo AWS a cui trasferire i dati o utilizzarlo per DataSync trasferirli in altre Cloud AWS località. Cloud AWS
- Storage compatibile con Amazon S3 su Snowball Edge: offre uno storage di oggetti sicuro con maggiore resilienza, scalabilità e un set di funzionalità API Amazon S3 esteso per ambienti robusti, mobili, edge e disconnessi. Utilizzando lo storage compatibile con Amazon S3 su Snowball Edge, puoi archiviare dati ed eseguire applicazioni ad alta disponibilità su Snowball Edge per l'edge computing.



Argomenti

- [Avvio di un'istanza EC2 compatibile con Amazon su Snowball Edge con AWS OpsHub](#)
- [Arresto di un'istanza EC2 compatibile con Amazon su Snowball Edge con AWS OpsHub](#)
- [Avvio di un'istanza EC2 compatibile con Amazon su Snowball Edge con AWS OpsHub](#)
- [Utilizzo di coppie di chiavi per EC2 istanze compatibili in AWS OpsHub](#)
- [Terminare un'istanza EC2 compatibile con Amazon con AWS OpsHub](#)
- [Utilizzo dei volumi di storage localmente su Snowball Edge con AWS OpsHub](#)
- [Importazione di un'immagine come EC2 AMI compatibile con Amazon con AWS OpsHub](#)
- [Eliminazione di un'istantanea da Snowball Edge con AWS OpsHub](#)
- [Annullamento della registrazione di un'AMI su Snowball Edge con AWS OpsHub](#)
- [Gestione di un EC2 cluster Amazon su Snowball Edge con AWS OpsHub](#)
- [Configura lo storage compatibile con Amazon S3 su Snowball Edge con AWS OpsHub](#)
- [Gestione dello storage degli adattatori Amazon S3 con AWS OpsHub](#)
- [Gestione dell'interfaccia NFS con AWS OpsHub](#)

Avvio di un'istanza EC2 compatibile con Amazon su Snowball Edge con AWS OpsHub

Segui questi passaggi per avviare un'istanza EC2 compatibile con Amazon utilizzando AWS OpsHub.

Per avviare un'istanza EC2 compatibile con Amazon

1. Apri l' AWS OpsHub applicazione.

2. Nella sezione Avvia elaborazione del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute. Tutte le risorse di calcolo vengono visualizzate nella sezione Risorse .
3. Se sul tuo dispositivo sono in esecuzione istanze EC2 compatibili con Amazon, queste vengono visualizzate nella colonna Nome dell'istanza sotto Istanze. Puoi vedere i dettagli di ogni istanza in questa pagina.
4. Scegliere Launch Instance (Avvia istanza). Si apre la procedura guidata dell'istanza di avvio.
5. Per Dispositivo, scegli il dispositivo Snow su cui desideri avviare, EC2 compatibile con Amazon.

Launch instance

×

Device

192.0.2.0

Image (AMI)

snow-al2-test-ami-1.0.2

Instance type

sbe-c.small

☒ Create public IP address (VNI)

☐ Use existing IP address (VNI)

☐ Do not attach IP address

Physical network interface

SFP+:a.bc-1d2ef456gg678gi9j

IP Address assignment

DHCP

☒ Create key pair

☐ Use existing key pair

☐ Do not attach key pair

Name

test-instance-key-pair

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Create key pair

Cancel

Launch

6. Per Immagine (AMI), scegliere un'immagine Amazon Machine (AMI) dall'elenco. Questo AMI viene utilizzato per avviare la tua istanza.
7. Per Tipo di istanza, sceglierne uno dall'elenco.
8. Scegliere la modalità per allegare un indirizzo IP all'istanza. Sono disponibili le seguenti opzioni:
 - Crea indirizzo IP pubblico (VNI): scegli questa opzione per creare un nuovo indirizzo IP utilizzando un'interfaccia di rete fisica. Scegliere un'interfaccia di rete fisica e un'assegnazione di indirizzo IP.
 - Usa indirizzo IP esistente (VNI): scegli questa opzione per utilizzare un indirizzo IP esistente e quindi utilizzare le interfacce di rete virtuali esistenti. Scegliere un'interfaccia di rete fisica e un'interfaccia di rete virtuale.
 - Non allegare un indirizzo IP: scegli questa opzione se non desideri allegare un indirizzo IP.
9. Scegli come collegare una key pair all'istanza. Sono disponibili le seguenti opzioni:

Crea coppia di chiavi: scegli questa opzione per creare una nuova coppia di chiavi e avviare la nuova istanza con questa coppia di chiavi.

Usa una coppia di chiavi esistente: scegli questa opzione per utilizzare una coppia di chiavi esistente per avviare l'istanza.

Non allegare l'indirizzo IP: scegli questa opzione se non desideri allegare una key pair. Devi riconoscere che non sarai in grado di connetterti a questa istanza a meno che tu non conosca già la password incorporata in questa AMI.

Per ulteriori informazioni, consulta [Utilizzo di coppie di chiavi per EC2 istanze compatibili in AWS OpsHub](#).

10. Scegli Avvia. Dovresti vedere l'avvio dell'istanza nella sezione Istanze di calcolo . Lo stato è in sospeso e poi cambia in esecuzione al termine.

Arresto di un'istanza EC2 compatibile con Amazon su Snowball Edge con AWS OpsHub

Utilizza i seguenti passaggi AWS OpsHub per interrompere un'istanza EC2 compatibile con Amazon.

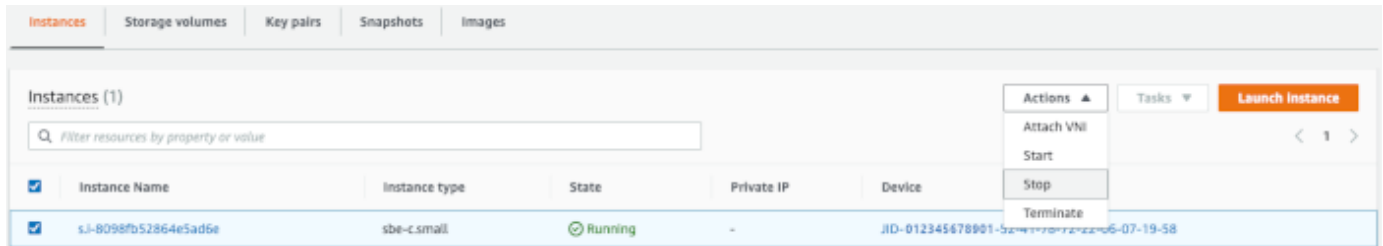
Per interrompere un'istanza EC2 compatibile con Amazon

1. Apri l' AWS OpsHub applicazione.

2. Nella sezione Avvia calcolo del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute.

Tutte le risorse di calcolo vengono visualizzate nella sezione Risorse .

3. Se sul tuo dispositivo sono in esecuzione istanze EC2 compatibili con Amazon, queste vengono visualizzate nella colonna Nome dell'istanza sotto Istanze.
4. Scegli l'istanza che desideri interrompere, scegli il menu Azioni e scegli Stop. Lo stato cambia in Arresto e poi in Arrestato al termine.



Avvio di un'istanza EC2 compatibile con Amazon su Snowball Edge con AWS OpsHub

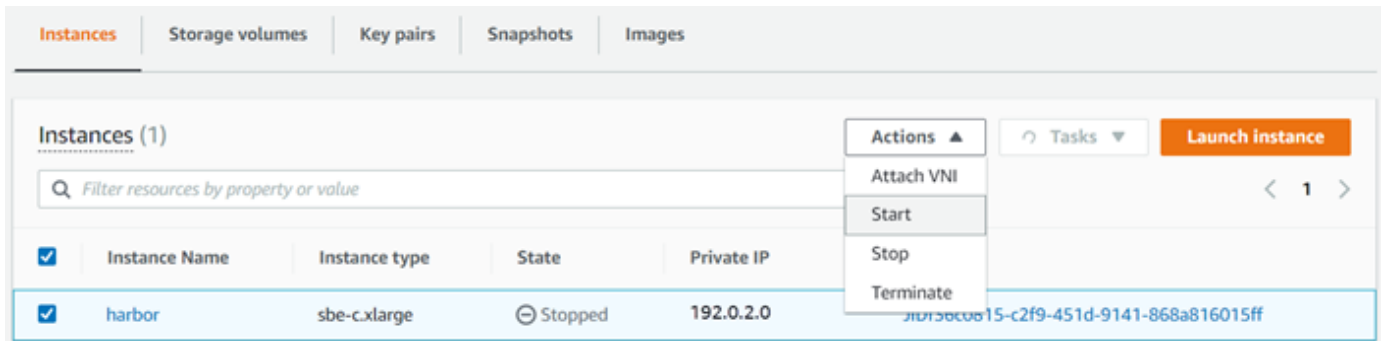
Segui questi passaggi per avviare un'istanza EC2 compatibile con Amazon utilizzando AWS OpsHub.

Per avviare un'istanza EC2 compatibile con Amazon

1. Apri l' AWS OpsHub applicazione.
2. Nella sezione Avvia calcolo del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute.

Le risorse di calcolo vengono visualizzate nella sezione Risorse .

3. Nella colonna Nome istanza in Istanze, individuare l'istanza che si desidera avviare.
4. Scegli l'istanza, quindi seleziona Avvia. Lo stato cambia In sospeso e poi in Esecuzione al termine.



Utilizzo di coppie di chiavi per EC2 istanze compatibili in AWS OpsHub

Quando avvii un'istanza EC2 compatibile con Amazon e intendi connetterti ad essa tramite SSH, devi fornire una key pair. Puoi usare Amazon EC2 per creare una nuova coppia di chiavi oppure puoi importare una coppia di chiavi esistente o gestire le tue coppie di chiavi.

Per creare, importare o gestire coppie di chiavi

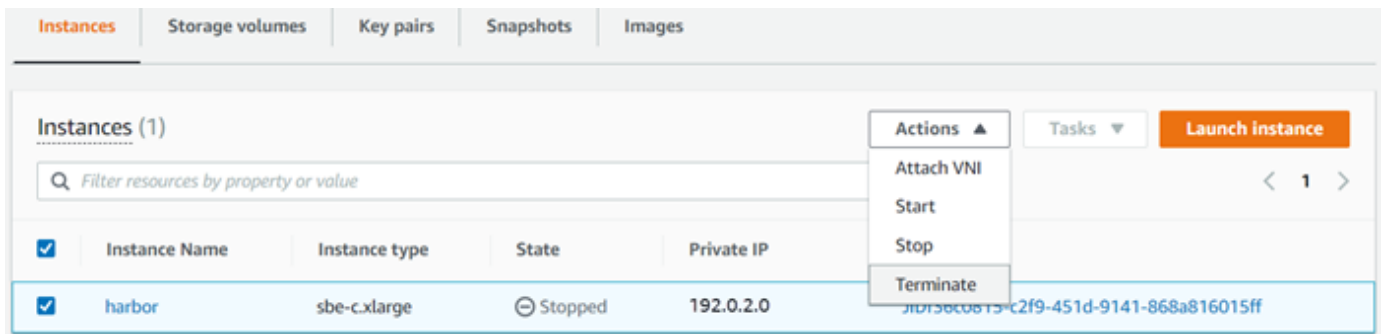
1. Apri Compute sulla AWS OpsHub dashboard.
2. Nel pannello di navigazione, scegli la pagina Compute (EC2), quindi scegli la scheda Key Pairs. Verrai reindirizzato alla EC2 console Amazon dove puoi creare, importare o gestire le tue coppie di chiavi.
3. Per istruzioni su come creare e importare coppie di chiavi, consulta le coppie di [EC2 chiavi Amazon e le istanze Linux](#) nella Amazon EC2 User Guide.

Terminare un'istanza EC2 compatibile con Amazon con AWS OpsHub

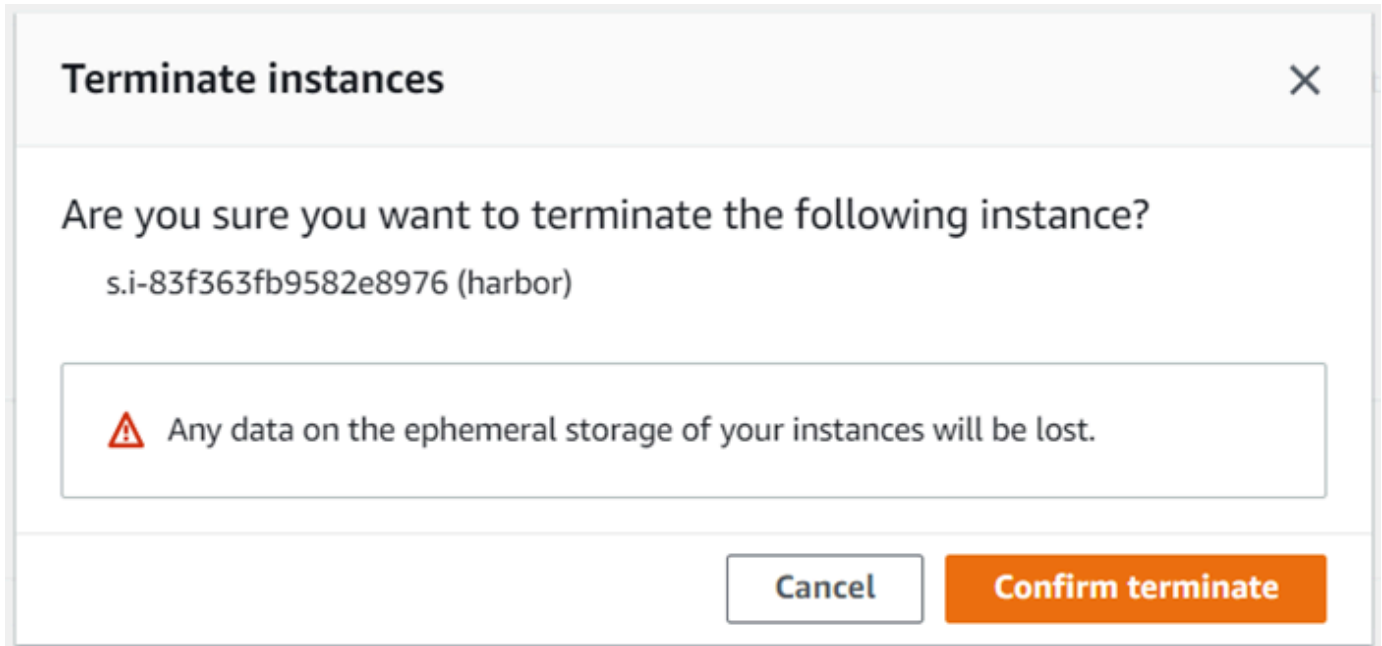
Dopo aver terminato un'istanza EC2 compatibile con Amazon, non puoi riavviarla.

Per terminare un'istanza compatibile EC2 con Amazon

1. Apri l'applicazione. AWS OpsHub
2. Nella sezione Avvia elaborazione del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute. È possibile visualizzare tutte le risorse di calcolo nella sezione Risorse .
3. Nella colonna Nome istanza in Istanze, individuare l'istanza che si desidera terminare.
4. Scegli l'istanza e scegli il menu Azioni. Dal menu Azioni, scegli Termina.



5. Nella finestra Termina istanze, scegli Conferma terminazione.



Note

Dopo che l'istanza è terminata, non è possibile riavviarla.

Lo stato cambia in Arresto in corso e quindi in Arrestato al termine.

Utilizzo dei volumi di storage localmente su Snowball Edge con AWS OpsHub

Le istanze EC2 compatibili con Amazon utilizzano volumi Amazon EBS per lo storage. In questa procedura, crei un volume di storage e lo colleghi all'istanza utilizzando AWS OpsHub

Per creare un volume di archiviazione

1. Apri l' AWS OpsHub applicazione.
2. Nella sezione Avvia elaborazione del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute.
3. Scegliere la scheda Volumi di archiviazione . Se sul dispositivo sono presenti volumi di archiviazione, i dettagli sui volumi vengono visualizzati in Volumi di archiviazione.
4. Scegliere Crea volume per aprire la pagina Crea volume .

Device
Select the device on which you wish to create the volume.

JID5a11d1db-8b98-4f37-80bf-97af46e45eb2 - 10.24.34.0

Size
Define the size of the volume, in GiBs.

100

Volume Type
Select a performance type for your volume.

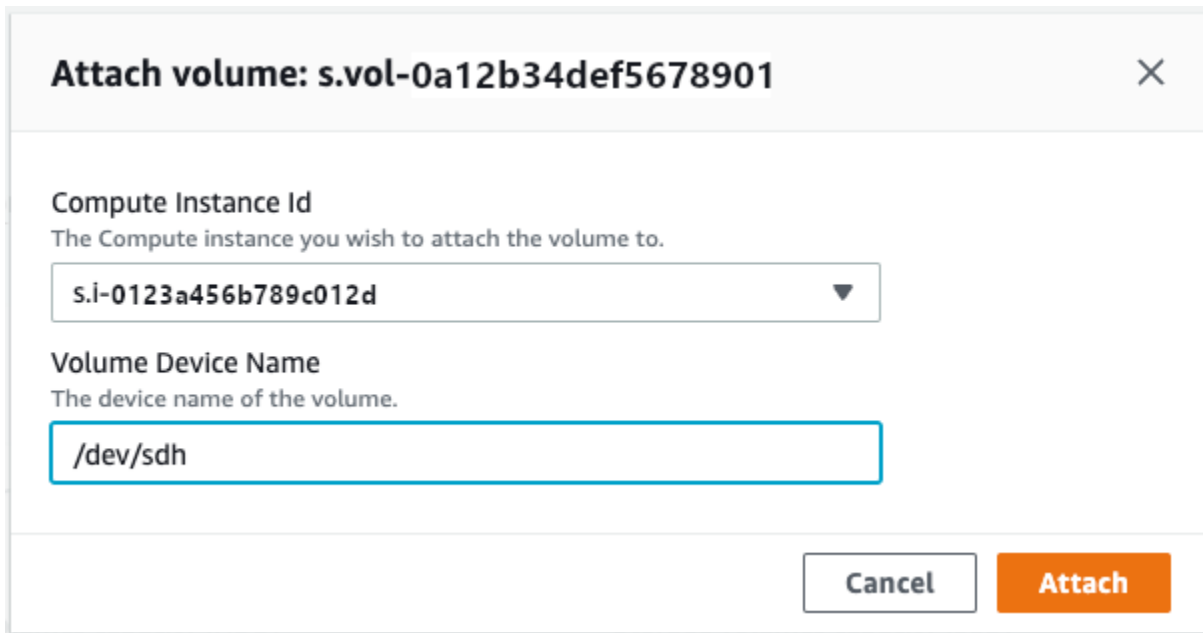
Capacity-optimized HDD volume (sbg1)

Cancel Submit

5. Scegli il dispositivo su cui vuoi creare il volume, inserisci la dimensione (in GiBs) che desideri creare e scegli il tipo di volume.
6. Scegli Invia. Lo stato sta creando e cambia in Disponibile al termine. È possibile visualizzare il volume e i dettagli su di esso nella scheda Volumi .

Per collegare un volume di archiviazione all'istanza

1. Scegliere il volume creato e quindi scegliere Allega volume.



Attach volume: s.vol-0a12b34def5678901

Compute Instance Id
The Compute instance you wish to attach the volume to.

s.i-0123a456b789c012d

Volume Device Name
The device name of the volume.

/dev/sdh

Cancel Attach

2. Per ID istanza di calcolo, scegli l'istanza a cui collegare il volume.
3. Per Nome dispositivo volume, immettere il nome del dispositivo del volume (ad esempio, **/dev/sdh** o **xvdh**).
4. Scegli Collega.

Se il volume non è più necessario, è possibile staccarlo dall'istanza e quindi eliminarlo.

Importazione di un'immagine come EC2 AMI compatibile con Amazon con AWS OpsHub

Puoi importare un'istantanea dell'immagine nel dispositivo Snowball Edge e registrarla come Amazon Machine Image (AMI) EC2 compatibile con Amazon. Un'istantanea è fondamentalmente una copia del volume di archiviazione che puoi utilizzare per creare un'AMI o un altro volume di archiviazione. In questo modo, puoi trasferire la tua immagine da una fonte esterna sul tuo dispositivo e avviarla come istanza EC2 compatibile con Amazon.

Segui questi passaggi per completare l'importazione dell'immagine.

1. Carica la tua istantanea in un bucket Amazon S3 sul tuo dispositivo.
2. Configura le autorizzazioni necessarie per concedere l'accesso ad Amazon S3, EC2 Amazon e VM Import/Export, la funzionalità utilizzata per importare ed esportare le istantanee.
3. Importa l'istantanea dal bucket S3 nel tuo dispositivo come immagine.

4. Registra l'immagine come AMI EC2 compatibile con Amazon.
5. Avvia l'AMI come istanza EC2 compatibile con Amazon.

Note

Tieni presente le seguenti limitazioni quando carichi istantanee su Snowball Edge.

- Attualmente Snowball Edge supporta solo l'importazione di istantanee in formato immagine RAW.
- Attualmente Snowball Edge supporta solo l'importazione di istantanee con dimensioni da 1 GB a 1 TB.

Passaggio 1: carica un'istanza in un bucket S3 sul tuo dispositivo

Devi caricare lo snapshot su Amazon S3 sul tuo dispositivo prima di importarlo. Questo perché le istantanee possono essere importate solo da Amazon S3 disponibile sul tuo dispositivo o cluster. Durante il processo di importazione, scegli il bucket S3 sul tuo dispositivo in cui archiviare l'immagine.

Per caricare uno snapshot su Amazon S3

- Per creare un bucket S3, consulta [Creazione di Amazon S3 Storage](#).

Per caricare uno snapshot in un bucket S3, consulta [Caricamento di file su Amazon S3 Storage](#).

Passaggio 2: importa lo snapshot da un bucket S3

Quando la tua istantanea viene caricata su Amazon S3, puoi importarla sul tuo dispositivo. Tutte le istantanee che sono state importate o sono in fase di importazione vengono visualizzate nella scheda Istanzae.

Per importare l'istantanea sul tuo dispositivo

1. Apri l' AWS OpsHub applicazione.
2. Nella sezione Avvia elaborazione del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute. Tutte le risorse di calcolo vengono visualizzate nella sezione Risorse .

3. Scegli la scheda Istantanee per vedere tutte le istantanee che sono state importate sul tuo dispositivo. Il file di immagine in Amazon S3 è un file.raw che viene importato nel dispositivo come istantanea. Puoi filtrare in base all'ID dello snapshot o allo stato dello snapshot per trovare istantanee specifiche. Puoi scegliere un ID di istantanea per visualizzare i dettagli di quell'istantanea.
4. Scegliete l'istantanea che desiderate importare e scegliete Importa istantanea per aprire la pagina Importa istantanea.
5. Per Dispositivo, scegli l'indirizzo IP del dispositivo Snow Family su cui desideri importare.
6. Per Descrizione dell'importazione e Descrizione dell'istantanea, inserisci una descrizione per ciascuno.
7. Nell'elenco Ruolo, scegliete un ruolo da utilizzare per l'importazione. Snowball Edge utilizza VM per Import/Export importare istantanee. AWS assume questo ruolo e lo utilizza per importare l'istantanea per tuo conto. Se non hai un ruolo configurato sul tuo AWS Snowball Edge, apri AWS Identity and Access Management (IAM) in AWS OpsHub cui puoi creare un ruolo IAM locale. Il ruolo necessita inoltre di una policy che disponga delle Import/Export autorizzazioni VM necessarie per eseguire l'importazione. È necessario allegare questa politica al ruolo. Per maggiori dettagli su questo argomento, consulta [Using IAM Locally](#).

Di seguito è riportato un esempio della politica.

JSON

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

Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

Il ruolo che crei deve avere autorizzazioni minime per accedere ad Amazon S3. Di seguito è riportato un esempio di policy minima.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetMetadata"
      ],
      "Resource": [
        "arn:aws:s3:::import-snapshot-bucket-name",
        "arn:aws:s3:::import-snapshot-bucket-name/*"
      ]
    }
  ]
}
```

8. Scegli Browse S3 e scegli il bucket S3 che contiene lo snapshot che desideri importare. Scegli l'istantanea e scegli Invia. L'istantanea inizia a essere scaricata sul tuo dispositivo. Puoi scegliere l'ID dell'istantanea per visualizzare i dettagli. Puoi annullare il processo di importazione da questa pagina.

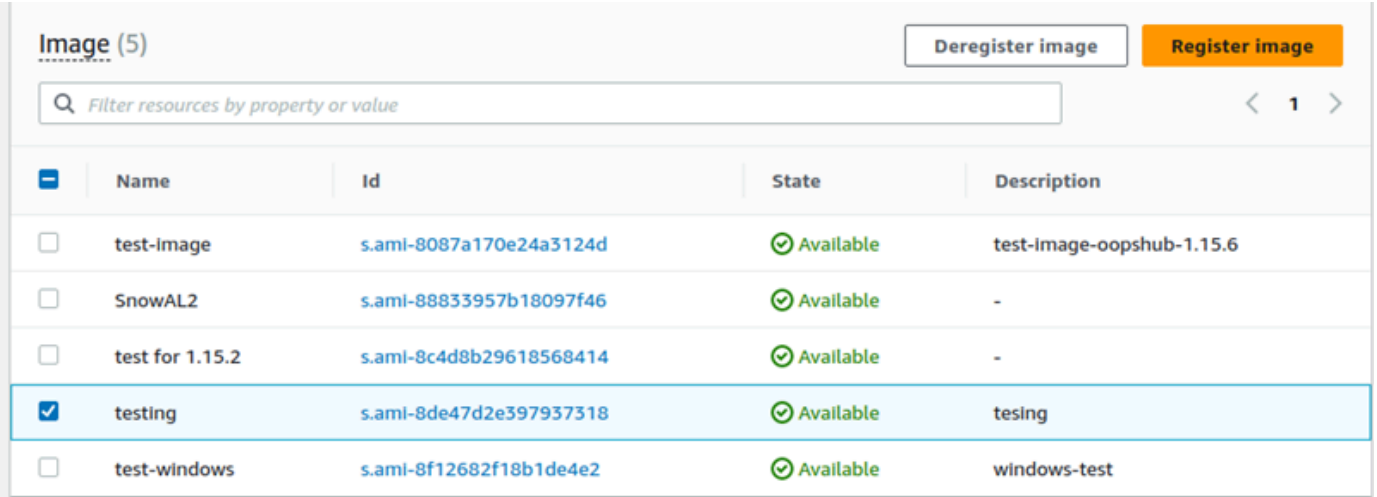
Fase 3: Registrare lo snapshot come AMI compatibile EC2 con Amazon

Il processo di creazione di un'AMI EC2 compatibile con Amazon da un'immagine importata come snapshot è noto come registrazione. Le immagini importate sul dispositivo devono essere registrate prima di poter essere avviate come istanze EC2 compatibili con Amazon.

Per registrare un'immagine importata come istantanea

1. Aprire l' AWS OpsHub applicazione.

2. Nella sezione Avvia elaborazione del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute. Tutte le risorse di calcolo vengono visualizzate nella sezione Risorse .
3. Scegli la scheda Images (Immagini). Puoi filtrare le immagini per nome, ID o stato per trovare un'immagine specifica.
4. Scegli l'immagine che desideri registrare e scegli Registra immagine.



	Name	Id	State	Description
☐	test-image	s.ami-8087a170e24a3124d	Available	test-image-oopshub-1.15.6
☐	SnowAL2	s.ami-88833957b18097f46	Available	-
☐	test for 1.15.2	s.ami-8c4d8b29618568414	Available	-
☒	testing	s.ami-8de47d2e397937318	Available	tesing
☐	test-windows	s.ami-8f12682f18b1de4e2	Available	windows-test

5. Nella pagina Registra immagine, fornisci un nome e una descrizione.
6. Per il volume Root, specificate il nome del dispositivo root.

Nella sezione Block device, puoi modificare la dimensione del volume e il tipo di volume.

7. Se desideri che il volume venga eliminato quando l'istanza viene terminata, scegli Elimina alla chiusura.
8. Se desideri aggiungere altri volumi, scegli Aggiungi nuovo volume.
9. Quando hai finito, scegli Invia.

Passaggio 4: avvia l'AMI EC2 compatibile con Amazon

- Per ulteriori informazioni, consulta [Avvio di un'istanza EC2 compatibile con Amazon](#).

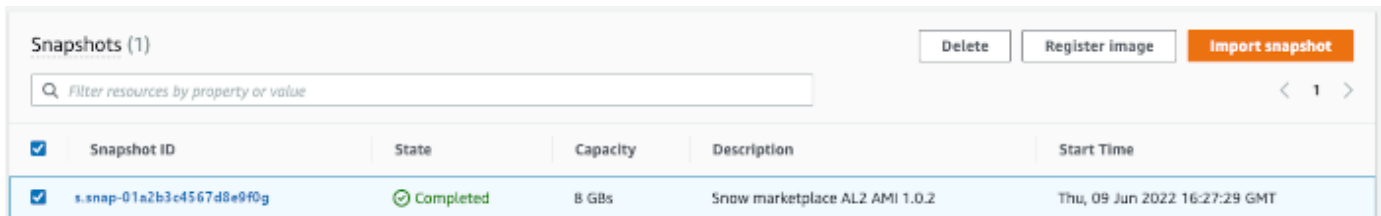
Eliminazione di un'istantanea da Snowball Edge con AWS OpsHub

Se non hai più bisogno di un'istantanea, puoi eliminarla dal tuo dispositivo. Il file di immagine in Amazon S3 è un file.raw che viene importato nel dispositivo come istantanea. Se l'istantanea che

stai eliminando viene utilizzata da un'immagine, non può essere eliminata. Una volta completata l'importazione, puoi anche eliminare il file.raw che hai caricato su Amazon S3 sul tuo dispositivo.

Per eliminare uno snapshot

1. Apri l'applicazione. AWS OpsHub
2. Nella sezione Avvia elaborazione del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute. Tutte le risorse di calcolo vengono visualizzate nella sezione Risorse .
3. Scegli la scheda Istantanea per vedere tutte le istantanee che sono state importate. Puoi filtrare in base all'ID dell'istananea o allo stato dell'istananea per trovare istantanee specifiche.
4. Scegliete l'istananea che desiderate eliminare e scegliete Elimina. Puoi scegliere più istantanee.



The screenshot shows the 'Snapshots (1)' section in AWS OpsHub. It includes a search bar, a 'Delete' button, a 'Register image' button, and an 'Import snapshot' button. Below is a table with columns: Snapshot ID, State, Capacity, Description, and Start Time. One snapshot is listed with ID 's.snap-01a2b3c4567d8e9f0g', State 'Completed', Capacity '8 GBs', Description 'Snow marketplace AL2 AMI 1.0.2', and Start Time 'Thu, 09 Jun 2022 16:27:29 GMT'.

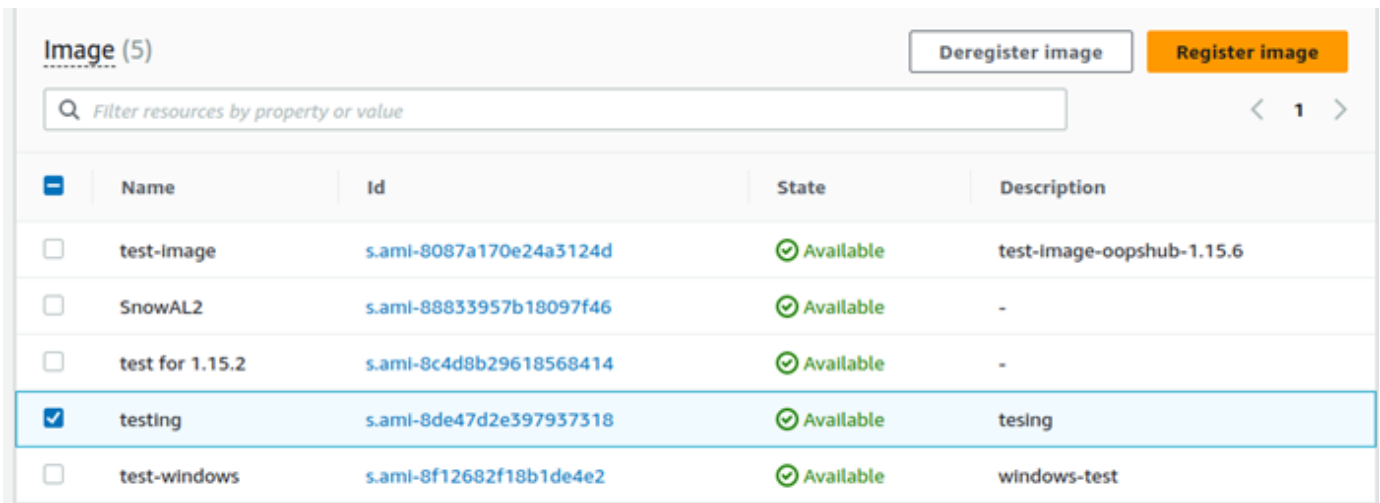
Snapshot ID	State	Capacity	Description	Start Time
s.snap-01a2b3c4567d8e9f0g	Completed	8 GBs	Snow marketplace AL2 AMI 1.0.2	Thu, 09 Jun 2022 16:27:29 GMT

5. Nella casella di conferma dell'eliminazione dell'istananea, scegli Elimina istantanea. Se l'eliminazione ha esito positivo, l'istananea viene rimossa dall'elenco nella scheda Istantanee.

Annullamento della registrazione di un'AMI su Snowball Edge con AWS OpsHub

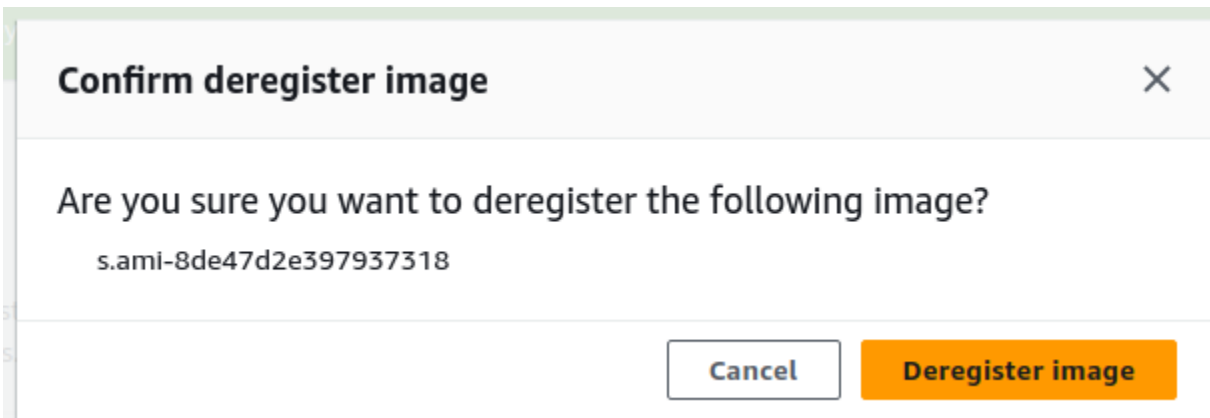
Per annullare la registrazione di un'AMI

1. Apri l'applicazione. AWS OpsHub
2. Nella sezione Avvia elaborazione del dashboard scegliere Inizia. Oppure, scegli il menu Servizi in alto, quindi scegli Compute (EC2) per aprire la pagina Compute. Tutte le risorse di calcolo vengono visualizzate nella sezione Risorse .
3. Scegli la scheda Images (Immagini). Sono elencate tutte le tue immagini. Puoi filtrare le immagini per nome, ID o stato per trovare un'immagine specifica.
4. Scegli l'immagine che desideri annullare la registrazione e scegli Annulla registrazione.



	Name	Id	State	Description
☐	test-image	s.ami-8087a170e24a3124d	Available	test-image-oopshub-1.15.6
☐	SnowAL2	s.ami-88833957b18097f46	Available	-
☐	test for 1.15.2	s.ami-8c4d8b29618568414	Available	-
☒	testing	s.ami-8de47d2e397937318	Available	tesing
☐	test-windows	s.ami-8f12682f18b1de4e2	Available	windows-test

5. Nella finestra Conferma annullamento della registrazione dell'immagine, conferma l'ID dell'immagine e scegli Annulla registrazione dell'immagine. Se l'annullamento della registrazione ha esito positivo, l'immagine viene rimossa dall'elenco delle immagini.



Gestione di un EC2 cluster Amazon su Snowball Edge con AWS OpsHub

Un EC2 cluster Amazon è un gruppo di dispositivi che forniscono insieme come cluster di dispositivi. Per utilizzare un cluster, i AWS servizi sul dispositivo devono essere in esecuzione sull'endpoint predefinito. È inoltre necessario scegliere il dispositivo specifico del cluster con cui si desidera parlare. È possibile utilizzare un cluster in base a ciascun dispositivo.

Per creare un EC2 cluster Amazon

1. Connettiti e accedi al tuo dispositivo Snow. Per istruzioni su come accedere al dispositivo, vedere [Sblocco di un dispositivo Snowball Edge con AWS OpsHub](#).
2. Nella pagina Scegli dispositivo, scegli cluster Snowball Edge, quindi scegli Avanti.

3. Nella pagina Connetti al dispositivo fornire l'indirizzo IP del dispositivo e gli indirizzi IP di altri dispositivi nel cluster.
4. Scegliere Aggiungi un altro dispositivo per aggiungere altri dispositivi, quindi scegliere Avanti.
5. Nella pagina Fornisci le chiavi immettere il codice di sblocco del client del dispositivo, caricare il manifesto del dispositivo e scegliere Sblocca dispositivo.

I dispositivi Snowball Edge utilizzano la crittografia a 256 bit per garantire la sicurezza e la completezza chain-of-custody dei dati.

6. (Facoltativo) Immettete un nome per creare un profilo, quindi scegliete Salva nome profilo. Si viene indirizzati al dashboard, dove vengono visualizzati tutti i cluster.

Ora puoi iniziare a utilizzare AWS i servizi e a gestire il tuo cluster. Le istanze del cluster vengono gestite nello stesso modo in cui vengono gestite singole istanze. Per istruzioni, consultare [Gestione dei AWS servizi su Snowball Edge con AWS OpsHub](#).

Configura lo storage compatibile con Amazon S3 su Snowball Edge con AWS OpsHub

Lo storage compatibile con Amazon S3 sul servizio Snowball Edge non è attivo per impostazione predefinita. Per avviare il servizio su un dispositivo o un cluster, è necessario creare due interfacce di rete virtuali (VNICs) su ciascun dispositivo da collegare agli `s3control` endpoint. `s3api`

Argomenti

- [Storage compatibile con Amazon S3 su Snowball Edge: prerequisiti per AWS OpsHub](#)
- [Utilizzando lo storage compatibile con Amazon S3 su Snowball Edge, una semplice opzione di configurazione in AWS OpsHub](#)
- [Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge, opzione di configurazione avanzata utilizzando AWS OpsHub](#)
- [Configurazione dello storage compatibile con Amazon S3 su Snowball Edge per l'avvio automatico tramite AWS OpsHub](#)
- [Creazione di un bucket in uno storage compatibile con Amazon S3 su Snowball Edge utilizzando AWS OpsHub](#)
- [Carica file e cartelle su uno storage compatibile con Amazon S3 su bucket Snowball Edge utilizzando AWS OpsHub](#)

- [Rimuovi file e cartelle dallo storage compatibile con Amazon S3 sui bucket Snowball Edge con AWS OpsHub AWS OpsHub](#)
- [Eliminare i bucket dallo storage compatibile con Amazon S3 su Snowball Edge](#)

Storage compatibile con Amazon S3 su Snowball Edge: prerequisiti per AWS OpsHub

Prima di poter configurare il dispositivo o il cluster utilizzando AWS OpsHub, procedi come segue:

- Accendi il dispositivo Snowball Edge e collegalo alla rete.
- Sul computer locale, scarica e installa la versione più recente di [AWS OpsHub](#). Connect al dispositivo o al cluster per sbloccarlo con un file manifest. Per ulteriori informazioni, consulta [Sblocco di un dispositivo](#).

Utilizzando lo storage compatibile con Amazon S3 su Snowball Edge, una semplice opzione di configurazione in AWS OpsHub

Utilizza l'opzione di configurazione semplice se la rete utilizza DHCP. Con questa opzione, VNICs vengono creati automaticamente su ogni dispositivo all'avvio del servizio.

1. Accedi a AWS OpsHub, quindi scegli Gestisci archiviazione.

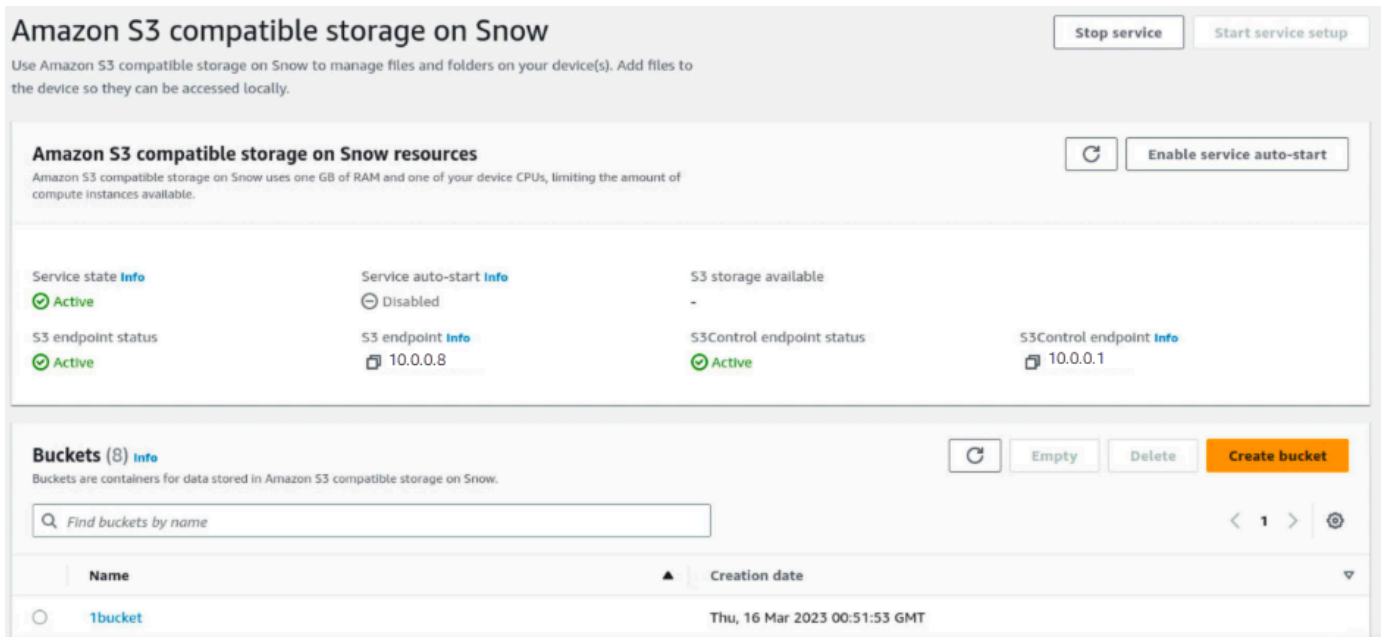
Verrai reindirizzato alla pagina di destinazione dello storage compatibile con Amazon S3 su Snowball Edge.

2. Per il tipo di configurazione del servizio Start, scegli Simple.
3. Scegli Avvia servizio.

Note

Il completamento dell'operazione richiede alcuni minuti e dipende dal numero di dispositivi che stai utilizzando.

Dopo l'avvio del servizio, lo stato del servizio è attivo e sono presenti endpoint.



Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge, opzione di configurazione avanzata utilizzando AWS OpsHub

Utilizza l'opzione di configurazione avanzata se la tua rete utilizza indirizzi IP statici o se desideri riutilizzare quelli esistenti. VNIs Con questa opzione, puoi creare manualmente VNICs per ogni dispositivo.

1. Accedi a AWS OpsHub, quindi scegli Gestisci archiviazione.

Verrai reindirizzato alla pagina di destinazione dello storage compatibile con Amazon S3 su Snowball Edge.

2. Per il tipo di configurazione Start del servizio, scegli Avanzato.
3. Seleziona i dispositivi VNICs per i quali devi creare.

Per i cluster, è necessario un quorum minimo di dispositivi per avviare lo storage compatibile con Amazon S3 sul servizio Snowball Edge. Il quorum è due per un cluster a tre nodi.

Note

Per l'avvio iniziale del servizio in una configurazione di cluster, è necessario che tutti i dispositivi del cluster siano configurati e disponibili per l'avvio del servizio. Per gli avvisi

successivi, è possibile utilizzare un sottoinsieme di dispositivi se si raggiunge il quorum, ma il servizio verrà avviato in uno stato degradato.

4. Per ogni dispositivo, scegli una VNIC esistente o seleziona Crea VNI.

Ogni dispositivo necessita di una VNIC per l'endpoint S3 per le operazioni sugli oggetti e un'altra per l'endpoint S3Control per le operazioni con i bucket.

5. Se stai creando una VNIC, scegli un'interfaccia di rete fisica e inserisci l'indirizzo IP di stato e la subnet mask, quindi scegli Crea interfaccia di rete virtuale.
6. Dopo aver creato il tuo VNICS, scegli Avvia servizio.

Note

Il completamento dell'operazione richiede alcuni minuti e dipende dal numero di dispositivi che stai utilizzando.

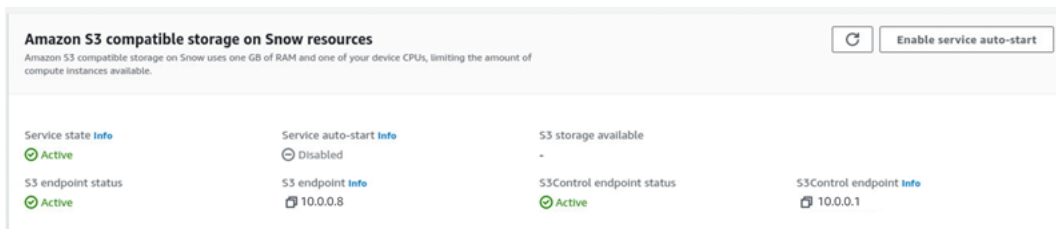
Dopo l'avvio del servizio, lo stato del servizio è attivo e sono presenti endpoint.

Configurazione dello storage compatibile con Amazon S3 su Snowball Edge per l'avvio automatico tramite AWS OpsHub

1. Accedi a, quindi scegli Manage AWS OpsHub Storage.

Verrai reindirizzato alla pagina di destinazione dello storage compatibile con Amazon S3 su Snowball Edge.

2. Nello storage compatibile con Amazon S3 sulle risorse Snow, scegli Abilita l'avvio automatico del servizio. Il sistema configura il servizio in modo che venga avviato automaticamente in futuro.



Creazione di un bucket in uno storage compatibile con Amazon S3 su Snowball Edge utilizzando AWS OpsHub

Usa l' AWS OpsHub interfaccia per creare un bucket Amazon S3 sul tuo dispositivo Snowball Edge.

1. Aprire. AWS OpsHub
2. In Gestisci spazio di archiviazione, scegli Inizia. Viene visualizzata la pagina Storage on Snow compatibile con Amazon S3.
3. In Bucket, scegli Crea bucket. Viene visualizzata la schermata Crea bucket.

Create bucket

Bucket settings

Bucket name [Info](#)

test123

Bucket names must be unique within your Snowball device or cluster and must not contain spaces or uppercase letters.

Default encryption

Automatically encrypt new objects uploaded to this snow bucket. [Learn more](#)

S3 compatible storage on Snow buckets are encrypted at all times and this setting cannot be changed.

Default encryption
Enabled

Encryption type
Amazon S3 key (SSE-S3)

Cancel Create bucket

4. In Bucket name, inserisci un nome per il bucket.

Note

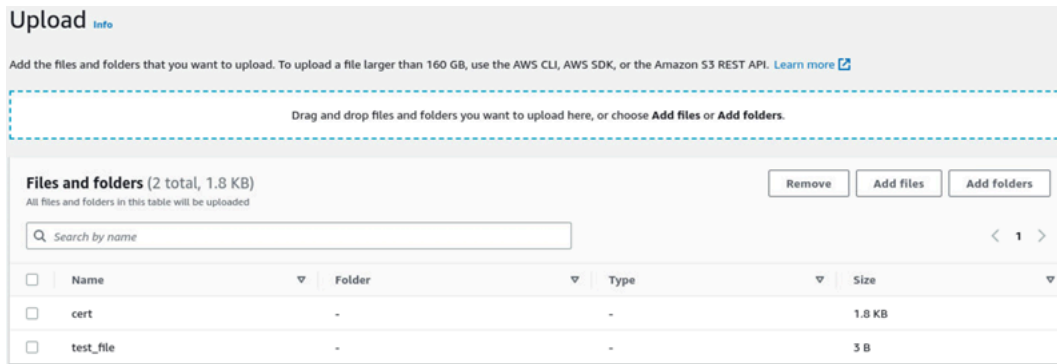
I nomi dei bucket devono essere univoci all'interno del dispositivo o del cluster Snowball e non devono contenere spazi o lettere maiuscole.

5. Seleziona Crea bucket. Il sistema crea il bucket e viene visualizzato in Bucket nella pagina di storage compatibile con Amazon S3 su Snow.

Carica file e cartelle su uno storage compatibile con Amazon S3 su bucket Snowball Edge utilizzando AWS OpsHub

Usa l' AWS OpsHub interfaccia per caricare file e cartelle su uno storage compatibile con Amazon S3 su bucket Snowball Edge. I file e le cartelle possono essere caricati separatamente o insieme.

1. Aprire AWS OpsHub
2. In Gestisci spazio di archiviazione, in Bucket, scegli un bucket in cui caricare i file. Viene visualizzata la pagina relativa a quel bucket.
3. Nella pagina del bucket, scegli Carica file. Viene visualizzata la pagina di caricamento.



4. Carica file o cartelle trascinandoli da un gestore di file del sistema operativo alla AWS OpsHub finestra o procedi come segue:
 - a. Seleziona Aggiungi file o Aggiungi cartelle.
 - b. Seleziona uno o più file o cartelle da caricare. Seleziona Apri.

Il sistema carica i file e le cartelle selezionati nel bucket del dispositivo. Una volta completato il caricamento, i nomi dei file e delle cartelle vengono visualizzati nell'elenco File e cartelle.

Rimuovi file e cartelle dallo storage compatibile con Amazon S3 sui bucket Snowball Edge con AWS OpsHub

Utilizza l' AWS OpsHub interfaccia per rimuovere ed eliminare definitivamente file e cartelle dai bucket sul dispositivo Snowball Edge.

1. Apri. AWS OpsHub
2. In Gestisci spazio di archiviazione, in Bucket, seleziona il nome di un bucket da cui eliminare file e cartelle. Viene visualizzata la pagina relativa a quel bucket.
3. In File e cartelle seleziona le caselle di controllo dei file e delle cartelle da eliminare definitivamente.
4. Selezionare Rimuovi. Il sistema rimuove i file o le cartelle dal bucket del dispositivo.

Eliminare i bucket dallo storage compatibile con Amazon S3 su Snowball Edge

Prima di poter eliminare un bucket da un dispositivo, il bucket deve essere vuoto. Rimuovi file e cartelle dal bucket o usa lo strumento del bucket vuoto. Per rimuovere file e cartelle, consulta.

[Rimuovi file e cartelle dallo storage compatibile con Amazon S3 sui bucket Snowball Edge con AWS OpsHub AWS OpsHub](#)

Per utilizzare lo strumento Empty Bucket

1. Aprire AWS OpsHub.
2. In Gestisci spazio di archiviazione, in Bucket, seleziona il pulsante di opzione del bucket da svuotare.
3. Seleziona Vuoto. Viene visualizzata la pagina Empty bucket.

Empty bucket info

⚠ Emptying the bucket deletes all objects in the bucket and cannot be undone.
Objects added to the bucket while the empty bucket action is in progress might be deleted.

ℹ If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket. [Go to lifecycle rule configuration](#)

Permanently delete all objects in bucket "test123"?

To confirm deletion, type *permanently delete* in the text input field.

permanently delete

Cancel Empty

4. Nella casella di testo della pagina Empty bucket, digita. **permanently delete**
5. Seleziona Vuoto. Il sistema svuota il secchio.

Per eliminare un bucket vuoto

1. In Gestisci spazio di archiviazione, in Bucket, seleziona il pulsante di opzione del bucket da eliminare.
2. Seleziona Elimina. Viene visualizzata la pagina Elimina bucket.

Delete bucket "test123"?

To confirm deletion, type the name of the bucket in the field.

test123

Cancel Delete

3. Nella casella di testo della pagina Elimina bucket, digita il nome del bucket.

4. Seleziona Elimina. Il sistema elimina il bucket dal dispositivo.

Gestione dello storage degli adattatori Amazon S3 con AWS OpsHub

Puoi utilizzarlo AWS OpsHub per creare e gestire lo storage Amazon Simple Storage Service (Amazon S3) su Snowball Edge utilizzando l'adattatore S3 per lavori di importazione ed esportazione.

Argomenti

- [Accesso allo storage Amazon S3 con AWS OpsHub](#)
- [Caricamento di file sullo storage Amazon S3 con AWS OpsHub](#)
- [Scaricamento di file dallo storage Amazon S3 con AWS OpsHub](#)
- [Eliminazione di file dallo storage Amazon S3 con AWS OpsHub](#)

Accesso allo storage Amazon S3 con AWS OpsHub

Puoi caricare file sul tuo dispositivo e accedervi localmente. Puoi spostarli fisicamente in un'altra posizione sul dispositivo o importarli nuovamente Cloud AWS quando il dispositivo viene restituito.

Snowball Edge utilizza i bucket Amazon S3 per archiviare e gestire i file sul dispositivo.

Per accedere a un bucket S3

1. Apri l'applicazione. AWS OpsHub
2. Nella sezione Gestisci archiviazione file del dashboard scegliere Inizia.

Se il dispositivo è stato ordinato con il meccanismo di trasferimento Amazon S3, viene visualizzato nella sezione Bucket della pagina di archiviazione di file e oggetti. Nella pagina di archiviazione di file e oggetti, puoi visualizzare i dettagli di ogni bucket.

Note

Se il dispositivo è stato ordinato con il meccanismo di trasferimento NFS, il nome del bucket verrà visualizzato nella sezione dei punti di montaggio dopo la configurazione e l'attivazione del servizio NFS. Per ulteriori informazioni sull'uso dell'interfaccia NFS, vedere. [Gestione dell'interfaccia NFS con AWS OpsHub](#)

File & object storage

Use Amazon S3 to manage files and objects stored on your device. Add files to the device so they can be accessed locally. For import jobs, the files will be transferred to AWS when the device is sent back.

Resources

Storage available

925.85 GB available of 925.93 GB

99%

Select a bucket below to start transferring files to your device.

Buckets (7)

Filter buckets

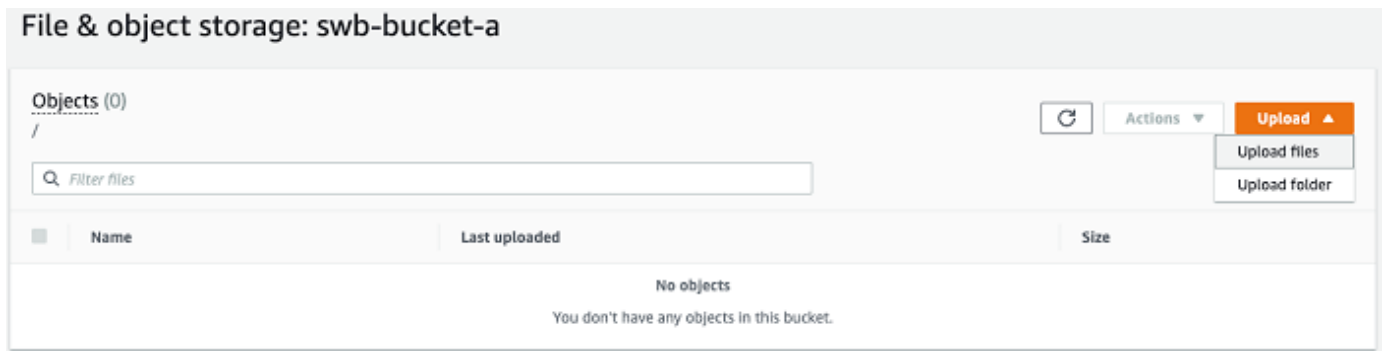
< 1 >

Bucket name	Date created
sbw-output	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-a	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-b	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-c	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-d	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-e	Mon, 12 Oct 2009 17:50:30 GMT
swb-bucket-f	Mon, 12 Oct 2009 17:50:30 GMT

Caricamento di file sullo storage Amazon S3 con AWS OpsHub

Caricamento di un file

1. Nella sezione Gestisci archiviazione file nel dashboard scegliere Inizia. Se sul dispositivo sono presenti bucket Amazon S3, questi vengono visualizzati nella sezione Bucket della pagina di archiviazione dei file. Puoi vedere i dettagli di ogni bucket nella pagina.
2. Scegliere il bucket in cui si desidera caricare i file.
3. Scegli Carica, quindi Carica file o trascina i file nel bucket e scegli OK.



Note

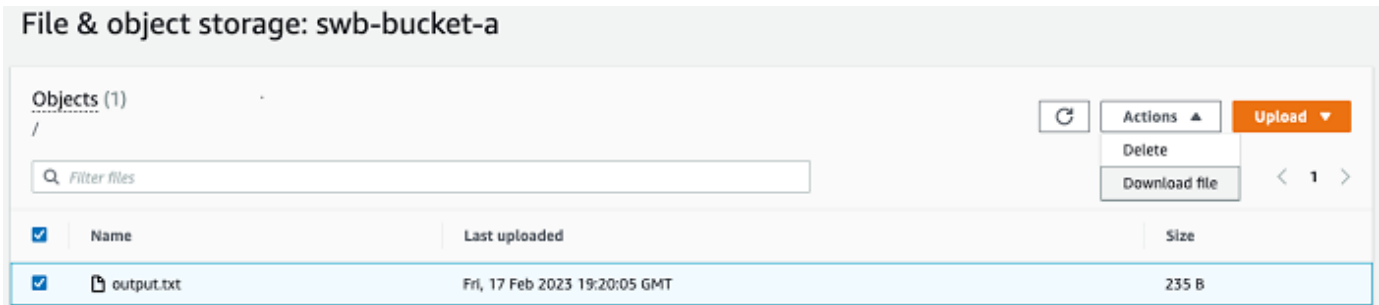
Per caricare file di dimensioni maggiori, puoi utilizzare la funzionalità di caricamento multiparte di Amazon S3 utilizzando il. AWS CLI [Per ulteriori informazioni sulla configurazione delle impostazioni della CLI di S3, consulta Configurazione CLI S3](#). Per ulteriori informazioni sul caricamento multiparte, consulta la [panoramica del caricamento multiparte nella Guida](#) per l'utente di Amazon Simple Storage Service

È supportato il caricamento di una cartella da un computer locale su Snowball Edge utilizzando AWS OpsHub il. Se la dimensione della cartella è molto grande, la lettura della selezione richiede del file/folder tempo. OpsHub Durante OpsHub la lettura dei file e delle cartelle, non viene visualizzato un indicatore dei progressi. Tuttavia, mostra che viene visualizzato un tracker dei progressi all'inizio del processo di caricamento.

Scaricamento di file dallo storage Amazon S3 con AWS OpsHub

Per scaricare un file

1. Nella sezione Gestisci archiviazione file del dashboard scegliere Inizia. Se sul dispositivo sono presenti bucket S3, questi vengono visualizzati nella sezione Bucket della pagina Archiviazione file . Puoi vedere i dettagli di ogni bucket nella pagina.
2. Scegliere il bucket da cui si desidera scaricare i file e passare al file che si desidera scaricare. Scegli uno o più file.



3. Nel menu Operazioni, scegliere Scarica.
4. Scegliere un percorso in cui scaricare il file e scegliere OK.

Eliminazione di file dallo storage Amazon S3 con AWS OpsHub

Se non hai più bisogno di un file, puoi eliminarlo dal tuo bucket Amazon S3.

Per eliminare un file

1. Nella sezione Gestisci archiviazione file del dashboard scegliere Inizia. Se sul dispositivo sono presenti bucket Amazon S3, questi vengono visualizzati nella sezione Bucket della pagina di archiviazione dei file. Puoi vedere i dettagli di ogni bucket nella pagina.
2. Scegli il bucket da cui vuoi eliminare i file e passa al file che vuoi eliminare.
3. Dal menu Actions (Operazioni), scegli Delete (Elimina).
4. Nella finestra di dialogo visualizzata, scegliere Conferma eliminazione.

Gestione dell'interfaccia NFS con AWS OpsHub

Utilizza l'interfaccia Network File System (NFS) per caricare file su Snowball Edge come se il dispositivo fosse una memoria locale del tuo sistema operativo. Ciò consente un approccio più intuitivo al trasferimento dei dati, poiché è possibile utilizzare funzionalità del sistema operativo, come copiare file, trascinarli e rilasciarli o altre funzionalità dell'interfaccia utente grafica. Ogni bucket S3 sul dispositivo è disponibile come endpoint di interfaccia NFS e può essere montato per copiare i dati. L'interfaccia NFS è disponibile per i lavori di importazione.

È possibile utilizzare l'interfaccia NFS se il dispositivo Snowball Edge è stato configurato per includerlo quando è stato creato il processo per ordinare il dispositivo. Se il dispositivo non è configurato per includere l'interfaccia NFS, utilizza l'adattatore S3 o lo storage compatibile con Amazon S3 su Snowball Edge per trasferire i dati. Per ulteriori informazioni sull'adattatore S3,

consulta. [Gestione dello storage degli adattatori Amazon S3 con AWS OpsHub](#) Per ulteriori informazioni sullo storage compatibile con Amazon S3 su Snowball Edge, consulta. [Configura lo storage compatibile con Amazon S3 su Snowball Edge con AWS OpsHub](#)

All'avvio, l'interfaccia NFS utilizza 1 GB di memoria e 1 CPU. Ciò può limitare il numero di altri servizi in esecuzione su Snowball Edge o il numero di istanze EC2 compatibili che possono essere eseguite.

I dati trasferiti tramite l'interfaccia NFS non vengono crittografati durante il transito. Durante la configurazione dell'interfaccia NFS, puoi fornire blocchi CIDR e Snowball Edge limiterà l'accesso all'interfaccia NFS dai computer client con indirizzi in quei blocchi.

I file sul dispositivo verranno trasferiti su Amazon S3 quando verranno restituiti a. AWS Per ulteriori informazioni, consulta [Importazione di lavori in Amazon](#) Edge.

Per ulteriori informazioni sull'utilizzo di NFS con il sistema operativo del computer, consulta la documentazione del sistema operativo in uso.

Tenete a mente i seguenti dettagli quando utilizzate l'interfaccia NFS.

- L'interfaccia NFS fornisce un bucket locale per l'archiviazione dei dati sul dispositivo. Per i lavori di importazione, nessun dato dal bucket locale verrà importato in Amazon S3.
- I nomi dei file sono chiavi oggetto nel bucket S3 locale su Snowball Edge. Il nome chiave è una sequenza di caratteri Unicode la cui codifica UTF-8 è lunga al massimo 1.024 byte. Si consiglia di utilizzare NFSv4 .1 laddove possibile e di codificare i nomi dei file con Unicode UTF-8 per garantire una corretta importazione dei dati. I nomi di file che non sono codificati con UTF-8 potrebbero non essere caricati su S3 o potrebbero essere caricati su S3 con un nome di file diverso a seconda della codifica NFS utilizzata.
- Assicuratevi che la lunghezza massima del percorso del file sia inferiore a 1024 caratteri. Snowball Edge non supporta percorsi di file che superano i 1024 caratteri. Il superamento di questa lunghezza del percorso di file comporterà errori di importazione dei file.
- Per ulteriori informazioni, consulta [Object keys](#) nella Amazon Simple Storage Service User Guide.
- Per i trasferimenti basati su NFS, i metadati standard in stile POSIX verranno aggiunti agli oggetti non appena vengono importati in Amazon S3 da Snowball Edge. Inoltre, vedrai i metadati "x-amz-meta-user-agent aws-datasync" che utilizziamo attualmente AWS DataSync come parte del meccanismo di importazione interno in Amazon S3 per l'importazione di Snowball Edge con l'opzione NFS.
- È possibile trasferire fino a 40 milioni di file utilizzando un solo dispositivo Snowball Edge. Se devi trasferire più di 40 milioni di file in un unico processo, raggruppa i file in batch per ridurre il

numero di file per ogni trasferimento. I singoli file possono essere di qualsiasi dimensione con una dimensione massima di 5 TB per i dispositivi Snowball Edge con l'interfaccia NFS avanzata o l'interfaccia S3.

Puoi anche configurare e gestire l'interfaccia NFS con il client Snowball Edge, uno strumento di interfaccia a riga di comando (CLI). Per ulteriori informazioni, consulta [Gestione dell'interfaccia NFS](#).

Argomenti

- [Avvio del servizio NFS su un sistema operativo Windows](#)
- [Configurazione automatica dell'interfaccia NFS con AWS OpsHub](#)
- [Configurazione manuale dell'interfaccia NFS con AWS OpsHub](#)
- [Gestione degli endpoint NFS su Snowball Edge con AWS OpsHub](#)
- [Montaggio degli endpoint NFS sui computer client](#)
- [Arresto dell'interfaccia NFS con AWS OpsHub](#)

Avvio del servizio NFS su un sistema operativo Windows

Se il computer client utilizza il sistema operativo Windows 10 Enterprise o Windows 7 Enterprise, avvia il servizio NFS sul computer client prima di configurare NFS nell'applicazione. AWS OpsHub

1. Sul computer client, apri Start, scegli Pannello di controllo e scegli Programmi.
2. Scegliere Turn Windows features on or off (Attiva o disattiva funzionalità di Windows).

Note

Per attivare le funzionalità di Windows, potrebbe essere necessario fornire un nome utente e una password di amministratore per il computer.

3. In Servizi per NFS, scegliere Client per NFS e scegliere OK.

Configurazione automatica dell'interfaccia NFS con AWS OpsHub

L'interfaccia NFS non è in esecuzione sul dispositivo Snowball Edge per impostazione predefinita, quindi è necessario avviarla per abilitare il trasferimento dei dati sul dispositivo. Con pochi clic, Snowball Edge può configurare rapidamente e automaticamente l'interfaccia NFS per te. Puoi anche

configurare tu stesso l'interfaccia NFS. Per ulteriori informazioni, consulta [Configurazione manuale dell'interfaccia NFS con AWS OpsHub](#).

1. Nella sezione Trasferisci dati del pannello di controllo scegli Abilita e avvia. Il completamento dell'operazione potrebbe richiedere uno o due minuti.



2. All'avvio del servizio NFS, l'indirizzo IP dell'interfaccia NFS viene visualizzato nella dashboard e la sezione Trasferimento dati indica che il servizio è attivo.
3. Scegli Apri in Explorer (se usi un sistema operativo Windows o Linux) per aprire la condivisione di file nel browser del tuo sistema operativo e iniziare a trasferire i file su Snowball Edge. Puoi copiare e incollare o trascinare i file dal computer client nella condivisione di file. Nel sistema operativo Windows, la condivisione di file ha il seguente aspetto `\\12.123.45.679` (Z:).

Note

Nei sistemi operativi Linux, il montaggio degli endpoint NFS richiede i permessi di root.

Configurazione manuale dell'interfaccia NFS con AWS OpsHub

L'interfaccia NFS non è in esecuzione sul dispositivo Snowball Edge per impostazione predefinita, quindi è necessario avviarla per abilitare il trasferimento dei dati sul dispositivo. È possibile configurare manualmente l'interfaccia NFS fornendo l'indirizzo IP di un'interfaccia di rete virtuale (VNI) in esecuzione sul dispositivo Snowball Edge e limitando l'accesso alla condivisione di file, se necessario. Prima di configurare manualmente l'interfaccia NFS, configura un'interfaccia di rete virtuale (VNI) sul dispositivo Snowball Edge. Per ulteriori informazioni, consulta [Configurazione di rete](#) per istanze di calcolo.

Puoi anche fare in modo che il dispositivo Snowball Edge configuri automaticamente l'interfaccia NFS. Per ulteriori informazioni, consulta [Configurazione automatica dell'interfaccia NFS con AWS OpsHub](#).

1. Nella parte inferiore della sezione Trasferisci dati nel pannello di controllo, scegli Configura manualmente.

- Scegli Abilita e avvia per aprire la procedura guidata Avvia NFS. Il campo Interfaccia fisica di rete viene compilato.

Start NFS

Physical network interface

RJ45: s.ni-8459d6c7273eed333

☒ Create IP address (VNI)

☐ Use existing IP address (VNI)

IP Address assignment

DHCP

☒ Restrict NFS to allowed hosts

☐ Allow all hosts

Allowed hosts

Provide a set of CIDR blocks allowed to connect to the NFS service.

192.0.2.0/24

0.0.0.0/0

Add allowed hosts

Allow instances on this device to access NFS

☒ Enable

Cancel

Start NFS

- Scegli Crea indirizzo IP (VNI) o Utilizza indirizzo IP esistente.

4. Se si sceglie Crea indirizzo IP (VNI), scegliere DHCP o IP statico nella casella di riepilogo Assegnazione indirizzo IP.

 Important

Se si utilizza una rete DHCP, è possibile che l'indirizzo IP dell'interfaccia NFS venga riassegnato dal server DHCP. Ciò può accadere dopo che il dispositivo è stato disconnesso e gli indirizzi IP sono stati riciclati. Se imposti un intervallo di host consentito e l'indirizzo del client cambia, un altro client può ritirare quell'indirizzo. In questo caso, il nuovo cliente avrà accesso alla condivisione. Per evitare ciò, utilizza prenotazioni DHCP o indirizzi IP statici.

Se scegli Usa l'indirizzo IP esistente, scegli un'interfaccia di rete virtuale dalla casella di riepilogo Interfaccia di rete virtuale.

5. Scegli di limitare l'accesso all'interfaccia NFS e fornire un blocco di indirizzi di rete consentiti oppure consenti a qualsiasi dispositivo della rete di accedere all'interfaccia NFS su Snowball Edge.
 - Per limitare l'accesso all'interfaccia NFS su Snowball Edge, scegli Limita NFS agli host consentiti. In Host consentiti inserisci un set di blocchi CIDR. Se desideri consentire l'accesso a più di un blocco CIDR, inserisci un altro set di blocchi. Per rimuovere un set di blocchi, scegli X accanto al campo contenente i blocchi. Scegli Aggiungi host consentiti.

 Note

Se scegli Limita NFS agli host autorizzati e non fornisci blocchi CIDR consentiti, Snowball Edge negherà tutte le richieste di montaggio dell'interfaccia NFS.

- Per consentire a qualsiasi dispositivo della rete di accedere all'interfaccia NFS, scegli Consenti tutti gli host.
6. Per consentire alle istanze EC2 compatibili in esecuzione su Snowball Edge di accedere all'adattatore NFS, scegli Abilita.
 7. Scegli Avvia NFS. Potrebbe volerci circa un paio di minuti al massimo per iniziare.

 Important

Non spegnere Snowball Edge all'avvio dell'interfaccia NFS.

Nella sezione Network File System (NFS) Resources, lo stato dell'interfaccia NFS viene visualizzato come Attivo. È necessario l'indirizzo IP elencato per montare l'interfaccia come storage locale sui computer client.

Gestione degli endpoint NFS su Snowball Edge con AWS OpsHub

Ogni bucket S3 su Snowball Edge è rappresentato come endpoint ed elencato nei percorsi di montaggio. Dopo l'avvio dell'interfaccia NFS, installa un endpoint per trasferire file da o verso quell'endpoint. È possibile montare un solo endpoint alla volta. Per montare un endpoint diverso, smonta prima l'endpoint corrente.

Per montare un endpoint

1. Nella sezione Monta percorsi, effettuate una delle seguenti operazioni per selezionare un endpoint:
 - Nel campo Filtra endpoint, inserisci in tutto o in parte il nome di un bucket per filtrare l'elenco degli endpoint disponibili sulla voce, quindi scegli l'endpoint.
 - Scegli l'endpoint da montare nell'elenco dei percorsi di montaggio.
2. Scegli Mount NFS endpoint. Lo Snowball Edge monta l'endpoint per l'uso.

Per smontare un endpoint

1. Nella sezione Percorsi di montaggio, scegli l'endpoint da smontare.
2. Scegli Unmount endpoint. Snowball Edge smonta l'endpoint e non è più disponibile per l'uso.

 Note

Prima di smontare un endpoint, assicurati che nessun dato venga copiato da o su di esso.

Montaggio degli endpoint NFS sui computer client

Dopo l'avvio dell'interfaccia NFS e il montaggio di un endpoint, monta l'endpoint come archiviazione locale sui computer client.

1. In Mount paths, scegliete l'icona di copia dell'endpoint da montare. Incollala nel tuo sistema operativo durante il montaggio dell'endpoint.
2. Di seguito sono riportati i comandi di montaggio predefiniti per i sistemi operativi Windows, Linux e macOS.

- Windows:

```
mount -o nolock rsize=128 wsize=128 mtype=hard nfs-interface-ip-address:/  
buckets/BucketName *
```

- Linux:

```
mount -t nfs nfs-interface-ip-address:/buckets/BucketName mount_point
```

- macOS:

```
mount -t nfs -o vers=3,rsize=131072,wsize=131072,nolocks,hard,retrans=2 nfs-  
interface-ip-address:/buckets/$bucketname mount_point
```

Arresto dell'interfaccia NFS con AWS OpsHub

Arresta l'interfaccia NFS sul dispositivo Snowball Edge al termine del trasferimento dei file da o verso il dispositivo.

1. Dal pannello di controllo scegli Servizi quindi Storage di file.
2. Nella pagina Storage di file scegli Disabilita trasferimento dati. In genere occorrono fino a 2 minuti prima che gli endpoint NFS scompaiano dalla dashboard.

Riavvio del dispositivo con AWS OpsHub

Segui questi passaggi per AWS OpsHub riavviare il dispositivo Snow.

⚠ Important

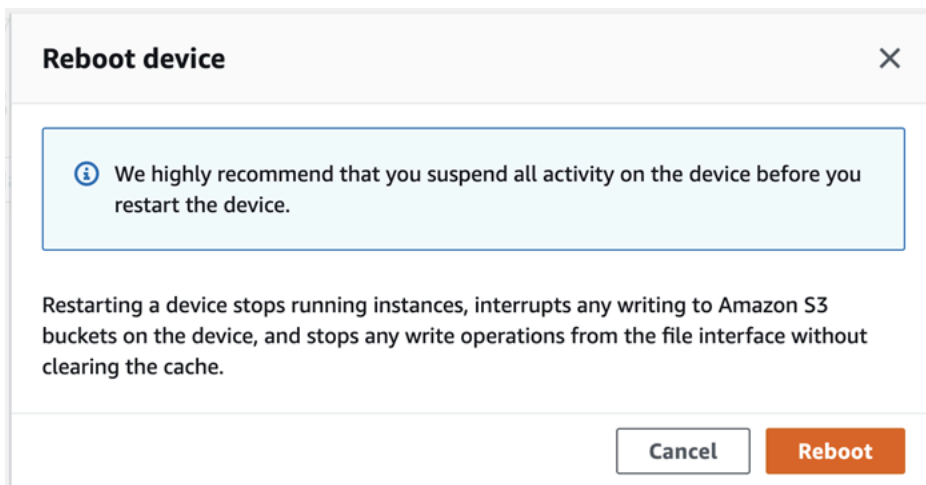
Ti consigliamo vivamente di sospendere tutte le attività sul dispositivo prima di riavviarlo. Il riavvio di un dispositivo interrompe l'esecuzione delle istanze e interrompe la scrittura sui bucket Amazon S3 sul dispositivo.

Per riavviare un dispositivo

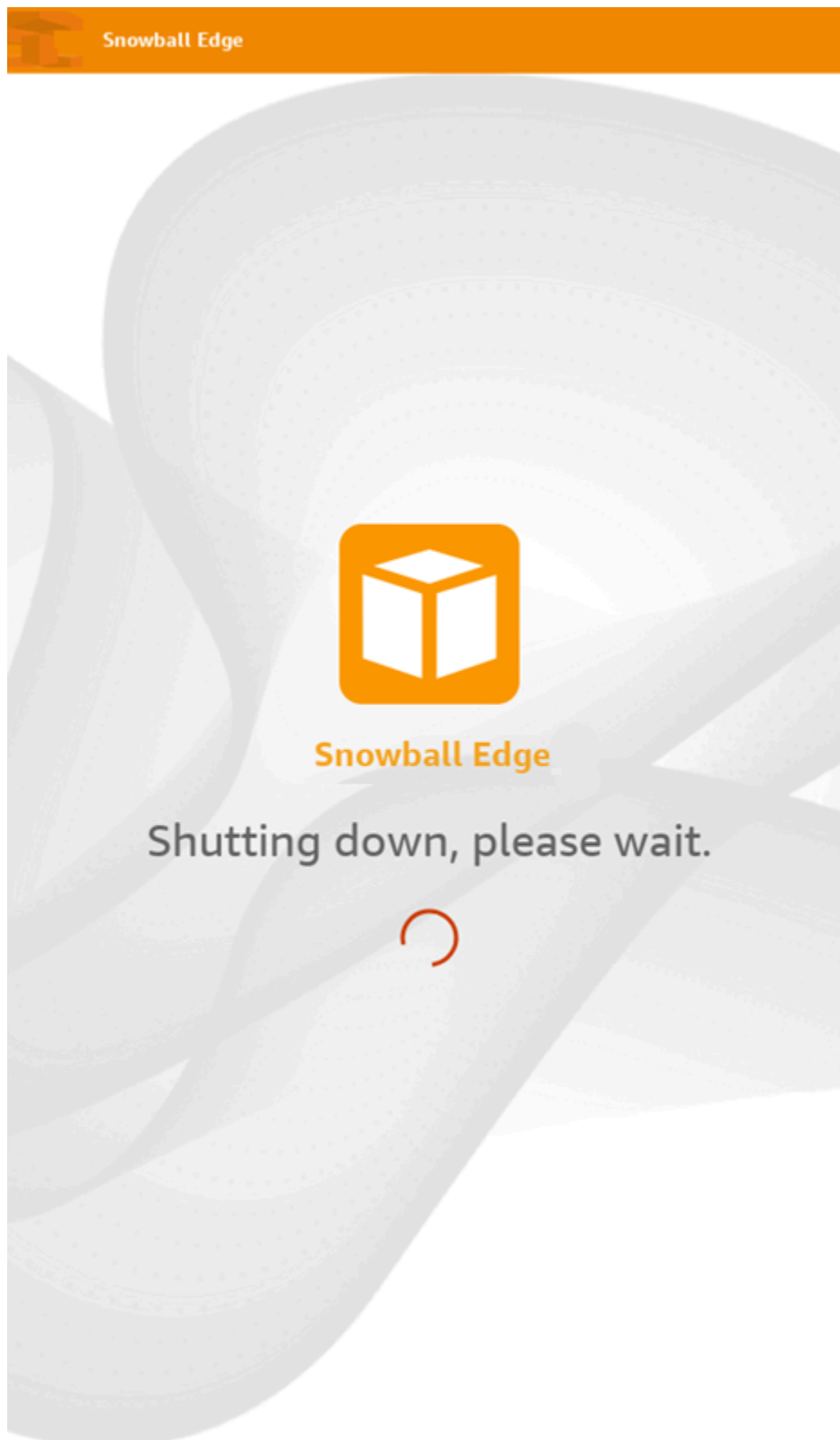
1. Nella AWS OpsHub dashboard, trova il tuo dispositivo in Dispositivi. Quindi scegli il dispositivo per aprire la pagina dei dettagli del dispositivo.
2. Scegli il menu Device Power, quindi scegli Riavvia. Viene visualizzata una finestra di dialogo.



3. Nella finestra di dialogo, scegli Riavvia. Il dispositivo inizia a riavviarsi.



Mentre il dispositivo si spegne, lo schermo LCD visualizza un messaggio che indica che il dispositivo si sta spegnendo.



Gestione dei profili con AWS OpsHub

È possibile creare un profilo per l'archiviazione persistente delle credenziali nel file system locale. Utilizzando AWS OpsHub, è possibile creare un nuovo profilo ogni volta che si sblocca il dispositivo utilizzando l'indirizzo IP del dispositivo, il codice di sblocco e il file manifest.

Puoi anche utilizzare il client Snowball Edge per creare un profilo in qualsiasi momento. Vedi [Configurazione di un profilo per il client Snowball Edge](#).

Per creare un profilo

1. Sblocca il dispositivo localmente e accedi seguendo le istruzioni riportate in. [Sblocco di un dispositivo Snowball Edge con AWS OpsHub](#)
2. Assegna un nome al profilo e scegli Salva nome profilo.

Spegnimento del dispositivo con AWS OpsHub

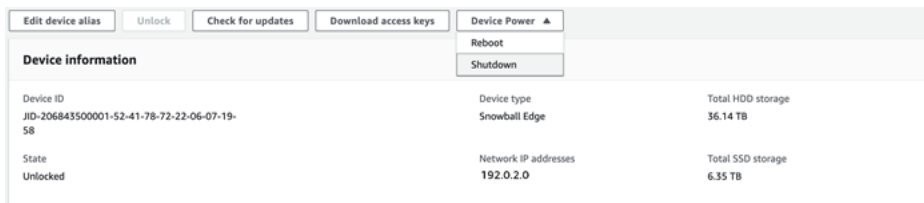
Segui questi passaggi per AWS OpsHub spegnere il dispositivo Snow.

Important

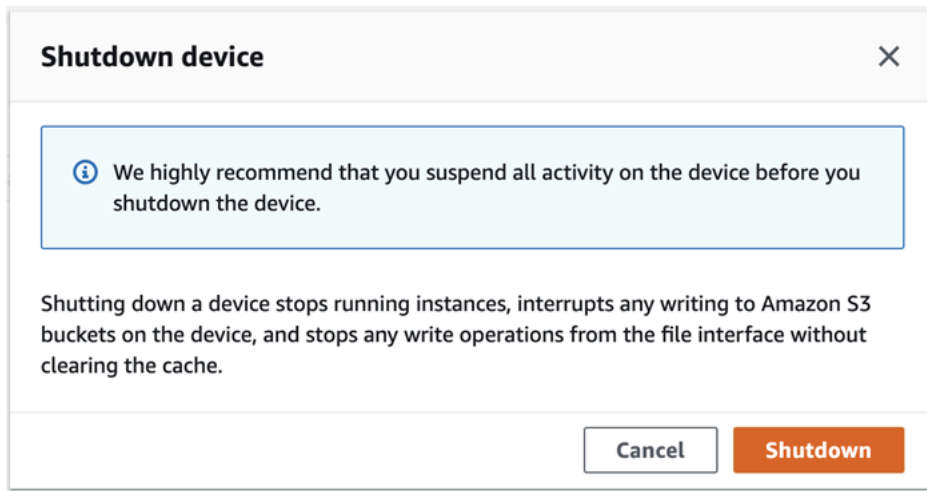
Ti consigliamo vivamente di sospendere tutte le attività sul dispositivo prima di spegnerlo. L'arresto di un dispositivo interrompe l'esecuzione delle istanze e interrompe la scrittura sui bucket Amazon S3 sul dispositivo.

Per spegnere un dispositivo

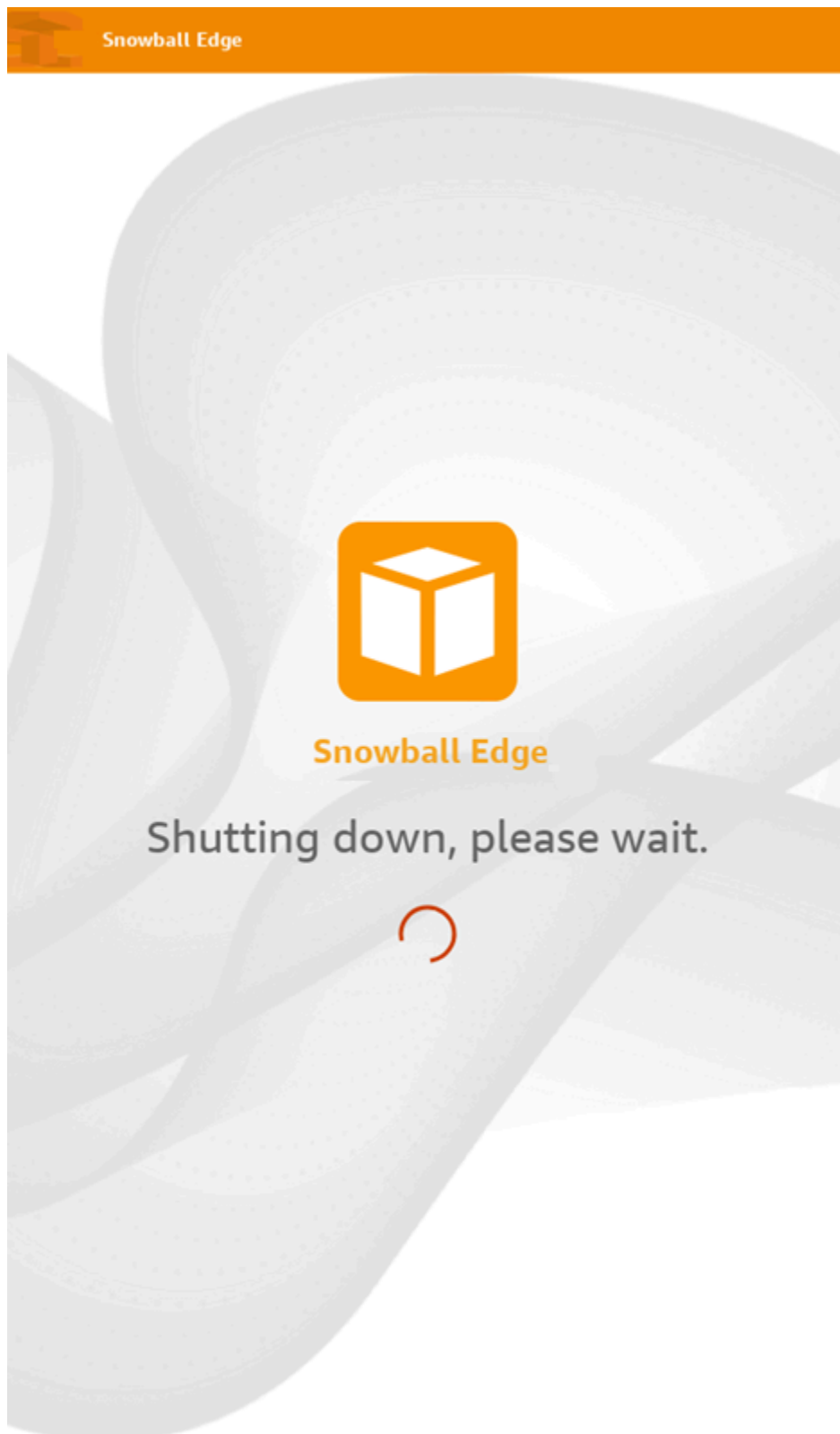
1. Nella AWS OpsHub dashboard, trova il tuo dispositivo in Dispositivi. Quindi scegli il dispositivo per aprire la pagina dei dettagli del dispositivo.
2. Scegli il menu Device Power, quindi scegli Shutdown. Viene visualizzata una finestra di dialogo.



3. Nella finestra di dialogo, scegli Shutdown. Il dispositivo inizia a spegnersi.



Mentre il dispositivo si spegne, lo schermo LCD visualizza un messaggio che indica che il dispositivo si sta spegnendo.

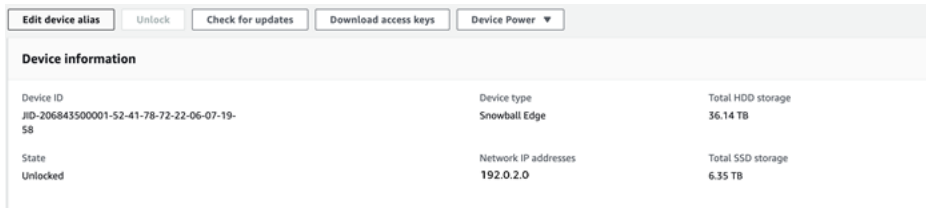


Modifica dell'alias del dispositivo con AWS OpsHub

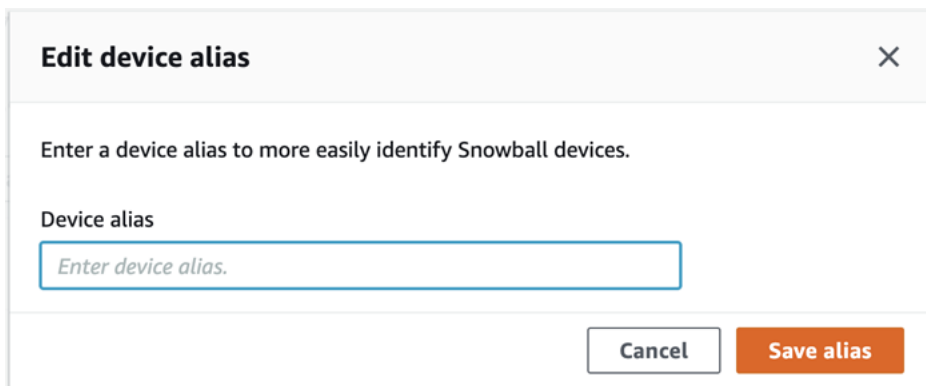
Segui questi passaggi per modificare l'alias del dispositivo utilizzando AWS OpsHub

Per modificare l'alias del dispositivo

1. Nella AWS OpsHub dashboard, trova il tuo dispositivo nella sezione Dispositivi. Scegliere il dispositivo per aprire la pagina dei dettagli del dispositivo.
2. Scegliere la scheda Modifica alias dispositivo .



3. Per Alias dispositivo, immettere un nuovo nome e scegliere Salva alias.



Gestione dei certificati a chiave pubblica tramite OpsHub

Puoi interagire in modo sicuro con AWS i servizi in esecuzione su un dispositivo Snowball Edge o su un cluster di dispositivi Snowball Edge tramite il protocollo HTTPS fornendo un certificato a chiave pubblica. Puoi utilizzare il protocollo HTTPS per interagire con AWS servizi come IAM, Amazon, adattatore S3 EC2, storage compatibile con Amazon S3 su Snowball Edge, Amazon EC2 Systems Manager AWS STS e su dispositivi Snowball Edge. Nel caso di un cluster di dispositivi, è richiesto un singolo certificato che può essere generato da qualsiasi dispositivo del cluster. Una volta che un dispositivo Snowball Edge genera il certificato e lo sblocca, puoi utilizzare i comandi del client Snowball Edge per elencare, ottenere ed eliminare il certificato.

Un dispositivo Snowball Edge genera un certificato quando si verificano i seguenti eventi:

- Il dispositivo o il cluster Snowball Edge viene sbloccato per la prima volta.
- Il dispositivo o il cluster Snowball Edge viene sbloccato dopo l'eliminazione del certificato (utilizzando il `delete-certificate` comando o Rinnova certificato in). AWS OpsHub
- Il dispositivo o il cluster Snowball Edge viene riavviato e sbloccato dopo la scadenza del certificato.

Ogni volta che viene generato un nuovo certificato, il vecchio certificato non è più valido. Un certificato è valido per un periodo di un anno dal giorno in cui è stato generato.

Puoi anche utilizzare il client Snowball Edge per gestire i certificati a chiave pubblica. Per ulteriori informazioni, consulta [Gestione dei certificati a chiave pubblica](#).

Argomenti

- [Scarica il certificato a chiave pubblica utilizzando OpsHub](#)
- [Rinnovo del certificato a chiave pubblica utilizzando OpsHub](#)

Scarica il certificato a chiave pubblica utilizzando OpsHub

Puoi scaricare il certificato a chiave pubblica attivo sul tuo computer.

1. Nella AWS OpsHub dashboard, individua il tuo dispositivo in Dispositivi. Scegliere il dispositivo per aprire la pagina dei dettagli del dispositivo.
2. Nella pagina dei dettagli del dispositivo, scegli il menu Gestisci certificato. Dal menu, scegli Scarica certificato.
3. Viene visualizzata una finestra in cui puoi assegnare un nome al file del certificato da scaricare e scegliere la posizione sul computer in cui verrà scaricato. Scegli Save (Salva).

Rinnovo del certificato a chiave pubblica utilizzando OpsHub

Prima di rinnovare il certificato a chiave pubblica, interrompi tutti i trasferimenti di dati da o verso il dispositivo Snowball Edge e interrompi quelli compatibili EC2 in esecuzione. Per ulteriori informazioni, consulta la sezione [Arresto di un'istanza EC2 compatibile con Amazon](#) in questa guida.

1. Nella AWS OpsHub dashboard, individua il tuo dispositivo in Dispositivi. Scegliere il dispositivo per aprire la pagina dei dettagli del dispositivo.
2. Nella pagina dei dettagli del dispositivo, scegli il menu Gestisci certificato. Dal menu, scegli Rinnova certificato.

3. Nella finestra Rinnova certificato, entra **Renew** nel campo e scegli Rinnova. Il dispositivo Snowball Edge elimina il certificato a chiave pubblica esistente e riavvia il dispositivo o il cluster.

Renew certificate



The following certificate will be deleted:

arn:aws:snowball-device:::certificate/example



Stop all activity on the Snow device or cluster before proceeding.

Clicking **Renew** will automatically reboot **all devices attached to this certificate** and terminate any ongoing data transfers and other running processes. A new certificate will be generated when you unlock the device or cluster after it reboots.

To confirm, enter **Renew** in the field and then choose **Renew**

Cancel

Renew

Ricevere aggiornamenti per Snowball Edge

Puoi verificare la presenza di aggiornamenti per il tuo dispositivo e installarli. versione.

Aggiornamento del dispositivo

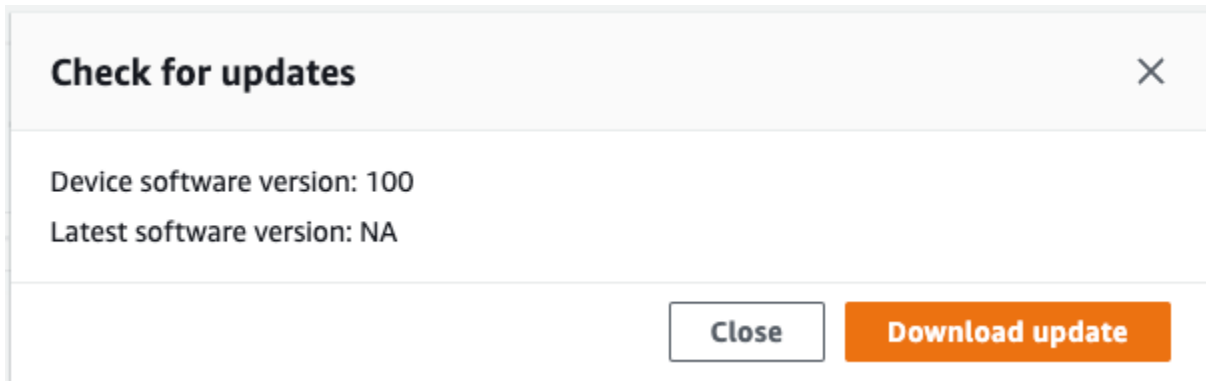
Segui questi passaggi per AWS OpsHub aggiornare il tuo dispositivo Snow.

Per aggiornare il dispositivo

1. Nella AWS OpsHub dashboard, trova il tuo dispositivo nella sezione Dispositivi. Scegliere il dispositivo per aprire la pagina dei dettagli del dispositivo.

2. Scegliere la scheda Verifica aggiornamenti .

La pagina Verifica aggiornamenti visualizza la versione software corrente sul dispositivo e la versione software più recente, se presente.

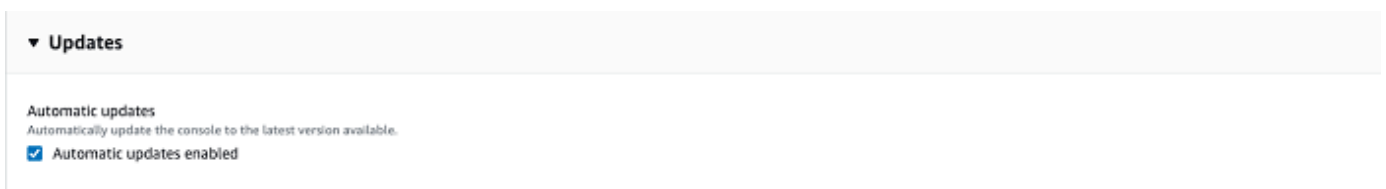


3. Se è disponibile un aggiornamento, scegli Scarica aggiornamento. Altrimenti, scegliere Close (Chiudi).

Aggiornamento dell' AWS OpsHub applicazione

Per verificare che gli aggiornamenti automatici siano abilitati per AWS OpsHub

1. Nella AWS OpsHub dashboard, scegli Preferenze.
2. Apri la scheda Aggiornamenti.
3. Verifica che sia selezionata l'opzione Aggiornamenti automatici abilitati. L'aggiornamento automatico è abilitato per impostazione predefinita.



Se l'opzione Aggiornamenti automatici abilitati non è selezionata, non sarà disponibile la versione più recente dell' AWS OpsHub applicazione.

Automatizzazione delle attività di gestione con AWS OpsHub

Puoi utilizzarlo AWS OpsHub per automatizzare le attività operative che esegui frequentemente su Snowball Edge. Puoi creare un'attività per le azioni ricorrenti che potresti voler eseguire sulle risorse,

come il riavvio di server virtuali, l'arresto di istanze EC2 compatibili con Amazon e così via. Fornisci un documento di automazione che esegue in modo sicuro le attività operative ed esegue l'operazione sulle risorse in blocco. AWS È inoltre possibile pianificare flussi di lavoro IT comuni.

Note

L'automazione delle attività non è supportata nei cluster.

Per utilizzare le attività, è necessario avviare prima il servizio Amazon EC2 Systems Manager. Per ulteriori informazioni, consulta [Attivazione della gestione dei dispositivi Snowball Edge su Snowball Edge](#).

Argomenti

- [Creazione e avvio di un'attività con AWS OpsHub](#)
- [Visualizzazione dei dettagli di un'attività in AWS OpsHub](#)
- [Eliminazione di un'attività in AWS OpsHub](#)

Creazione e avvio di un'attività con AWS OpsHub

Quando si crea un'attività, specificare i tipi di risorse su cui eseguire l'attività e quindi fornire un documento di attività contenente le istruzioni che eseguono l'attività. Il documento attività è in formato YAML o JSON. È quindi necessario fornire i parametri necessari per l'attività e avviare l'attività.

Per creare un'attività

1. Nella sezione Attività di avvio del dashboard scegliere Inizia per aprire la pagina Attività . Se sono state create attività, queste vengono visualizzate in Attività.
2. Scegliere Crea attività e fornire i dettagli per l'attività.
3. Per Nome ruolo: immettere un nome univoco per la tabella.

Tip

Il nome deve contenere da 3 a 128 caratteri. I caratteri validi sono a-z, A-Z, 0-9, ., _ e -.

4. Facoltativamente, è possibile scegliere un tipo di destinazione dall'elenco Tipo di destinazione facoltativo. Questo è il tipo di risorsa su cui si desidera eseguire l'attività.

Ad esempio, puoi specificare **/AWS::EC2::Instance** che le attività devono essere eseguite su un'istanza EC2 compatibile con Amazon o / su tutti i tipi di risorse.

5. Nella sezione Contenuto, scegli YAML o JSON e fornisci lo script che esegue l'operazione. Sono disponibili due opzioni, il formato YAML o JSON. Per alcuni esempi, consulta [Esempi di attività in AWS OpsHub](#).
6. Scegli Create (Crea). L'attività creata viene quindi visualizzata nella pagina Attività .

Avviare un'attività

1. Nella sezione Attività di avvio del dashboard scegliere Inizia per aprire la pagina Attività . Le attività vengono visualizzate in Attività.
2. Scegliere l'attività per aprire la pagina Attività Start.
3. Scegliere Esecuzione semplice da eseguire sulle destinazioni.

Scegliere Controllo frequenza per un'esecuzione più sicura su più destinazioni e per definire soglie di concorrenza e di errore. Per questa opzione, si forniscono le informazioni aggiuntive di destinazione e soglia di errore nella sezione Controllo frequenza .

4. Fornire i parametri di input richiesti e scegliere Avvia attività.

Lo stato dell'attività è In sospeso e cambia in Successo quando l'attività è stata eseguita correttamente.

Esempi di attività in AWS OpsHub

L'esempio seguente riavvia un'istanza EC2 compatibile con Amazon. Richiede due parametri di input: endpoint e instance ID.

Esempio YAML

```
description: Restart EC2 instance
schemaVersion: '0.3'
parameters:
  Endpoint:
    type: String
    description: (Required) EC2 Service Endpoint URL
  Id:
```

```

    type: String
    description: (Required) Instance Id
mainSteps:
- name: restartInstance
  action: aws:executeScript
  description: Restart EC2 instance step
  inputs:
    Runtime: python3.7
    Handler: restart_instance
    InputPayload:
      Endpoint: "{{ Endpoint }}"
      Id: "{{ Id }}"
    TimeoutSeconds: 30
  Script: |-
    import boto3
    import time
    def restart_instance(payload, context):
        ec2_endpoint = payload['Endpoint']
        instance_id = payload['Id']
        ec2 = boto3.resource('ec2', endpoint_url=ec2_endpoint)
        instance = ec2.Instance(instance_id)
        if instance.state['Name'] != 'stopped':
            instance.stop()
            instance.wait_until_stopped()
        instance.start()
        instance.wait_until_running()
        return {'InstanceState': instance.state}

```

Esempio JSON

```

{
  "description" : "Restart EC2 instance",
  "schemaVersion" : "0.3",
  "parameters" : {
    "Endpoint" : {
      "type" : "String",
      "description" : "(Required) EC2 Service Endpoint URL"
    },
    "Id" : {
      "type" : "String",
      "description" : "(Required) Instance Id"
    }
  }
}

```

```

},
"mainSteps" : [ {
  "name" : "restartInstance",
  "action" : "aws:executeScript",
  "description" : "Restart EC2 instance step",
  "inputs" : {
    "Runtime" : "python3.7",
    "Handler" : "restart_instance",
    "InputPayload" : {
      "Endpoint" : "{{ Endpoint }}",
      "Id" : "{{ Id }}"
    }
  },
  "TimeoutSeconds" : 30,
  "Script" : "import boto3\nimport time\ndef restart_instance(payload, context):\n\n    ec2_endpoint = payload['Endpoint']\n    instance_id = payload['Id']\n    ec2 = boto3.resource('ec2', endpoint_url=ec2_endpoint)\n    instance = ec2.Instance(instance_id)\n    if instance.state['Name'] != 'stopped':\n    instance.stop()\n    instance.wait_until_stopped()\n    instance.start()\n    instance.wait_until_running()\n    return {'InstanceState': instance.state}"
}
} ]
}

```

Visualizzazione dei dettagli di un'attività in AWS OpsHub

È possibile visualizzare i dettagli di un'attività di gestione, ad esempio la descrizione e i parametri necessari per eseguire l'attività.

Per visualizzare i dettagli di un'attività

1. Nella sezione Attività di avvio del dashboard scegliere Inizia per aprire la pagina Attività .
2. Nella pagina Attività individuare e scegliere l'attività di cui si desidera visualizzare i dettagli.
3. Scegli Visualizza dettagli e scegli una delle schede per visualizzare i dettagli. Ad esempio, la scheda Parametri mostra i parametri di input nello script.

Eliminazione di un'attività in AWS OpsHub

Attenersi alla seguente procedura per eliminare un'attività di gestione.

Per eliminare un'attività

1. Nella sezione Attività di avvio del dashboard scegliere Inizia per aprire la pagina Attività .
2. Individuare l'attività che si desidera eliminare. Scegliere l'attività, quindi scegliere Elimina.

Impostazione dei time server NTP per il dispositivo con AWS OpsHub

Segui questi passaggi per visualizzare e aggiornare i server orari con cui il dispositivo deve sincronizzare l'ora.

Per controllare le fonti di orario

1. Nella AWS OpsHub dashboard, trova il tuo dispositivo nella sezione Dispositivi. Scegliere il dispositivo per aprire la pagina dei dettagli del dispositivo.
2. Nella tabella Sorgenti orarie verrà visualizzato un elenco di fonti di orario con cui il dispositivo sta sincronizzando l'ora.

La tabella Sorgenti orarie è composta da quattro colonne:

- Indirizzo: il nome DNS/indirizzo IP della sorgente temporale
- Stato: lo stato attuale della connessione tra il dispositivo e quella fonte di tempo, ci sono 5 stati possibili:
 - ATTUALE: La fonte di orario è attualmente utilizzata per sincronizzare l'ora
 - COMBINATO: La fonte dell'ora è combinata con la fonte corrente
 - ESCLUSA: la fonte di tempo è esclusa dall'algoritmo di combinazione
 - PERSO: la connessione con la fonte dell'ora è stata interrotta
 - INDISPONIBILITÀ: fonte temporale non valida in cui l'algoritmo di combinazione è stato considerato falso o presenta troppa variabilità
- Tipo: Le fonti NTP (Network Time Protocol) possono essere un server o un peer. Un server può essere impostato dall'utente utilizzando il update-time-server comando, mentre un peer

può essere configurato solo utilizzando altri dispositivi Snowball Edge nel cluster e viene configurato automaticamente quando il cluster viene associato.

- Strato: lo strato della fonte. Stratum 1 indica una sorgente con un orologio di riferimento collegato localmente. Una sorgente sincronizzata con una sorgente Stratum 1 è impostata su Stratum 2. Una sorgente sincronizzata con una sorgente Stratum 2 viene impostata su Stratum 3 e così via.

Per aggiornare i time server

1. Nella AWS OpsHub dashboard, trova il tuo dispositivo in Dispositivi. Scegliere il dispositivo per aprire la pagina dei dettagli del dispositivo.
2. Nella tabella Sorgenti orarie verrà visualizzato un elenco di fonti di orario con cui il dispositivo sta sincronizzando l'ora.
3. Scegli Aggiorna server orari nella tabella Sorgenti orarie.
4. Fornisci il nome DNS o l'indirizzo IP dei time server con cui desideri che il dispositivo sincronizzi l'ora e scegli Aggiorna.

Update time servers

Update time servers on JID-206843500001-52-41-78-72-22-06-07-19-58

Overriding Existing Settings
Updating the time servers will override existing time server settings.

NTP server IP address or DNS name

You can add up to 4 more time servers.

Tipi di dispositivi NTP e versioni software supportati

NTP non è disponibile su nessun tipo di dispositivo di archiviazione e calcolo versione 2. Tuttavia, i tipi di dispositivi di storage ed elaborazione Snowball Edge versione 3 con versione software 77 o successiva supportano NTP. Per verificare se NTP è abilitato, utilizzate il comando Snowball Edge CLI. `describe-time-sources`

Configurazione e utilizzo del client Snowball Edge

Lo Snowball Edge Client è uno strumento di interfaccia a riga di comando (CLI) AWS che puoi utilizzare per lavorare con Snowball Edge o un cluster di Snowball Edge. Puoi utilizzare il client per sbloccare uno Snowball Edge o un cluster di dispositivi, configurare Snowball Edge, avviare e interrompere i servizi sui dispositivi e trasferire dati da o verso i dispositivi. Il client Snowball Edge è compatibile con i computer che eseguono sistemi operativi Linux, macOS e Windows.

Argomenti

- [Scaricamento e installazione del client Snowball Edge](#)
- [Configurazione di un profilo per il client Snowball Edge](#)
- [Ricerca della versione client Snowball Edge](#)
- [Ottenere le credenziali per uno Snowball Edge](#)
- [Avvio di un servizio su Snowball Edge](#)
- [Interruzione di un servizio su Snowball Edge](#)
- [Visualizzazione e download dei log da Snowball Edge](#)
- [Visualizzazione dello stato di uno Snowball Edge](#)
- [Visualizzazione dello stato dei servizi in esecuzione su Snowball Edge](#)
- [Visualizzazione dello stato delle funzionalità di Snowball Edge](#)
- [Impostazione dei time server per Snowball Edge](#)
- [Ottenere un codice QR per convalidare i tag NFC di Snowball Edge](#)
- [Aggiornamento delle dimensioni MTU](#)

Scaricamento e installazione del client Snowball Edge

[È possibile scaricare il client Snowball Edge da AWS Snowball Edge Resources.](#) In quella pagina puoi trovare il pacchetto di installazione per il tuo sistema operativo.

Installa e configura il client seguendo le istruzioni riportate di seguito.

Linux

Note

Il client Snowball Edge è supportato solo su distribuzioni Linux a 64 bit.

1. Estrarre il file `snowball-client-linux.tar.gz`. Crea la struttura delle `/snowball-client-linux-build_number/bin` cartelle e vi estrae i file.
2. Esegui i seguenti comandi per configurare le cartelle.

```
chmod u+x snowball-client-linux-build_number/bin/snowballEdge
```

```
chmod u+x snowball-client-linux-build_number/jre/bin/java
```

3. `/snowball-client-linux-build_number/bin` Aggiungila alla variabile di ambiente `$PATH` del sistema operativo per eseguire i comandi del client Snowball Edge da qualsiasi directory. Per ulteriori informazioni, consulta la documentazione del sistema operativo del dispositivo o della shell.

macOS

1. Estrarre il file `snowball-client-mac.tar.gz`. Crea la struttura delle `/snowball-client-linux-build_number/bin` cartelle e vi estrae i file.
2. Esegui i seguenti comandi per configurare le cartelle.

```
chmod u+x snowball-client-mac-build_number/bin/snowballEdge
```

```
chmod u+x snowball-client-mac-build_number/jre/bin/java
```

3. `/snowball-client-mac-build_number/bin` Aggiungila alla variabile di ambiente `$PATH` del sistema operativo per eseguire i comandi del client Snowball Edge da qualsiasi directory. Per ulteriori informazioni, consulta la documentazione del sistema operativo del dispositivo o della shell.

Windows

Il client è confezionato come file Microsoft Software Installer (MSI). Apri il file e segui le istruzioni della procedura guidata di installazione. Una volta installato il client, è possibile eseguirlo da qualsiasi directory senza alcuna preparazione aggiuntiva.

Configurazione di un profilo per il client Snowball Edge

Ogni volta che esegui un comando per il client Snowball Edge, fornisci il file manifest, il codice di sblocco e l'indirizzo IP di Snowball Edge. Invece di fornirli ogni volta che si esegue un comando, è possibile utilizzare il `configure` comando per memorizzare il percorso del file manifest, il codice di sblocco di 29 caratteri e l'endpoint (l'indirizzo IP di Snowball Edge) come profilo. Dopo la configurazione, è possibile utilizzare i comandi del client Snowball Edge senza dover inserire manualmente questi valori per ogni comando, includendo il nome del profilo nel comando. Dopo aver configurato il client Snowball Edge, le informazioni vengono salvate in formato JSON di testo normale in `home directory/.aws/snowball/config/snowball-edge.config`. Assicurati che l'ambiente sia configurato per consentirti di creare questo file.

Important

Chiunque possa accedere al file di configurazione può accedere ai dati sui dispositivi o sui cluster Snowball Edge. La gestione del controllo dell'accesso locale per questo file è una delle responsabilità amministrative.

Puoi anche utilizzarli AWS OpsHub per creare un profilo. I profili creati in AWS OpsHub possono essere utilizzati con il client Snowball Edge, mentre i profili creati in AWS OpsHub possono essere utilizzati con lo Snowball Edge Client. Per ulteriori informazioni, consulta [Gestione dei](#) profili.

Per creare un profilo

1. Immettete il comando nell'interfaccia a riga di comando del sistema operativo in uso. Il valore del `profile-name` parametro è il nome del profilo. Lo fornirai in futuro quando eseguirai i comandi del client Snowball Edge.

```
snowballEdge configure --profile profile-name
```

2. Il client Snowball Edge richiederà all'utente di specificare ogni parametro. Quando richiesto, inserisci le informazioni relative al tuo ambiente e a Snowball Edge.

Note

Il valore del endpoint parametro è l'indirizzo IP di Snowball Edge, preceduto da. `https://` È possibile individuare l'indirizzo IP del dispositivo Snowball Edge sullo schermo LCD sulla parte anteriore del dispositivo.

Example uscita del comando **configure**

```
Configuration will stored at home directory\.aws\snowball\config\snowball-  
edge.config  
Snowball Edge Manifest Path: /Path/to/manifest/file  
Unlock Code: 29 character unlock code  
Default Endpoint: https://192.0.2.0
```

Il client Snowball Edge verificherà che il codice di sblocco sia corretto per il file manifest. Se non corrispondono, il comando si interrompe e non crea il profilo. Controlla il codice di sblocco e il file manifest ed esegui nuovamente il comando.

Per utilizzare il profilo, includi `--profile profile-name` dopo la sintassi del comando.

Se utilizzi più Snowball Edge autonomi, puoi creare un profilo per ognuno di essi. Per creare un altro profilo, esegui nuovamente il `configure` comando, fornisci un valore diverso per il `--profile` parametro e fornisci le informazioni per un altro dispositivo.

Example Esempio di file **snowball-edge.config**

Questo esempio mostra un file di profilo contenente tre profili:

SnowDevice1profileSnowDevice2profile, e. SnowDevice3profile

```
{
  "version": 1,
  "profiles": [
    {
      "SnowDevice1profile": {
        "name": "SnowDevice1profile",
        "jobId": "JID12345678-136f-45b4-b5c2-847db8adc749",
        "unlockCode": "db223-12345-dbe46-44557-c7cc2",
        "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-136f-45b4-b5c2-847db8adc749_manifest-1670622989203.bin",
        "defaultEndpoint": "https://10.16.0.1",
        "isCluster": false,
        "deviceIps": []
      },
      "SnowDevice2profile": {
        "name": "SnowDevice2profile",
        "jobId": "JID12345678-fdb2-436a-a4ff-7c510dec1bae",
        "unlockCode": "b893b-54321-0f65c-6c5e1-7f748",
        "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-fdb2-436a-a4ff-7c510dec1bae_manifest-1670623746908.bin",
        "defaultEndpoint": "https://10.16.0.2",
        "isCluster": false,
        "deviceIps": []
      },
      "SnowDevice3profile": {
        "name": "SnowDevice3profile",
        "jobId": "JID12345678-c384-4a5e-becd-ab5f38888463",
        "unlockCode": "64c89-13524-4d054-13d93-c1b80",
        "manifestPath": "C:\\Users\\Administrator\\.aws\\ops-hub\\manifest\\JID12345678-c384-4a5e-becd-ab5f38888463_manifest-1670623999136.bin",
        "defaultEndpoint": "https://10.16.0.3",
        "isCluster": false,
        "deviceIps": []
      }
    ]
  }
}
```

Per modificare o eliminare i profili, modificate il file di profilo in un editor di testo.

Per modificare un profilo

1. In un editor di testo, apri `snowball-edge.config` da `home directory\aws\snowball\config`.

 Note

Assicurati che il tuo ambiente sia configurato per consentirti di accedere per leggere e scrivere questo file.

2. Modifica il file in base alle esigenze. Ad esempio, per modificare l'indirizzo IP di Snowball Edge associato al profilo, modifica la `defaultEndpoint` voce.
3. Salva e chiudi il file.

Per eliminare un profilo

1. Utilizzando un editor di testo, apri `snowball-edge.config` da `home directory\aws\snowball\config`.

 Note

Assicurati che il tuo ambiente sia configurato per consentirti di accedere per leggere e scrivere questo file.

2. Elimina la riga che contiene il nome del profilo, le parentesi curve `{ }` che seguono il nome del profilo e il contenuto tra quelle parentesi.
3. Salva e chiudi il file.

Ricerca della versione client Snowball Edge

Utilizzate il `version` comando per visualizzare la versione del client Snowball Edge Command Line Interface (CLI).

Utilizzo

```
snowballEdge version
```

Output di esempio

```
Snowball Edge client version: 1.2.0 Build 661
```

Ottenere le credenziali per uno Snowball Edge

Utilizzando i `snowballEdge get-secret-access-key` comandi `snowballEdge list-access-keys` and, puoi ottenere le credenziali dell'utente amministratore del tuo account Account AWS su Snowball Edge. Puoi utilizzare queste credenziali per creare AWS Identity and Access Management (utenti IAM) e ruoli e per autenticare le tue richieste quando usi AWS CLI o con un SDK. AWS Queste credenziali sono associate solo a un singolo job per Snowball Edge e possono essere utilizzate solo sul dispositivo o sul cluster di dispositivi. Il dispositivo o i dispositivi non dispongono di autorizzazioni IAM in Cloud AWS

Note

Se utilizzi Snowball Edge, devi usare queste credenziali quando configuri la CLI. AWS CLI Per informazioni sulla configurazione delle credenziali per AWS CLI, consulta [Configuring the](#) nella Guida per l'utente. AWS CLI AWS Command Line Interface

Utilizzo (client Snowball Edge configurato)

```
snowballEdge list-access-keys
```

Example Output

```
{
  "AccessKeyIds" : [ "AKIAIOSFODNN7EXAMPLE" ]
}
```

Utilizzo (client Snowball Edge configurato)

```
snowballEdge get-secret-access-key --access-key-id Access Key
```

Example Output

```
[snowballEdge]  
aws_access_key_id = AKIAIOSFODNN7EXAMPLE  
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
```

Avvio di un servizio su Snowball Edge

I dispositivi Snowball Edge supportano più servizi. Questi includono istanze di calcolo, l'interfaccia Network File System (NFS), Snowball Edge Device Management e AWS IoT Greengrass. Il servizio adattatore Amazon S3 EC2 AWS STS, Amazon e IAM vengono avviati per impostazione predefinita e non possono essere interrotti o riavviati. Tuttavia, l'interfaccia NFS, Snowball Edge Device Management, AWS IoT Greengrass può essere avviata utilizzando il relativo ID di servizio con `start-service` il comando. Per ottenere l'ID servizio per ogni servizio, puoi utilizzare il comando `list-services`.

Prima di eseguire questo comando, crea una singola interfaccia di rete virtuale da associare al servizio che intendi avviare. Per ulteriori informazioni, consulta [Creazione di un'interfaccia di rete virtuale su Snowball Edge](#).

```
snowballEdge start-service --service-id service_id --virtual-network-interface-  
arns virtual-network-interface-arn --profile profile-name
```

Example output del comando **start-service**

```
Starting the AWS service on your Snowball Edge. You can determine the status of the AWS  
service using the describe-service command.
```

Interruzione di un servizio su Snowball Edge

Per interrompere l'esecuzione di un servizio su Snowball Edge, puoi usare il `stop-service` comando.

L'adattatore Amazon S3 EC2, AWS STS Amazon e i servizi IAM non possono essere interrotti.

Warning

La perdita di dati può verificarsi se il servizio Network File System (NFS) viene interrotto prima che i dati rimanenti nel buffer vengano scritti sul dispositivo. Per ulteriori informazioni sull'utilizzo del servizio NFS, vedere. [Gestione dell'interfaccia NFS su Snowball Edge](#)

Note

L'interruzione dello storage compatibile con Amazon S3 sul servizio Snowball Edge disabilita l'accesso ai dati archiviati nei bucket S3 sul dispositivo o sul cluster. L'accesso viene ripristinato quando lo storage compatibile con Amazon S3 su Snowball Edge viene riavviato. Per i dispositivi dotati di storage compatibile con Amazon S3 su Snowball Edge, si consiglia di avviare il servizio dopo l'accensione del dispositivo Snowball Edge. Vedi [Configurazione di Snowball Edge](#) in questa guida.

```
snowballEdge stop-service --service-id service_id --profile profile-name
```

Example output del comando **stop-service**

```
Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS service using the describe-service command.
```

Visualizzazione e download dei log da Snowball Edge

Quando trasferisci dati tra il data center locale e uno Snowball Edge, i log vengono generati automaticamente. Se si verificano errori imprevisti durante il trasferimento dei dati nel dispositivo, puoi utilizzare i comandi seguenti per salvare una copia dei log nel server locale.

Esistono tre comandi correlati ai log:

- **list-logs**— Restituisce un elenco di log in formato JSON. Questo elenco segnala le dimensioni dei log in byte, l'ARN per i log, l'ID servizio per i log e il tipo di log.

Utilizzo

```
snowballEdge list-logs --profile profile-name
```

Example output del comando **list-logs**

```
{
  "Logs" : [ {
    "LogArn" : "arn:aws:snowball-device::log/s3-storage-JIEXAMPLE2f-1234-4953-a7c4-dfEXAMPLE709",
    "LogType" : "SUPPORT",
    "ServiceId" : "s3",
    "EstimatedSizeBytes" : 53132614
  }, {
    "LogArn" : "arn:aws:snowball-device::log/fileinterface-JIDEXAMPLEf-1234-4953-a7c4-dfEXAMPLE709",
    "LogType" : "CUSTOMER",
    "ServiceId" : "fileinterface",
    "EstimatedSizeBytes" : 4446
  } ]
}
```

- **get-log**— Scarica una copia di un registro specifico da Snowball Edge sul dispositivo in un percorso specificato. CUSTOMERi log vengono salvati nel .zip formato ed è possibile estrarre questo tipo di log per visualizzarne il contenuto. SUPPORTi registri sono crittografati e possono essere letti solo da. Supporto AWSÈ possibile specificare un nome e un percorso per il log.

Utilizzo

```
snowballEdge get-log --log-arn arn:aws:snowball-device::log/fileinterface-JIDEXAMPLEf-1234-4953-a7c4-dfEXAMPLE709 --profile profile-name
```

Example output del comando **get-log**

```
Logs are being saved to download/path/snowball-edge-logs-1515EXAMPLE88.bin
```

- **get-support-logs**— Scarica una copia di tutti i SUPPORT tipi di log da Snowball Edge al servizio in un percorso specificato.

Utilizzo

```
snowballEdge get-support-logs --profile profile-name
```

Example output del comando **get-support-logs**

```
Logs are being saved to download/path/snowball-edge-logs-1515716135711.bin
```

Important

Il tipo CUSTOMER potrebbe contenere informazioni riservate sui propri dati. Per proteggere queste informazioni potenzialmente riservate, ti consigliamo di eliminare questi log quando non servono più.

Visualizzazione dello stato di uno Snowball Edge

È possibile determinare lo stato e lo stato generale di Snowball Edge con il `describe-device` comando.

```
snowballEdge describe-device --profile profile-name
```

Example output del comando **describe-device**

```
{
  "DeviceId": "JID-EXAMPLE12345-123-456-7-890",
  "UnlockStatus": {
    "State": "UNLOCKED"
  },
  "ActiveNetworkInterface": {
    "IpAddress": "192.0.2.0"
  },
  "PhysicalNetworkInterfaces": [
    {
      "PhysicalNetworkInterfaceId": "s.ni-EXAMPLEd9ecbf03e3",
      "PhysicalConnectorType": "RJ45",
      "IpAddressAssignment": "STATIC",
      "IpAddress": "0.0.0.0",
      "Netmask": "0.0.0.0",
```



```

    "DefaultGateway": "192.0.2.1",
    "MacAddress": "EX:AM:PL:E0:12:34"
  },
  {
    "PhysicalNetworkInterfaceId": "s.ni-EXAMPLE4c3840068f",
    "PhysicalConnectorType": "QSFP",
    "IpAddressAssignment": "STATIC",
    "IpAddress": "0.0.0.0",
    "Netmask": "0.0.0.0",
    "DefaultGateway": "192.0.2.2",
    "MacAddress": "EX:AM:PL:E0:56:78"
  },
  {
    "PhysicalNetworkInterfaceId": "s.ni-EXAMPLE0a3a6499fd",
    "PhysicalConnectorType": "SFP_PLUS",
    "IpAddressAssignment": "DHCP",
    "IpAddress": "192.168.1.231",
    "Netmask": "255.255.255.0",
    "DefaultGateway": "192.0.2.3",
    "MacAddress": "EX:AM:PL:E0:90:12"
  }
]
}

```

Visualizzazione dello stato dei servizi in esecuzione su Snowball Edge

È possibile determinare lo stato e lo stato generale dei servizi in esecuzione sui dispositivi Snowball Edge con il `describe-service` comando. Puoi eseguire innanzitutto il comando `list-services` per vedere quali servizi sono in esecuzione.

- `list-services`

Utilizzo

```
snowballEdge list-services --profile profile-name
```

Example output del comando **list-services**

```
{
```

```
"ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]
}
```

- **describe-service**

Questo comando restituisce un valore di stato per un servizio. Include anche informazioni sullo stato che possono essere utili per la risoluzione dei problemi rilevati con il servizio. Gli stati sono riportati di seguito.

- **ACTIVE**: il servizio è in esecuzione e disponibile per l'uso.
- **ACTIVATING**: il servizio è in fase di avvio, ma non è ancora disponibile per l'uso.
- **DEACTIVATING**: il servizio è in fase di chiusura.
- **DEGRADED**— Per lo storage compatibile con Amazon S3 su Snowball Edge, questo stato indica che uno o più dischi o dispositivi del cluster non sono attivi. Lo storage compatibile con Amazon S3 sul servizio Snowball Edge funziona senza interruzioni, ma è necessario ripristinare o sostituire il dispositivo interessato prima che il quorum del cluster vada perso per ridurre al minimo il rischio di perdita di dati. [Consulta la panoramica sul clustering in questa guida.](#)
- **INACTIVE**: il servizio non è in esecuzione e non è disponibile per l'uso.

Utilizzo

```
snowballEdge describe-service --service-id service-id --profile profile-name
```

Example output del comando **describe-service**

```
{
  "ServiceId": "s3",
  "Status": {
    "State": "ACTIVE"
  },
  "Storage": {
    "TotalSpaceBytes": 99608745492480,
    "FreeSpaceBytes": 99608744468480
  },
  "Endpoints": [
    {
      "Protocol": "http",
      "Port": 8080,
      "Host": "192.0.2.0"
    }
  ]
}
```

```

    },
    {
      "Protocol": "https",
      "Port": 8443,
      "Host": "192.0.2.0",
      "CertificateAssociation": {
        "CertificateArn": "arn:aws:snowball-
device:::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
      }
    }
  ]
}

```

Example Storage compatibile con Amazon S3 sull'output del servizio Snowball Edge

Il `describe-service` comando fornisce il seguente output per il `s3-snow` valore del `service-id` parametro.

```

{
  "ServiceId" : "s3-snow",
  "Autostart" : false,
  "Status" : {
    "State" : "ACTIVE"
  },
  "ServiceCapacities" : [ {
    "Name" : "S3 Storage",
    "Unit" : "Byte",
    "Used" : 640303104,
    "Available" : 219571981512
  } ],
  "Endpoints" : [ {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.123",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device:::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID6ebd4c50-c3a1-4b16-b32c-b254f9b7f2dc",
    "Status" : {
      "State" : "ACTIVE"
    }
  } ]
}

```

```

    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.202",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID6ebd4c50-c3a1-4b16-b32c-b254f9b7f2dc",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.63",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID2a1e0deb-38b1-41f8-b904-a396c62da70d",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.243",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID2a1e0deb-38b1-41f8-b904-a396c62da70d",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.220",

```

```

    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JIDcc45fa8f-b994-4ada-a821-581bc35d8645",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.55",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JIDcc45fa8f-b994-4ada-a821-581bc35d8645",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.213",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID4ec68543-d974-465f-b81d-89832dd502db",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.144",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",

```

```

    "DeviceId" : "JID4ec68543-d974-465f-b81d-89832dd502db",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.2.143",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow bucket API endpoint",
    "DeviceId" : "JID6331b8b5-6c63-4e01-b3ca-eab48b5628d2",
    "Status" : {
      "State" : "ACTIVE"
    }
  }, {
    "Protocol" : "https",
    "Port" : 443,
    "Host" : "10.0.3.224",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-device::certificate/
a65ba817f2c5ac9683fc3bc1ae123456"
    },
    "Description" : "s3-snow object API endpoint",
    "DeviceId" : "JID6331b8b5-6c63-4e01-b3ca-eab48b5628d2",
    "Status" : {
      "State" : "ACTIVE"
    }
  }
]
}

```

Visualizzazione dello stato delle funzionalità di Snowball Edge

Per elencare lo stato delle funzionalità disponibili su Snowball Edge, usa il `describe-features` comando.

`RemoteManagementState` indica lo stato di Snowball Edge Device Management e restituisce uno dei seguenti stati:

- **INSTALLED_ONLY**— La funzionalità è installata ma non abilitata.
- **INSTALLED_AUTOSTART**— La funzione è abilitata e il dispositivo tenterà di connettersi ad essa Regione AWS quando viene acceso.
- **NOT_INSTALLED**— Il dispositivo non supporta la funzionalità o era già presente sul campo prima del lancio.

Utilizzo

```
snowballEdge describe-features --profile profile-name
```

Example uscita del **describe-features** comando

```
{  
  "RemoteManagementState" : String  
}
```

Impostazione dei time server per Snowball Edge

È possibile utilizzare i comandi del client Snowball Edge per visualizzare la configurazione NTP (Network Time Protocol) corrente e scegliere un server o un peer per fornire l'ora. È possibile utilizzare i comandi del client Snowball Edge quando il dispositivo è bloccato e sbloccato.

È tua responsabilità fornire un time server NTP sicuro. Per impostare a quali time server NTP si connette il dispositivo, usa il `update-time-servers` comando.

Controllo delle sorgenti temporali di Snowball Edge

Per vedere a quali sorgenti orarie NTP è attualmente connesso il dispositivo, usa il `describe-time-sources` comando.

```
snowballEdge describe-time-sources --profile profile-name
```

Example output del comando **describe-time-sources**

```
{  
  "Sources" : [ {
```

```

    "Address" : "172.31.2.71",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "172.31.3.203",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "172.31.0.178",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "172.31.3.178",
    "State" : "LOST",
    "Type" : "PEER",
    "Stratum" : 10
  }, {
    "Address" : "216.239.35.12",
    "State" : "CURRENT",
    "Type" : "SERVER",
    "Stratum" : 1
  } ]
}

```

Il `describe-time-sources` comando restituisce un elenco di stati di origine temporale. Ogni stato dell'origine temporale contiene i `Stratum` campi `Address` `State` `Type`, e. Di seguito sono riportati i significati di questi campi.

- **Address**— Il nome DNS/indirizzo IP della sorgente temporale.
- **State**— Lo stato attuale della connessione tra il dispositivo e quella fonte di tempo. Esistono cinque stati possibili:
 - **CURRENT**— La fonte dell'ora è attualmente utilizzata per sincronizzare l'ora.
 - **COMBINED**— La fonte dell'ora è combinata con la fonte corrente.
 - **EXCLUDED**— L'origine temporale è esclusa dall'algoritmo di combinazione.
 - **LOST**— La connessione con la fonte dell'ora è stata interrotta.
 - **UNACCEPTABLE**— Una fonte temporale non valida in cui l'algoritmo di combinazione è stato considerato un falso indicatore o presenta troppa variabilità.

- **Type**— Una fonte di tempo NTP può essere un server o un peer. I server possono essere impostati tramite il `update-time-servers` comando. I peer possono essere solo altri dispositivi Snowball Edge del cluster e vengono configurati automaticamente quando il cluster viene associato.
- **Stratum**— Questo campo mostra lo strato della sorgente. Stratum 1 indica una sorgente con un orologio di riferimento collegato localmente. Una sorgente sincronizzata con una sorgente dello strato 1 si trova nello strato 2. Una sorgente sincronizzata con una sorgente di strato 2 si trova allo strato 3 e così via..

Una fonte di tempo NTP può essere un server o un peer. Un server può essere impostato dall'utente con il `update-time-servers` comando, mentre un peer può essere costituito solo da altri dispositivi Snowball Edge del cluster. Nell'output di esempio, `describe-time-sources` viene chiamato su uno Snowball Edge che si trova in un cluster di 5. L'output contiene 4 peer e 1 server. I peer hanno uno strato di 10 mentre il server ha uno strato di 1; pertanto, il server viene selezionato come fonte di tempo corrente.

Aggiornamento dei time server

Usa il `update-time-servers` comando e l'indirizzo del time server per configurare Snowball Edge per l'utilizzo di un server o peer NTP per NTP.

```
snowballEdge update-time-servers time-server-address --profile profile-name
```

Note

Il `update-time-servers` comando sostituirà le precedenti impostazioni dei time server NTP.

Example output del comando **update-time-servers**

```
Updating time servers now.
```

Ottenere un codice QR per convalidare i tag NFC di Snowball Edge

Puoi utilizzare questo comando per generare un codice QR specifico del dispositivo da utilizzare con l'app di verifica. AWS Snowball Edge Per ulteriori informazioni sulla convalida NFC, consulta.

[Convalida dei tag NFC](#)

Utilizzo

```
snowballEdge get-app-qr-code --output-file ~/downloads/snowball-qr-code.png --  
profile profile-name
```

Example Output

```
QR code is saved to ~/downloads/snowball-qr-code.png
```

Aggiornamento delle dimensioni MTU

Utilizzate il `update-mtu-size` comando per modificare la dimensione in byte dell'unità di trasmissione massima (MTU) di un'interfaccia fisica di un dispositivo Snowball Edge. Tutte le interfacce di rete virtuali e le interfacce di rete dirette associate a questa interfaccia di rete fisica verranno configurate con le stesse dimensioni MTU.

Note

La dimensione minima dell'MTU è di 1500 byte e la dimensione massima è di 9216 byte.

È possibile utilizzare il `describe-device` comando per recuperare l'interfaccia di rete fisica IDs e le dimensioni MTU correnti di tali interfacce. Per ulteriori informazioni, consulta [Visualizzazione dello stato di uno Snowball Edge](#).

È possibile utilizzare i `describe-virtual-network-interface` comandi `describe-direct-network-interface` and per recuperare le dimensioni MTU correnti di tali interfacce.

Utilizzo

```
snowballEdge update-mtu-size --physical-network-interface-id physical-network-  
interface-id --mtu-size size-in-bytes --profile profile-name
```

Example di **update-mtu-size** output

```
{
  "PhysicalNetworkInterface": {
    "PhysicalNetworkInterfaceId": "s.ni-8c1f891d7f5b87cfe",
    "PhysicalConnectorType": "SFP_PLUS",
    "IpAddressAssignment": "DHCP",
    "IpAddress": "192.0.2.0",
    "Netmask": "255.255.255.0",
    "DefaultGateway": "192.0.2.255",
    "MacAddress": "8A:2r:5G:9p:6Q:4s",
    "MtuSize": "5743"
  }
}
```

Trasferimento di file tramite l'adattatore Amazon S3 per la migrazione dei dati da o verso Snowball Edge

Di seguito è riportata una panoramica dell'adattatore Amazon S3, che puoi utilizzare per trasferire dati a livello di codice da e verso i bucket S3 già presenti sul dispositivo utilizzando le azioni dell'API REST di AWS Snowball Edge Amazon S3. Il supporto dell'API REST di Amazon S3 è limitato a un sottoinsieme di azioni. Puoi utilizzare questo sottoinsieme di azioni con una delle seguenti AWS SDKs per trasferire dati a livello di codice. Puoi anche utilizzare il sottoinsieme di comandi supportati AWS Command Line Interface (AWS CLI) per Amazon S3 per trasferire dati a livello di codice.

Se la tua soluzione utilizza la AWS SDK per Java versione 1.11.0 o successiva, devi usare quanto segue: `S3ClientOptions`

- `disableChunkedEncoding()`— Indica che la codifica a blocchi non è supportata dall'interfaccia.
- `setPathStyleAccess(true)`— Configura l'interfaccia per utilizzare l'accesso in stile path per tutte le richieste.

Per ulteriori informazioni, consulta [Class S3 ClientOptions .Builder](#) in Amazon SDK for AppStream Java.

Important

Ti consigliamo di utilizzare un solo metodo alla volta per leggere e scrivere dati in un bucket locale su un dispositivo. AWS Snowball Edge L'utilizzo simultaneo dell'interfaccia NFS e dell'adattatore Amazon S3 sullo stesso bucket può causare conflitti. read/write

[AWS Snowball Edge quotes](#) specifica i limiti.

AWS Affinché i servizi funzionino correttamente su Snowball Edge, è necessario consentire le porte per i servizi. Per informazioni dettagliate, consultare [Requisiti delle porte per AWS i servizi su Snowball Edge](#).

Argomenti

- [Download e installazione della AWS CLI versione 1.16.14 da utilizzare con l'adattatore Amazon S3](#)
- [Utilizzo delle operazioni AWS CLI e dell'API sui dispositivi Snowball Edge](#)
- [Acquisizione e utilizzo delle credenziali locali di Amazon S3 su Snowball Edge](#)

- [Funzionalità di Amazon S3 non supportate per l'adattatore Amazon S3 su Snowball Edge](#)
- [Suddivisione in batch di file di piccole dimensioni per migliorare le prestazioni di trasferimento dei dati su Snowball Edge](#)
- [AWS CLI Comandi supportati per il trasferimento di dati da o verso Snowball Edge](#)
- [Azioni API REST di Amazon S3 supportate su Snowball Edge per il trasferimento dei dati](#)

Download e installazione della AWS CLI versione 1.16.14 da utilizzare con l'adattatore Amazon S3

Attualmente, i dispositivi Snowball Edge supportano solo la versione 1.16.14 e precedenti AWS CLI per l'uso con l'adattatore Amazon S3. Le versioni più recenti di non AWS CLI sono compatibili con l'adattatore Amazon S3 perché non supportano tutte le funzionalità dell'adattatore S3.

Note

Se utilizzi uno storage compatibile con Amazon S3 su Snowball Edge, puoi utilizzare la versione più recente di AWS CLI. Per scaricare e utilizzare la versione più recente, consulta la Guida per [AWS Command Line Interface l'utente](#).

Installa AWS CLI su sistemi operativi Linux

Esegui questo comando concatenato:

```
curl "https://s3.amazonaws.com/aws-cli/awscli-bundle-1.16.14.zip" -o "awscli-bundle.zip"; unzip awscli-bundle.zip; sudo ./awscli-bundle/install -i /usr/local/aws -b /usr/local/bin/aws; /usr/local/bin/aws --version;
```

Installa AWS CLI su sistemi operativi Windows

Scarica ed esegui il file di installazione per il tuo sistema operativo:

- [Programma di installazione a 32 bit fornito in bundle con Python 2](#)
- [Programma di installazione a 32 bit fornito in bundle con Python 3](#)

- [programma di installazione a 64 bit fornito in bundle con Python 2](#)
- [programma di installazione a 64 bit fornito in bundle con Python 3](#)
- [File di installazione che include programmi di installazione a 32 e 64 bit che installeranno automaticamente la versione corretta](#)

Utilizzo delle operazioni AWS CLI e dell'API sui dispositivi Snowball Edge

Quando utilizzi le operazioni AWS CLI o API per emettere EC2 comandi IAM, Amazon S3 e Amazon su Snowball Edge, devi specificare la regione come "». snow È possibile eseguire questa operazione utilizzando AWS `configure` o all'interno del comando stesso, come negli esempi seguenti.

```
aws configure --profile abc
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Or

```
aws s3 ls --endpoint http://192.0.2.0:8080 --region snow --profile snowballEdge
```

Autorizzazione con l'interfaccia API Amazon S3 per AWS Snowball Edge

Quando utilizzi l'adattatore Amazon S3, ogni interazione viene firmata con l'algoritmo AWS Signature versione 4 per impostazione predefinita. Questa autorizzazione viene utilizzata solo per verificare i dati che viaggiano dalla fonte all'interfaccia. Tutta la crittografia e la decrittografia viene eseguita nel dispositivo. I dati non crittografati non vengono mai archiviati nel dispositivo.

Quando usi l'interfaccia, tieni presente quanto segue:

- Per ottenere le credenziali locali di Amazon S3 per firmare le richieste sul AWS Snowball Edge dispositivo, esegui i comandi del client e `snowballEdge list-access-keys snowballEdge get-secret-access-keys` Snowball Edge. Per ulteriori informazioni, consulta [Configurazione e utilizzo del client Snowball Edge](#). Queste credenziali Amazon S3 locali includono un paio di chiavi: una chiave di accesso e una chiave segreta. Queste chiavi sono valide solo per i dispositivi

associati al processo. Non possono essere utilizzate in Cloud AWS perché non hanno una controparte AWS Identity and Access Management (IAM).

- La chiave di crittografia non viene modificata in base alle AWS credenziali utilizzate. La firma con l'algoritmo Signature Version 4 viene utilizzata solo per verificare i dati che viaggiano dalla fonte all'interfaccia. Pertanto, questa firma non influisce mai sulle chiavi di crittografia utilizzate per crittografare i dati sullo Snowball.

Acquisizione e utilizzo delle credenziali locali di Amazon S3 su Snowball Edge

Ogni interazione con Snowball Edge è firmata con l'algoritmo AWS Signature Version 4. Per ulteriori informazioni sull'algoritmo, vedere il [processo di firma versione 4 della firma](#) nella Riferimenti generali di AWS.

Puoi ottenere le credenziali locali di Amazon S3 per firmare le tue richieste sul dispositivo client Edge Snowball Edge eseguendo le informazioni sul client e `snowballEdge list-access-keys` `snowballEdge get-secret-access-key` Snowball Edge, vedi. [Ottenere le credenziali per uno Snowball Edge](#) Queste credenziali locali di Amazon S3 includono un paio di chiavi: un ID della chiave di accesso e una chiave segreta. Queste credenziali sono valide solo per i dispositivi associati al processo. Non possono essere utilizzate in Cloud AWS perché non hanno una controparte IAM.

Puoi aggiungere queste credenziali al file delle AWS credenziali sul tuo server. Il file dei profili delle credenziali predefinito si trova in genere in `~/.aws/credentials`, ma il percorso può variare a seconda della piattaforma. Questo file è condiviso da molti di AWS SDKs e da AWS CLI. Puoi salvare le credenziali locali con un nome del profilo come nell'esempio seguente.

```
[snowballEdge]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFcYEXAMPLEKEY
```

Configurazione AWS CLI per utilizzare l'adattatore S3 su uno Snowball Edge come endpoint

Quando si utilizza AWS CLI per inviare un comando al AWS Snowball Edge dispositivo, si specifica che l'endpoint è l'adattatore Amazon S3. Puoi scegliere di utilizzare l'endpoint HTTPS o un endpoint HTTP non protetto, come mostrato di seguito.

Endpoint protetto HTTPS

```
aws s3 ls --endpoint https://192.0.2.0:8443 --ca-bundle path/to/certificate --profile snowballEdge
```

Endpoint non protetto HTTP

```
aws s3 ls --endpoint http://192.0.2.0:8080 --profile snowballEdge
```

Se si utilizza l'endpoint HTTPS di 8443, i dati vengono trasferiti in modo sicuro dal server a Snowball Edge. Questa crittografia è garantita da un certificato generato da Snowball Edge quando riceve un nuovo indirizzo IP. Dopo aver ottenuto il certificato, puoi salvarlo in un file `ca-bundle.pem` locale. Quindi puoi configurare il tuo AWS CLI profilo per includere il percorso del certificato, come descritto di seguito.

Per associare il certificato all'endpoint dell'interfaccia

1. Connect Snowball Edge all'alimentazione e alla rete e accendilo.
2. Al termine della procedura di avvio, prendere nota del relativo indirizzo IP sulla rete locale.
3. Da un terminale della rete, assicurati di poter eseguire il ping di Snowball Edge.
4. Eseguire il comando `snowballEdge get-certificate` nel terminale. Per ulteriori informazioni su questo comando, consulta [Gestione dei certificati a chiave pubblica su Snowball Edge](#).
5. Salvare l'output del comando `snowballEdge get-certificate` in un file, ad esempio `ca-bundle.pem`.
6. Eseguire il seguente comando dal terminale.

```
aws configure set profile.snowballEdge.ca_bundle /path/to/ca-bundle.pem
```

Al termine della procedura, puoi eseguire comandi CLI con queste credenziali locali, il certificato e l'endpoint specificato, come nell'esempio seguente.

```
aws s3 ls --endpoint https://192.0.2.0:8443 --profile snowballEdge
```


Funzionalità di Amazon S3 non supportate per l'adattatore Amazon S3 su Snowball Edge

Utilizzando l'adattatore Amazon S3, puoi trasferire dati a livello di codice da e verso uno Snowball Edge con azioni API Amazon S3. Tuttavia, non tutte le funzionalità di trasferimento e le azioni API di Amazon S3 sono supportate per l'uso con un dispositivo Snowball Edge quando si utilizza l'adattatore Amazon S3. Ad esempio, le seguenti funzionalità e azioni non sono supportate per l'uso con Snowball Edge:

- [TransferManager](#)— Questa utilità trasferisce file da un ambiente locale ad Amazon S3 con l'SDK for Java. Valuta invece la possibilità di utilizzare le azioni o AWS CLI i comandi API supportati con l'interfaccia.
- [GET Bucket \(List Objects\) Versione 2](#): questa implementazione dell'azione GET restituisce alcuni o tutti (fino a 1.000) gli oggetti in un bucket. Valuta se utilizzare l'operazione [GET Bucket \(Elenca oggetti\) Versione 1](#) o il comando `ls` della AWS CLI .
- [ListBuckets](#)— L'endpoint ListBuckets con l'oggetto non è supportato. Il comando seguente non funziona con lo storage compatibile con Amazon S3 su Snowball Edge:

```
aws s3 ls --endpoint https://192.0.2.0 --profile profile
```

Suddivisione in batch di file di piccole dimensioni per migliorare le prestazioni di trasferimento dei dati su Snowball Edge

Ogni operazione di copia genera un overhead a causa della crittografia. Per velocizzare il processo di trasferimento di file di piccole dimensioni AWS Snowball Edge sul dispositivo, puoi raggrupparli in un unico archivio. Quando i file vengono raggruppati in batch, possono essere estratti automaticamente quando vengono importati in Amazon S3, se sono stati raggruppati in batch in uno dei formati di archivio supportati.

In genere, i file aventi dimensioni di 1 MB o inferiori devono essere inclusi in batch. Non esiste un limite fisico al numero di file in un batch, sebbene consigliamo di limitare i batch a circa 10.000 file. La presenza di più di 100.000 file in un batch può influire sulla velocità di importazione di tali file in

Amazon S3 dopo la restituzione del dispositivo. La dimensione totale di ogni batch non deve superare i 100 GB.

Il raggruppamento di file è un processo manuale facilmente gestibile. Dopo aver eseguito il batch dei file, trasferiscili su un dispositivo Snowball Edge utilizzando il AWS CLI `cp` comando con l' `--metadata snowball-auto-extract=true` opzione. Specificando `estrae snowball-auto-extract=true` automaticamente il contenuto dei file archiviati quando i dati vengono importati in Amazon S3, a condizione che la dimensione del file in batch non superi i 100 GB.

Note

I batch di dimensioni superiori a 100 GB non vengono estratti quando vengono importati in Amazon S3.

Per raggruppare file di piccole dimensioni

1. Scegliere il formato da utilizzare per raggruppare i file di piccole dimensioni. La funzione di estrazione automatica supporta i formati TAR, ZIP e `tar.gz`.
2. Identificare i file di piccole dimensioni da raggruppare, incluse le dimensioni e il numero totale di file da raggruppare.
3. Batch dei file sulla riga di comando, come illustrato negli esempi seguenti.
 - Per Linux, è possibile raggruppare i file nella stessa riga di comando utilizzata per trasferire i file sul dispositivo.

```
tar -cf - /Logs/April | aws s3 cp - s3://amzn-s3-demo-bucket/batch01.tar --  
metadata snowball-auto-extract=true --endpoint http://192.0.2.0:8080
```

Note

In alternativa, è possibile utilizzare l'utilità di archiviazione preferita per raggruppare file in uno o più archivi di grandi dimensioni. Tuttavia, questo approccio richiede uno spazio di archiviazione locale aggiuntivo per salvare gli archivi prima di trasferirli su Snowball Edge.

- Per Windows, utilizzate il seguente comando di esempio per raggruppare i file in batch quando tutti i file si trovano nella stessa directory da cui viene eseguito il comando:

```
7z a -tzip -so "test" | aws s3 cp - s3://amzn-s3-demo-bucket/batch01.zip --  
metadata snowball-auto-extract=true --endpoint http://192.0.2.0:8080
```

Per inserire in batch i file da una directory diversa da cui viene eseguito il comando, utilizzate il seguente comando di esempio:

```
7z a -tzip -so "test" "c:\temp" | aws s3 cp - s3://amzn-s3-demo-bucket/  
batch01.zip --metadata snowball-auto-extract=true --endpoint http://10.x.x.x:8080
```

Note

Per Microsoft Windows 2016, tar non è disponibile, ma è possibile scaricarlo dal sito Web di Tar for Windows.

È possibile scaricare 7 ZIP dal sito Web 7ZIP.

4. Ripeti l'operazione fino ad archiviare tutti i file di piccole dimensioni che desideri trasferire su Amazon S3 utilizzando Snowball Edge.
5. Trasferisci i file archiviati su Snowball. Se desideri che i dati vengano estratti automaticamente e hai utilizzato uno dei formati di archivio supportati menzionati in precedenza nel passaggio 1, usa il AWS CLI cp comando con l'--metadata snowball-auto-extract=true opzione.

Note

Se sono presenti file non di archivio, non utilizzare questo comando.

Durante la creazione dei file di archivio, l'estrazione manterrà la struttura dei dati corrente. Ciò significa che se crei un file di archivio contenente file e cartelle, Snowball Edge lo ricreerà durante il processo di inserimento in Amazon S3.

Il file di archivio verrà estratto nella stessa directory in cui è memorizzato e le strutture delle cartelle verranno create di conseguenza. Tieni presente che quando copi i file di archivio, è importante impostare la bandiera. --metadata snowball-auto-extract=true Altrimenti, Snowball Edge non estrarrà i dati quando vengono importati in Amazon S3.

Utilizzando l'esempio del passaggio 3, se la struttura delle cartelle di /Logs/April/ contiene i file, e. a.txt b.txt c.txt Se questo file di archivio è stato inserito nella radice di/amzn-s3-demo-bucket/, dopo l'estrazione i dati avrebbero il seguente aspetto:

```
/amzn-s3-demo-bucket/Logs/April/a.txt  
/amzn-s3-demo-bucket/Logs/April/b.txt  
/amzn-s3-demo-bucket/Logs/April/c.txt
```

Se il file di archivio è stato inserito in/amzn-s3-demo-bucket/Test/, l'estrazione sarebbe simile alla seguente:

```
/amzn-s3-demo-bucket/Test/Logs/April/a.txt  
/amzn-s3-demo-bucket/Test/Logs/April/b.txt  
/amzn-s3-demo-bucket/Test/Logs/April/c.txt
```

AWS CLI Comandi supportati per il trasferimento di dati da o verso Snowball Edge

Di seguito, puoi trovare informazioni su come specificare l'adattatore Amazon S3 o lo storage compatibile con Amazon S3 su Snowball Edge come endpoint per i comandi applicabile (). AWS Command Line Interface AWS CLI Puoi anche trovare l'elenco dei AWS CLI comandi per Amazon S3 supportati per il trasferimento di dati al AWS Snowball Edge dispositivo con l'adattatore o lo storage compatibile con Amazon S3 su Snowball Edge.

Note

[Per informazioni sull'installazione e la configurazione di AWS CLI, inclusa l'indicazione delle regioni verso cui effettuare AWS CLI chiamate, consulta la Guida per l'utente.AWS Command Line Interface](#)

Attualmente, i dispositivi Snowball Edge supportano solo la versione 1.16.14 e precedenti di AWS CLI quando si utilizza l'adattatore Amazon S3. Consultare [Ricerca della versione client Snowball Edge](#). Se utilizzi uno storage compatibile con Amazon S3 su Snowball Edge, puoi utilizzare la versione più recente di AWS CLI [Per scaricare e utilizzare la versione più recente,AWS Command Line Interface consulta la Guida per l'utente.](#)

 Note

Assicurati di installare la versione 2.6.5 o successive o 3.4 o successive di Python prima di installare la versione 1.16.14 di AWS CLI.

AWS CLI Comandi supportati per il trasferimento di dati con Amazon S3 e Snowball Edge

Di seguito è riportata una descrizione del sottoinsieme di AWS CLI comandi e opzioni per Amazon S3 supportato AWS Snowball Edge dal dispositivo. Se un comando o un'opzione non è elencato, non è supportato. Insieme al comando, puoi dichiarare alcune opzioni non supportate, come `--sse` o `--storage-class`. Tuttavia, queste vengono ignorate e non influiscono sulla modalità di importazione dei dati.

- [cp](#) — Copia un file o un oggetto su o dal AWS Snowball Edge dispositivo. Di seguito sono elencate le opzioni per questo comando:
 - `--dryrun`(Boolean) — Le operazioni che verrebbero eseguite utilizzando il comando specificato vengono visualizzate senza essere eseguite.
 - `--quiet`(Boolean) — Le operazioni eseguite dal comando specificato non vengono visualizzate.
 - `--include`(stringa) — Non esclude file o oggetti nel comando che corrispondono al modello specificato. Per i dettagli, vedete [Uso dei filtri di esclusione e inclusione](#) nel riferimento ai AWS CLI comandi.
 - `--exclude`(stringa) — Esclude tutti i file o gli oggetti dal comando che corrisponde al modello specificato.
 - `--follow-symlinks` | `--no-follow-symlinks`(Boolean) — I link simbolici (collegamenti simbolici) vengono seguiti solo durante il caricamento su Amazon S3 dal file system locale. Amazon S3 non supporta i link simbolici, quindi i contenuti della destinazione del link vengono caricati sotto il nome del link. Quando nessuna delle due opzioni è specificata, l'impostazione predefinita è seguire symlink.
 - `--only-show-errors`(Boolean): vengono visualizzati solo gli errori e gli avvisi. L'output restante viene soppresso.
 - `--recursive`(Boolean) — Il comando viene eseguito su tutti i file o gli oggetti nella directory o nel prefisso specificato.

- `--page-size`(numero intero) — Il numero di risultati da restituire in ogni risposta a un'operazione di elenco. Il valore predefinito è 1000 (il massimo consentito). L'utilizzo di un valore inferiore potrebbe essere utile se un'operazione scade.
- `--metadata`(mappa) — Una mappa di metadati da archiviare con gli oggetti in Amazon S3. Questa mappa viene applicata a ogni oggetto che fa parte di questa richiesta. In una sincronizzazione, questa funzionalità significa che i file che non sono cambiati non ricevono i nuovi metadati. Quando si esegue la copia tra due posizioni Amazon S3, `metadata-directive` l'argomento per impostazione predefinita `REPLACE` è se non diversamente specificato.
- [`ls`](#) — Elenca gli oggetti sul dispositivo. AWS Snowball Edge Di seguito sono elencate le opzioni per questo comando:
 - `--human-readable`(Boolean) — Le dimensioni dei file vengono visualizzate in un formato leggibile dall'uomo.
 - `--summarize`(Boolean): vengono visualizzate informazioni di riepilogo, che rappresentano il numero di oggetti e le relative dimensioni totali.
 - `--recursive`(Boolean) — Il comando viene eseguito su tutti i file o gli oggetti contenuti nella directory o nel prefisso specificato.
 - `--page-size`(numero intero) — Il numero di risultati da restituire in ogni risposta a un'operazione di elenco. Il valore predefinito è 1000 (il massimo consentito). L'utilizzo di un valore inferiore potrebbe essere utile se un'operazione scade.
- [`rm`](#) — Elimina un oggetto sul dispositivo. AWS Snowball Edge Di seguito sono elencate le opzioni per questo comando:
 - `--dryrun`(Boolean) — Le operazioni che verrebbero eseguite utilizzando il comando specificato vengono visualizzate senza essere eseguite.
 - `--include`(stringa) — Non esclude file o oggetti nel comando che corrispondono allo schema specificato. Per i dettagli, vedete [Uso dei filtri di esclusione e inclusione](#) nel riferimento ai AWS CLI comandi.
 - `--exclude`(stringa) — Esclude tutti i file o gli oggetti dal comando che corrisponde al modello specificato.
 - `--recursive`(Boolean) — Il comando viene eseguito su tutti i file o gli oggetti nella directory o nel prefisso specificato.
 - `--page-size`(numero intero) — Il numero di risultati da restituire in ogni risposta a un'operazione di elenco. Il valore predefinito è 1000 (il massimo consentito). L'utilizzo di un valore inferiore potrebbe essere utile se un'operazione scade.

- `--only-show-errors`(Boolean) — Vengono visualizzati solo gli errori e gli avvisi. L'output restante viene soppresso.
- `--quiet`(Boolean) — Le operazioni eseguite dal comando specificato non vengono visualizzate.
- [sync — Sincronizza](#) le directory e i prefissi. Questo comando consente di copiare file nuovi e aggiornati dalla directory di origine nella destinazione. Questo comando crea cartelle nella destinazione solo se contengono uno o più file.

Important

La sincronizzazione da una directory a un'altra sullo stesso Snowball Edge non è supportata.

La sincronizzazione da un AWS Snowball Edge dispositivo a un altro non è AWS Snowball Edge supportata.

Puoi utilizzare questa opzione solo per sincronizzare i contenuti tra l'archiviazione dei dati locale e Snowball Edge.

- `--dryrun`(Boolean) — Le operazioni che verrebbero eseguite utilizzando il comando specificato vengono visualizzate senza essere eseguite.
- `--quiet`(Boolean) — Le operazioni eseguite dal comando specificato non vengono visualizzate.
- `--include`(stringa) — Non esclude file o oggetti nel comando che corrispondono al modello specificato. Per i dettagli, vedete [Uso dei filtri di esclusione e inclusione](#) nel riferimento ai AWS CLI comandi.
- `--exclude`(stringa) — Esclude tutti i file o gli oggetti dal comando che corrisponde al modello specificato.
- `--follow-symlinks` or `--no-follow-symlinks` (Boolean) — I link simbolici (collegamenti simbolici) vengono seguiti solo durante il caricamento su Amazon S3 dal file system locale. Amazon S3 non supporta i link simbolici, quindi i contenuti della destinazione del link vengono caricati sotto il nome del link. Quando nessuna delle due opzioni è specificata, l'impostazione predefinita è seguire symlink.
- `--only-show-errors`(Boolean): vengono visualizzati solo gli errori e gli avvisi. L'output restante viene soppresso.
- `--no-progress`(Boolean) — L'avanzamento del trasferimento dei file non viene visualizzato. Questa opzione viene applicata solo quando le opzioni `--quiet` e `--only-show-errors` non sono fornite.

- `--page-size`(numero intero) — Il numero di risultati da restituire in ogni risposta a un'operazione di elenco. Il valore predefinito è 1000 (il massimo consentito). L'utilizzo di un valore inferiore potrebbe essere utile se un'operazione scade.
- `--metadata`(mappa) — Una mappa di metadati da archiviare con gli oggetti in Amazon S3. Questa mappa viene applicata a ogni oggetto che fa parte di questa richiesta. In una sincronizzazione, questa funzionalità significa che i file che non sono cambiati non ricevono i nuovi metadati. Quando si esegue la copia tra due posizioni Amazon S3, `metadata-directive` l'argomento per impostazione predefinita REPLACE è se non diversamente specificato.

 Important

La sincronizzazione da una directory a un'altra sullo stesso Snowball Edge non è supportata.

La sincronizzazione da un AWS Snowball Edge dispositivo a un altro non è AWS Snowball Edge supportata.

Puoi utilizzare questa opzione solo per sincronizzare i contenuti tra l'archiviazione dei dati locale e Snowball Edge.

- `--size-only`(Boolean): con questa opzione, la dimensione di ogni chiave è l'unico criterio utilizzato per decidere se eseguire la sincronizzazione dall'origine alla destinazione.
- `--exact-timestamps`(Boolean): durante la sincronizzazione da Amazon S3 allo storage locale, gli elementi delle stesse dimensioni vengono ignorati solo quando i timestamp corrispondono esattamente. Il comportamento predefinito consiste nell'ignorare gli articoli delle stesse dimensioni a meno che la versione locale non sia più recente della versione di Amazon S3.
- `--delete`(Boolean) — I file presenti nella destinazione ma non nell'origine vengono eliminati durante la sincronizzazione.

Puoi utilizzare file o cartelle i cui nomi contengono spazi, ad esempio `my photo.jpg` o `My Documents`. Tuttavia, assicuratevi di gestire correttamente gli spazi nei comandi. AWS CLI Per ulteriori informazioni, consulta [Specificazione dei valori dei parametri per la AWS CLI](#) nella Guida per AWS Command Line Interface l'utente.

Azioni API REST di Amazon S3 supportate su Snowball Edge per il trasferimento dei dati

Di seguito, puoi trovare l'elenco delle azioni dell'API REST di Amazon S3 supportate per l'utilizzo dell'adattatore Amazon S3. L'elenco include collegamenti a informazioni su come funzionano le azioni API con Amazon S3. L'elenco include anche eventuali differenze di comportamento tra l'azione dell'API Amazon S3 e la controparte del AWS Snowball Edge dispositivo. Tutte le risposte che arrivano da un AWS Snowball Edge dispositivo vengono dichiarate `Server` come `AWSSnowball`, come nell'esempio seguente.

```
HTTP/1.1 201 OK
x-amz-id-2: JuKZqmXuiwFeDQxhD7M8KtsKobSzWA1QEjLbTMTagkKdBX2z7I1/jGhDeJ3j6s80
x-amz-request-id: 32FE2CEB32F5EE25
Date: Fri, 08 2016 21:34:56 GMT
Server: AWSSnowball
```

Le chiamate API REST di Amazon S3 richiedono la firma SigV4. Se utilizzi AWS CLI o un AWS SDK per effettuare queste chiamate API, la firma SigV4 viene gestita automaticamente. In caso contrario, devi implementare la tua soluzione di firma SigV4. Per ulteriori informazioni, consulta la sezione [Autenticazione delle richieste \(AWS Signature versione 4\)](#) nella Guida per l'utente di Amazon Simple Storage Service.

- [GET Bucket \(List Objects\) versione 1](#) — Supportata. Tuttavia, in questa implementazione dell'operazione GET, non è supportato quanto segue:
 - Paginazione
 - Contrassegni
 - Delimitatori
 - Quando l'elenco viene restituito, l'elenco non viene ordinato

È supportata solo la versione 1. GET Bucket (List Objects) version 2 non è supportato.

- [GET Service](#)
- [HEAD Bucket](#)
- [HEAD Object](#)
- [GET Object](#): è un DOWNLOAD di un oggetto dal bucket S3 del dispositivo Snow.
- [Oggetto PUT](#): quando un oggetto viene caricato su un AWS Snowball Edge dispositivo utilizzando `PUT Object`, ETag viene generato un.

ETag È un hash dell'oggetto. ETag Riflette le modifiche solo al contenuto di un oggetto, non ai suoi metadati. ETag Potrebbe essere o meno un riepilogo MD5 dei dati dell'oggetto. Per ulteriori informazioni ETags, consulta [Common Response Headers](#) nel riferimento all'API di Amazon Simple Storage Service.

- [DELETE Object](#)
- [Avvia caricamento multipart](#): in questa implementazione, l'avvio di una richiesta di caricamento multipart per un oggetto già presente sul AWS Snowball Edge dispositivo elimina innanzitutto quell'oggetto. Quindi lo copia in parti sul dispositivo. AWS Snowball Edge
- [Elenco dei caricamenti in più parti](#)
- [Upload Part](#)
- [Completamento del caricamento in più parti](#)
- [Abort Multipart Upload](#)

Note

Tutte le azioni dell'API REST dell'adattatore Amazon S3 non elencate qui non sono supportate. L'utilizzo di azioni API REST non supportate con Snowball Edge restituisce un messaggio di errore che indica che l'azione non è supportata.

Gestione dell'interfaccia NFS su Snowball Edge

Utilizza l'interfaccia Network File System (NFS) per caricare file su Snowball Edge come se il dispositivo fosse una memoria locale del tuo sistema operativo. Ciò consente un approccio più intuitivo al trasferimento dei dati, poiché è possibile utilizzare funzionalità del sistema operativo, come copiare file, trascinarli e rilasciarli o altre funzionalità dell'interfaccia utente grafica. Ogni bucket S3 sul dispositivo è disponibile come endpoint di interfaccia NFS e può essere montato per copiare i dati. L'interfaccia NFS è disponibile per i lavori di importazione.

È possibile utilizzare l'interfaccia NFS se il dispositivo Snowball Edge è stato configurato per includerlo quando è stato creato il processo per ordinare il dispositivo. Se il dispositivo non è configurato per includere l'interfaccia NFS, utilizza l'adattatore S3 o lo storage compatibile con Amazon S3 su Snowball Edge per trasferire i dati. Per ulteriori informazioni sull'adattatore S3, consulta [Gestione dello storage degli adattatori Amazon S3 con AWS OpsHub](#). Per ulteriori informazioni sullo storage compatibile con Amazon S3 su Snowball Edge, consulta [Configura lo storage compatibile con Amazon S3 su Snowball Edge con AWS OpsHub](#).

All'avvio, l'interfaccia NFS utilizza 1 GB di memoria e 1 CPU. Ciò può limitare il numero di altri servizi in esecuzione su Snowball Edge o il numero di istanze EC2 compatibili che possono essere eseguite.

I dati trasferiti tramite l'interfaccia NFS non vengono crittografati durante il transito. Durante la configurazione dell'interfaccia NFS, puoi fornire blocchi CIDR e Snowball Edge limiterà l'accesso all'interfaccia NFS dai computer client con indirizzi in quei blocchi.

I file sul dispositivo verranno trasferiti su Amazon S3 quando verranno restituiti a. AWS Per ulteriori informazioni, consulta [Importazione di lavori in Amazon](#) Edge.

Per ulteriori informazioni sull'utilizzo di NFS con il sistema operativo del computer, consulta la documentazione del sistema operativo in uso.

Tenete a mente i seguenti dettagli quando utilizzate l'interfaccia NFS.

- L'interfaccia NFS fornisce un bucket locale per l'archiviazione dei dati sul dispositivo. Per i lavori di importazione, nessun dato dal bucket locale verrà importato in Amazon S3.
- I nomi dei file sono chiavi oggetto nel bucket S3 locale su Snowball Edge. Il nome chiave è una sequenza di caratteri Unicode la cui codifica UTF-8 è lunga al massimo 1.024 byte. Si consiglia di utilizzare NFSv4 .1 laddove possibile e di codificare i nomi dei file con Unicode UTF-8 per garantire una corretta importazione dei dati. I nomi di file che non sono codificati con UTF-8 potrebbero non

essere caricati su S3 o potrebbero essere caricati su S3 con un nome di file diverso a seconda della codifica NFS utilizzata.

- Assicuratevi che la lunghezza massima del percorso del file sia inferiore a 1024 caratteri. Snowball Edge non supporta percorsi di file che superano i 1024 caratteri. Il superamento di questa lunghezza del percorso di file comporterà errori di importazione dei file.
- Per ulteriori informazioni, consulta [Object keys](#) nella Amazon Simple Storage Service User Guide.
- Per i trasferimenti basati su NFS, i metadati standard in stile POSIX verranno aggiunti agli oggetti non appena vengono importati in Amazon S3 da Snowball Edge. Inoltre, vedrai i metadati "x-amz-meta-user-agent aws-datasync» che utilizziamo attualmente AWS DataSync come parte del meccanismo di importazione interno in Amazon S3 per l'importazione di Snowball Edge con l'opzione NFS.
- È possibile trasferire fino a 40 milioni di file utilizzando un solo dispositivo Snowball Edge. Se devi trasferire più di 40 milioni di file in un unico processo, raggruppa i file in batch per ridurre il numero di file per ogni trasferimento. I singoli file possono essere di qualsiasi dimensione con una dimensione massima di 5 TB per i dispositivi Snowball Edge con l'interfaccia NFS avanzata o l'interfaccia S3.

Puoi anche configurare e gestire l'interfaccia NFS con AWS OpsHub uno strumento GUI. Per ulteriori informazioni, vedere [Gestione dell'interfaccia NFS utilizzando NFS](#) il trasferimento di file offline.

Configurazione NFS per Snowball Edge

L'interfaccia NFS non è in esecuzione sul dispositivo Snowball Edge per impostazione predefinita, quindi è necessario avviarla per abilitare il trasferimento dei dati sul dispositivo. È possibile configurare l'interfaccia NFS fornendo l'indirizzo IP di un'interfaccia di rete virtuale (VNI) in esecuzione su Snowball Edge e limitando l'accesso alla condivisione di file, se necessario. Prima di configurare l'interfaccia NFS, configura un'interfaccia di rete virtuale (VNI) su Snowball Edge. Per ulteriori informazioni, consulta [Configurazione di rete](#) per istanze di calcolo.

Configurare Snowball Edge per l'interfaccia NFS

- Utilizzate il `describe-service` comando per determinare se l'interfaccia NFS è attiva.

```
snowballEdge describe-service --service-id nfs
```

Il comando restituirà lo stato del servizio NFS, ACTIVE oppure. INACTIVE

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "ACTIVE"
  }
}
```

Se il valore del State nome èACTIVE, il servizio di interfaccia NFS è attivo ed è possibile montare il volume NFS Snowball Edge. Per ulteriori informazioni, consulta

Dopo l'avvio dell'interfaccia NFS, monta l'endpoint come memoria locale sui computer client.

Di seguito sono riportati i comandi di montaggio predefiniti per i sistemi operativi Windows, Linux e macOS.

- Windows:

```
mount -o nolock rsize=128 wsize=128 mtype=hard nfs-interface-ip-address:/
buckets/BucketName *
```

- Linux:

```
mount -t nfs nfs-interface-ip-address:/buckets/BucketName mount_point
```

- macOS:

```
mount -t nfs -o vers=3,rsize=131072,wsize=131072,nolocks,hard,retrans=2 nfs-
interface-ip-address:/buckets/$bucketname mount_point
```

. Se il valore èINACTIVE, è necessario avviare il servizio.

Avvio del servizio NFS su Snowball Edge

Avvia un'interfaccia di rete virtuale (VNI), se necessario, quindi avvia il servizio NFS su Snowball Edge. Se necessario, all'avvio del servizio NFS, fornisci un blocco di indirizzi di rete consentiti. Se non fornisci alcun indirizzo, l'accesso agli endpoint NFS sarà illimitato.

1. Usa il `describe-virtual-network-interface` comando per vedere le VNI opzioni disponibili su Snowball Edge.

```
snowballEdge describe-virtual-network-interfaces
```

Se uno o più VNI sono attivi su Snowball Edge, il comando restituisce quanto segue.

```
snowballEdge describe-virtual-network-interfaces
[
  {
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/
s.ni-8EXAMPLE8EXAMPLE8",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.0",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "EX:AM:PL:E1:23:45"
  },{
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/
s.ni-1EXAMPLE1EXAMPLE1",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.2",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "12:34:5E:XA:MP:LE"
  }
]
```

Annotate il valore del `VirtualNetworkInterfaceArn` nome del VNI da utilizzare con l'interfaccia NFS.

2. Se non ce VNI ne sono disponibili, utilizzate il `create-virtual-network-interface` comando per creare un VNI per l'interfaccia NFS. Per ulteriori informazioni, vedere [Configurazione di un'interfaccia di rete virtuale \(VNI\)](#).
3. Utilizzare il `start-service` comando per avviare il servizio NFS e associarlo al VNI. Per limitare l'accesso all'interfaccia NFS, includi i `AllowedHosts` parametri `service-configuration` e nel comando.

```
snowballEdge start-service --virtual-network-interface-arns arn-of-vni --service-id  
nfs --service-configuration AllowedHosts=CIDR-address-range
```

4. Utilizzate il `describe-service` comando per controllare lo stato del servizio. È in esecuzione quando il valore del `State` nome è `ACTIVE`.

```
snowballEdge describe-service --service-id nfs
```

Il comando restituisce lo stato del servizio, nonché l'indirizzo IP e il numero di porta dell'endpoint NFS e gli intervalli CIDR autorizzati ad accedere all'endpoint.

```
{  
  "ServiceId" : "nfs",  
  "Status" : {  
    "State" : "ACTIVE"  
  },  
  "Endpoints" : [ {  
    "Protocol" : "nfs",  
    "Port" : 2049,  
    "Host" : "192.0.2.0"  
  } ],  
  "ServiceConfiguration" : {  
    "AllowedHosts" : [ "10.24.34.0/23", "198.51.100.0/24" ]  
  }  
}
```

Montaggio degli endpoint NFS sui computer client

Dopo l'avvio dell'interfaccia NFS, monta l'endpoint come memoria locale sui computer client.

Di seguito sono riportati i comandi di montaggio predefiniti per i sistemi operativi Windows, Linux e macOS.

- Windows:

```
mount -o nolock rsize=128 wsize=128 mtype=hard nfs-interface-ip-address:/  
buckets/BucketName *
```

- Linux:

```
mount -t nfs nfs-interface-ip-address:/buckets/BucketName mount_point
```

- macOS:

```
mount -t nfs -o vers=3,rsize=131072,wsize=131072,nolocks,hard,retrans=2 nfs-  
interface-ip-address:/buckets/$bucketname mount_point
```

Arresto dell'interfaccia NFS su Snowball Edge

Al termine del trasferimento dei file tramite l'interfaccia NFS e prima di spegnere Snowball Edge, utilizzare il `stop-service` comando per interrompere il servizio NFS.

```
snowballEdge stop-service --service-id nfs
```


Utilizzo di istanze EC2 di calcolo compatibili con Amazon su Snowball Edge

Puoi eseguire istanze di calcolo EC2 compatibili con Amazon ospitate su Snowball Edge con i tipi di istanza `sbe1`, `sbe-c` e `sbe-g`. Il tipo di istanza `sbe1` funziona sui dispositivi con l'opzione Snowball Edge Storage Optimized. Il tipo di istanza `sbe-c` funziona sui dispositivi con l'opzione Snowball Edge Compute Optimized. Per una lista di tipi di istanze supportate, consulta [Quote per le istanze di calcolo su un dispositivo Snowball Edge](#).

Tutti e tre i tipi di istanza di calcolo supportati per l'uso sulle opzioni dei dispositivi Snowball Edge sono esclusivi dei dispositivi Snowball Edge. Come le loro controparti basate sul cloud, queste istanze richiedono Amazon Machine Images (AMIs) per l'avvio. Prima di creare il job Snowball Edge, scegli l'AMI come immagine di base per un'istanza nel cloud.

Per utilizzare un'istanza di calcolo su Snowball Edge, crea un lavoro per ordinare un dispositivo Snowball Edge e specifica il tuo AMI. È possibile eseguire questa operazione utilizzando il [Console di gestione della famiglia di servizi AWS Snow](#), AWS CLI, o uno dei AWS SDKs. In genere, sono presenti dei prerequisiti di manutenzione da eseguire prima di creare il processo e utilizzare le istanze.

Dopo l'arrivo del dispositivo, puoi iniziare a gestire le tue istanze AMI e. Puoi gestire le tue istanze di calcolo su Snowball Edge tramite un endpoint compatibile con Amazon EC2. Questo tipo di endpoint supporta molti comandi e azioni EC2 CLI compatibili con Amazon per AWS SDKs. Non puoi usare Snowball Edge per gestire le tue istanze AMI e quelle di calcolo. Console di gestione AWS

Quando hai finito con il dispositivo, restituiscilo a AWS. Se il dispositivo è stato utilizzato in un processo di importazione, i dati trasferiti utilizzando l'adattatore Amazon S3 o l'interfaccia NFS vengono importati in Amazon S3. Altrimenti, eseguiamo una cancellazione completa del dispositivo quando viene restituito. AWS Questa cancellazione rispetta gli standard 800-88 della National Institute of Standards and Technology (NIST).

Important

- L'utilizzo AMI della crittografia su dispositivi Snowball Edge non è supportato.
- I dati nelle istanze di calcolo in esecuzione su Snowball Edge non vengono importati in AWS.

Argomenti

- [Differenza tra istanze EC2 compatibili con Amazon EC2 e Amazon su Snowball Edge](#)
- [Prezzi delle istanze di calcolo su Snowball Edge](#)
- [Utilizzo di un'AMI EC2 compatibile con Amazon su Snowball Edge](#)
- [Importazione dell'immagine di una macchina virtuale su un dispositivo Snowball Edge](#)
- [Utilizzo delle operazioni AWS CLI e dell'API sul dispositivo Snowball Edge](#)
- [Configurazioni di rete per istanze di calcolo su Snowball Edge](#)
- [Utilizzo di SSH per connettersi alle istanze di calcolo su uno Snowball Edge](#)
- [Trasferimento di dati da istanze EC2 di calcolo compatibili a bucket S3 sullo stesso Snowball Edge](#)
- [Avvio automatico di EC2 istanze compatibili](#)
- [Utilizzo dell'endpoint EC2 compatibile con Amazon su Snowball Edge](#)
- [Istanze EC2 compatibili con avvio automatico con modelli di avvio su Snowball Edge](#)
- [Utilizzo di Instance Metadata Service for Snow con istanze EC2 compatibili con Amazon su Snowball Edge](#)
- [Utilizzo dello storage a blocchi con istanze EC2 compatibili con Amazon su Snowball Edge](#)
- [Controllo del traffico di rete con gruppi di sicurezza su Snowball Edge](#)
- [Metadati EC2 di istanza e dati utente compatibili supportati su Snowball Edge](#)
- [Arresto delle istanze EC2 compatibili in esecuzione su Snowball Edge](#)

Differenza tra istanze EC2 compatibili con Amazon EC2 e Amazon su Snowball Edge

AWS Le istanze EC2 compatibili con Snowball Edge consentono ai clienti di utilizzare e gestire istanze EC2 compatibili con Amazon utilizzando un sottoinsieme e un sottoinsieme di. EC2 APIs AMIs

Prezzi delle istanze di calcolo su Snowball Edge

Sono previsti costi aggiuntivi associati all'utilizzo delle istanze di calcolo. Per ulteriori informazioni, consultare [AWS Snowball Edge Prezzi](#).

Utilizzo di un'AMI EC2 compatibile con Amazon su Snowball Edge

Per utilizzare un'Amazon Machine Image (AMI) sul dispositivo AWS Snowball Edge, devi prima aggiungerla al dispositivo. Puoi aggiungere un AMI nei seguenti modi:

- Carica l'AMI quando ordini il dispositivo.
- Aggiungi l'AMI quando il dispositivo arriva sul tuo sito.

Le istanze di EC2 calcolo Amazon fornite con Snowball Edge vengono lanciate sulla base di Amazon EC2 AMIs che aggiungi al tuo dispositivo. EC2Compatibile con Amazon, AMIs supporta i sistemi operativi Linux e Microsoft Windows.

Linux

Sono supportati i seguenti sistemi operativi Linux:

- [Amazon Linux 2 per Snowball Edge](#)

Note

La versione più recente di questa AMI verrà fornita al momento della preparazione della spedizione di Snowball Edge. AWS Per determinare la versione di questo AMI sul dispositivo al momento della ricezione, consulta [Determinazione della versione dell'AMI Amazon Linux 2 per Snowball Edge](#).

- [CentOS 7 \(x86_64\) - con aggiornamenti HVM](#)
- Ubuntu 16.04 LTS - Xenial (HVM)

Note

Ubuntu 16.04 LTS - Le immagini Xenial (HVM) non sono più supportate in Marketplace AWS, ma sono ancora supportate per l'uso su dispositivi Snowball Edge tramite Amazon VM e in esecuzione localmente in. EC2 Import/Export AMIs

- [Ubuntu 20.04 LTS - Focal](#)
- [Ubuntu 22.04 LTS - Jammy](#)

Come best practice per la sicurezza, mantieni Amazon Linux 2 AMIs up-to-date su Snowball Edge non appena viene rilasciato il nuovo Amazon Linux AMIs 2. Consultare [Aggiornamento di Amazon Linux 2 AMIs su Snowball Edge](#).

Windows

Sono supportati i seguenti sistemi operativi Windows:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

È possibile aggiungere Windows AMIs al dispositivo importando l'immagine della macchina virtuale Windows (VM) AWS utilizzando VM Import/Export. In alternativa, puoi importare l'immagine nel tuo dispositivo subito dopo che il dispositivo è stato distribuito sul tuo sito. Per ulteriori informazioni, consulta [Aggiungere un'AMI Microsoft Windows a Snowball Edge](#).

Note

Le finestre AMIs che hanno avuto origine in non AWS possono essere aggiunte al tuo dispositivo.

AMIs importato localmente deve essere in modalità di avvio BIOS poiché UEFI non è supportato.

Snowball Edge supporta il modello Bring Your Own License (BYOL). Per ulteriori informazioni, consulta [Aggiungere un'AMI Microsoft Windows a Snowball Edge](#).

Note

AWS Le istanze EC2 compatibili con Snowball Edge consentono ai clienti di utilizzare e gestire istanze EC2 compatibili con Amazon utilizzando un sottoinsieme e un sottoinsieme di EC2 APIs AMIs

Argomenti

- [Aggiungere un'AMI durante la creazione di un lavoro per ordinare uno Snowball Edge](#)
- [Aggiungere un'AMI da Marketplace AWS a Snowball Edge](#)

- [Aggiungere un'AMI a Snowball Edge dopo aver ricevuto il dispositivo](#)
- [Aggiungere un'AMI Microsoft Windows a Snowball Edge](#)
- [Importazione di un'immagine di macchina virtuale in uno Snowball Edge](#)
- [Esportazione dell'ultima AMI Amazon Linux 2 per Snowball Edge](#)

Aggiungere un'AMI durante la creazione di un lavoro per ordinare uno Snowball Edge

Quando ordini un dispositivo, puoi aggiungerlo AMIs al dispositivo selezionandoli nella sezione Compute using EC2 instances - opzionale del. Console di gestione della famiglia di servizi AWS Snow. La sezione Compute using EC2 instances - opzionale elenca tutte le istanze AMIs che possono essere caricate sul tuo dispositivo. AMIs rientrano nelle seguenti categorie:

- AMIs da AWS Marketplace: vengono AMIs creati dall'elenco dei supportati AMIs. Per informazioni sulla creazione di un'AMI dal supporto fornito AMIs da AWS Marketplace, consulta [Aggiungere un'AMI da Marketplace AWS a Snowball Edge](#).
- AMIs caricato utilizzando VM Import/Export: quando ordini il tuo dispositivo, quelli AMIs che sono stati caricati utilizzando VM Import/Export vengono elencati nella console. Per ulteriori informazioni, vedere [Importazione di una macchina virtuale come immagine utilizzando VM Import/Export](#) nella Guida per l'utente della macchina virtuale. Import/Export Per informazioni sugli ambienti di virtualizzazione supportati, vedere Requisiti di [importazione/esportazione delle macchine virtuali](#).

Aggiungere un'AMI da Marketplace AWS a Snowball Edge

Puoi aggiungerne molti AMIs Marketplace AWS al tuo dispositivo Snowball Edge avviando l'AWS Marketplace istanza, creando un'AMI da essa e configurando l'AMI nella stessa regione da cui ordinerai il dispositivo Snow. Quindi, puoi scegliere di includere l'AMI sul dispositivo quando crei un lavoro per ordinare il dispositivo. Quando scegli un'AMI dal Marketplace, assicurati che abbia un codice prodotto e una piattaforma supportati.

Argomenti

- [Verifica dei codici di prodotto e dei dettagli della piattaforma di Marketplace AWS AMIs per Snowball Edge](#)
- [Determinazione della versione dell'AMI Amazon Linux 2 per Snowball Edge](#)
- [Configurazione dell'AMI per il dispositivo Snowball Edge](#)

Verifica dei codici di prodotto e dei dettagli della piattaforma di Marketplace AWS AMIs per Snowball Edge

Prima di iniziare il processo di aggiunta di un'AMI Marketplace AWS al dispositivo Snowball Edge, assicurati che il codice prodotto e i dettagli della piattaforma dell'AMI siano supportati nel tuo.

Regione AWS

1. Apri la EC2 console Amazon all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Dalla barra di navigazione, seleziona la regione in cui avviare le istanze e da cui creare il processo per ordinare il dispositivo Snowball Edge. Puoi selezionare qualsiasi regione disponibile, indipendentemente dalla tua posizione.
3. Nel pannello di navigazione, scegli AMIs.
4. Utilizza i filtri e le opzioni di ricerca per definire l'elenco delle opzioni visualizzate e AMIs visualizzare solo quelle AMIs che corrispondono ai tuoi criteri. Ad esempio, AMIs fornito da Marketplace AWS, scegli Immagini pubbliche. Quindi utilizzate le opzioni di ricerca per definire ulteriormente l'elenco delle immagini visualizzate AMIs:
 - (Nuova console) Scegli la barra di ricerca e, dal menu, scegli l'alias del proprietario, quindi l'operatore = e infine il valore amazon.
 - (Vecchia console) Scegliere la barra di ricerca e dal menu scegliere Owner (Proprietario), quindi il valore Amazon images (Immagini Amazon)

Note

AMIs da Marketplace AWS includere aws-marketplace nella colonna Source.

5. Nella colonna ID AMI, scegli l'ID AMI dell'AMI.
6. Nel riepilogo dell'immagine dell'AMI, assicurati che i codici prodotto siano supportati dalla tua regione. Per ulteriori informazioni, consulta la tabella seguente.

Codici di prodotto Marketplace AWS AMI supportati

Sistema operativo AMI	Codice del prodotto
Server Ubuntu 14.04 LTS	b3dl4415quatdnd14qa6kcu45
CentOS 7 (x86_64)	aw0evgkw8e5c1q413zgy5pjce

Sistema operativo AMI	Codice del prodotto
Ubuntu 16.04 LTS	csv6h7oyg29b7epjzg7qdr7no
Amazon Linux 2	avyfzznywektml5qv5f57ska
Ubuntu 20.04 LTS	a8jyynf4hjutohctm41o2z18m
Ubuntu 22.04 LTS	47xbqns9xujfkkjt189a13aqe

7. Quindi, assicurati anche che i dettagli della piattaforma contengano una delle voci dell'elenco seguente.

- Amazon Linux, Ubuntu o Debian
- Red Hat Linux bring-your-own-license
- Amazon RDS per Oracle bring-your-own-license
- Windows bring-your-own-license

Determinazione della versione dell'AMI Amazon Linux 2 per Snowball Edge

Usa la procedura seguente per determinare la versione dell'AMI Amazon Linux 2 per Snowball Edge su Snowball Edge. Installa la versione più recente di AWS CLI prima di continuare. Per ulteriori informazioni, consulta [Installare o aggiornare alla versione più recente di AWS CLI nella Guida per l'AWS Command Line Interface utente](#).

- Usa il `describe-images` AWS CLI comando per vedere la descrizione dell'AMI. La versione è contenuta nella descrizione. Fornisci il certificato a chiave pubblica del passaggio precedente. Per ulteriori informazioni, vedere [describe-images](#) nel Command Reference. AWS CLI

```
aws ec2 describe-images --endpoint http://snow-device-ip:8008 --region snow
```

Example dell'output del comando **describe-images**

```
{
  "Images": [
```

```

    {
      "CreationDate": "2024-02-12T23:24:45.705Z",
      "ImageId": "s.ami-02ba84cb87224e16e",
      "Public": false,
      "ProductCodes": [
        {
          "ProductCodeId": "avyfzznywektkgl5qv5f57ska",
          "ProductCodeType": "marketplace"
        }
      ],
      "State": "AVAILABLE",
      "BlockDeviceMappings": [
        {
          "DeviceName": "/dev/xvda",
          "Ebs": {
            "DeleteOnTermination": true,
            "Iops": 0,
            "SnapshotId": "s.snap-0efb49f2f726fde63",
            "VolumeSize": 8,
            "VolumeType": "sbp1"
          }
        }
      ],
      "Description": "Snow Family Amazon Linux 2 AMI 2.0.20240131.0 x86_64
HVM gp2",
      "EnaSupport": false,
      "Name": "amzn2-ami-snow-family-hvm-2.0.20240131.0-x86_64-gp2-
b7e7f8d2-1b9e-4774-a374-120e0cd85d5a",
      "RootDeviceName": "/dev/xvda"
    }
  ]
}

```

In questo esempio, la versione dell'AMI Amazon Linux 2 per Snowball Edge è.
2.0.20240131.0 Si trova nel valore del Description nome.

Configurazione dell'AMI per il dispositivo Snowball Edge

1. Apri la EC2 console Amazon all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Avvia una nuova istanza di un'AMI supportata in Marketplace AWS.

 Note

Quando avvii l'istanza, assicurati che la dimensione di archiviazione che assegni all'istanza sia appropriata per il tuo caso d'uso. Nella EC2 console Amazon, esegui questa operazione nella fase Aggiungi spazio di archiviazione.

3. Installa e configura le applicazioni che desideri eseguire su Snowball Edge e assicurati che funzionino come previsto.

 Important

- Sono AMIs supportati solo volumi singoli.
- Il volume EBS dell'AMI deve essere pari o inferiore a 10 TB. Ti consigliamo di fornire la dimensione del volume EBS necessaria per i dati nell'AMI. Ciò contribuirà a ridurre il tempo necessario per esportare l'AMI e caricarla sul dispositivo. Puoi ridimensionare o aggiungere altri volumi all'istanza dopo la distribuzione del dispositivo.
- L'istantanea EBS nell'AMI non deve essere crittografata.

4. Crea una copia del file PEM o PPK che hai usato per la coppia di chiavi SSH quando hai creato questa istanza. Salva questo file sul server che intendi utilizzare per comunicare con il dispositivo Snowball Edge. Prendi nota del percorso di questo file perché ne avrai bisogno quando usi SSH per connetterti all'istanza EC2 compatibile sul tuo dispositivo.

 Important

Se non segui questa procedura, non puoi connetterti alle istanze con SSH quando ricevi il dispositivo Snowball Edge.

5. Salvare l'istanza come AMI. Per ulteriori informazioni, consulta la [Amazon EC2 User Guide for Linux Instances](#) nella Amazon EC2 User Guide.
6. Ripeti i passaggi da 1 a 4 per ciascuna delle istanze a cui desideri connetterti tramite SSH. Assicurati di fare copie di ciascuna coppia di chiavi SSH e tieni traccia di AMIs quella a cui sono associate.
7. Ora, quando ordini il tuo dispositivo, questi possono essere AMIs aggiunti al tuo dispositivo.

Aggiungere un'AMI a Snowball Edge dopo aver ricevuto il dispositivo

Quando il dispositivo arriva sul tuo sito, puoi aggiungerne uno nuovo AMIs . Per istruzioni, consultare [Importazione dell'immagine di una macchina virtuale su un dispositivo Snowball Edge](#). Tieni presente che, sebbene tutti VMs siano supportati, solo quelli supportati sono AMIs stati testati per verificarne la piena funzionalità.

Note

Quando usi una macchina virtuale Import/Export per aggiungere AMIs al tuo dispositivo o importi una macchina virtuale dopo VMs che il dispositivo è stato distribuito, puoi aggiungerla utilizzando qualsiasi sistema operativo. Tuttavia, solo i sistemi operativi supportati sono stati testati e convalidati su Snowball Edge. L'utente è responsabile del rispetto dei termini e delle condizioni di qualsiasi sistema operativo o software presente nell'immagine virtuale importata sul dispositivo.

Important

AWS Affinché i servizi funzionino correttamente su Snowball Edge, è necessario consentire le porte per i servizi. Per informazioni dettagliate, consultare [Requisiti delle porte per AWS i servizi su Snowball Edge](#).

Aggiungere un'AMI Microsoft Windows a Snowball Edge

Per le macchine virtuali (VMs) che utilizzano un sistema operativo Windows supportato, puoi aggiungere l'AMI importando l'immagine della macchina virtuale Windows AWS utilizzando VM Import/Export o importandola nel tuo dispositivo subito dopo la distribuzione sul tuo sito.

Modello di licenza Bring Your Own License (BYOL)

Snowball Edge supporta l'importazione di Microsoft AMIs Windows sul dispositivo con una licenza propria. Bring Your Own License (BYOL) è il processo di trasferimento di un'AMI di tua proprietà con la relativa licenza locale. AWS AWS fornisce opzioni di distribuzione condivise e dedicate per l'opzione BYOL.

È possibile aggiungere l'immagine della macchina virtuale Windows al dispositivo AWS importandola su VM Import/Export o importandola nel dispositivo subito dopo la distribuzione sul sito. Non puoi

aggiungere Windows che ha avuto origine in. AMIs AWS Pertanto, devi creare e importare la tua immagine di macchina virtuale Windows e portare la tua licenza se desideri utilizzare l'AMI sul tuo dispositivo Snowball Edge. Per ulteriori informazioni sulle licenze Windows e sul BYOL, consulta [Amazon Web Services e Microsoft: domande frequenti](#).

Creazione di un'immagine di macchina virtuale Windows da importare in uno Snowball Edge

Per creare un'immagine di macchina virtuale Windows, è necessario un ambiente di virtualizzazione, ad esempio VirtualBox, supportato per i sistemi operativi Windows e macOS. Quando crei una macchina virtuale per dispositivi Snow, ti consigliamo di allocare almeno due core con almeno 4 GB di RAM. Quando la macchina virtuale è attiva e funzionante, è necessario installare il sistema operativo (Windows Server 2012, 2016 o 2019). Per installare i driver necessari per il dispositivo Snowball Edge, segui le istruzioni in questa sezione.

Affinché un'AMI Windows funzioni su un dispositivo Snow, è necessario aggiungere VirtIO, FLR, NetVCM, Vioinput, Viorng, Vioscsi, Vioserial e i driver. VioStor È possibile [scaricare un Microsoft Software Installer \(virtio-win-guest-tools-installer\)](#) per installare questi driver su immagini Windows dal repository in poi. [virtio-win-pkg-scripts](#) GitHub

Note

Se prevedi di importare l'immagine della macchina virtuale direttamente sul dispositivo Snow distribuito, il file di immagine della macchina virtuale deve essere in formato RAW.

Per creare un'immagine Windows

1. Sul tuo computer Microsoft Windows, scegli Start e accedi **devmgmt.msc** per aprire Gestione dispositivi.
2. Nel menu principale, scegli Azioni, quindi scegli Aggiungi hardware legacy.

Note

Per Windows 11, seleziona innanzitutto qualsiasi dispositivo nel pannello sottostante prima che l'opzione Aggiungi hardware legacy venga visualizzata nel menu Azioni.

3. Nella procedura guidata, scegli Avanti.

4. Scegli Installa l'hardware che ho selezionato manualmente da un elenco (avanzato) e scegli Avanti.
5. Scegli Mostra tutti i dispositivi e scegli Avanti.
6. Scegli Have Disk, apri l'elenco Copia i file del produttore e accedi al file ISO.
7. Nel file ISO, accedi alla `Driver\W2K8R2\amd64` directory, quindi trova il `.INF` file.
8. Scegliete il file.INF, scegliete Apri, quindi fate clic su OK.
9. Quando viene visualizzato il nome del driver, scegliete Avanti, quindi scegliete Avanti altre due volte. Quindi scegli Finish (Fine).

In questo modo viene installato un dispositivo che utilizza il nuovo driver. L'hardware effettivo non esiste, quindi vedrai un punto esclamativo giallo che indica un problema sul dispositivo. È necessario risolvere questo problema.

Per risolvere il problema hardware

1. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per il dispositivo con il punto esclamativo.
2. Scegliete Disinstalla, deselezionate Elimina il software del driver per questo dispositivo e scegliete OK.

Il driver è installato e sei pronto per avviare l'AMI sul tuo dispositivo.

Importazione di un'immagine di macchina virtuale in uno Snowball Edge

Dopo aver preparato l'immagine della macchina virtuale, puoi utilizzare una delle opzioni per importare l'immagine sul dispositivo.

- Nel cloud utilizzando VM Import/Export: quando importi l'immagine della macchina virtuale AWS e la registri come AMI, puoi aggiungerla al tuo dispositivo quando effettui un ordine da Console di gestione della famiglia di servizi AWS SnowPer ulteriori informazioni, vedere [Importazione di una macchina virtuale come immagine utilizzando VM Import/Export](#) nella Guida per l'utente della macchina virtuale. Import/Export
- A livello locale sul dispositivo distribuito presso il sito: è possibile importare l'immagine della macchina virtuale direttamente nel dispositivo utilizzando o (). AWS OpsHub AWS Command Line Interface AWS CLI

Per informazioni sull'utilizzo AWS OpsHub, consulta [Utilizzo locale di istanze EC2 di calcolo compatibili con Amazon](#).

Per informazioni sull'utilizzo di, consulta. AWS CLI [Importazione dell'immagine di una macchina virtuale su un dispositivo Snowball Edge](#)

Esportazione dell'ultima AMI Amazon Linux 2 per Snowball Edge

Per aggiornare Amazon Linux 2 AMIs alla versione più recente, esporta prima l'ultima immagine di macchina virtuale Amazon Linux 2 da Marketplace AWS, quindi importa l'immagine della macchina virtuale nel dispositivo Snow.

1. Usa il `ssm get-parameters` AWS CLI comando per trovare l'ID immagine più recente dell'AMI Amazon Linux 2 in Marketplace AWS.

```
aws ssm get-parameters --names /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 --query 'Parameters[0].[Value]' --region your-region
```

Il comando restituisce l'ID immagine più recente dell'AMI. Ad esempio, `ami-0ccb473bada910e74`.

2. Esporta l'immagine Amazon Linux 2 più recente. Consulta [Esportazione di una macchina virtuale direttamente da un'Amazon Machine Image \(AMI\)](#) nella Amazon EC2 User Guide. Usa l'ID immagine più recente dell'AMI Amazon Linux 2 come valore del `image-id` parametro del `ec2 export-image` comando.
3. Importa l'immagine della macchina virtuale nel dispositivo Snow usando AWS CLI o AWS OpsHub.
 - Per informazioni sull'utilizzo AWS CLI, vedere [Importazione dell'immagine di una macchina virtuale su un dispositivo Snowball Edge](#).
 - Per informazioni sull'utilizzo AWS OpsHub, vedere [Importazione di un'immagine come EC2 AMI compatibile con Amazon con AWS OpsHub](#).

Importazione dell'immagine di una macchina virtuale su un dispositivo Snowball Edge

Puoi utilizzare il Import/Export servizio AWS CLI and VM per importare un'immagine di macchina virtuale (VM) nel dispositivo Snowball Edge come Amazon Machine Image (AMI). Dopo aver importato un'immagine VM, registra l'immagine come AMI e avviala come istanza compatibile con Amazon EC2.

Puoi aggiungere qualcosa AMIs da Amazon EC2 al dispositivo quando crei un lavoro per ordinare un dispositivo Snowball Edge. Utilizzare questa procedura dopo aver ricevuto il dispositivo Snowball Edge. Per ulteriori informazioni, consulta [Scelta delle opzioni di elaborazione e archiviazione](#).

Puoi anche utilizzarlo AWS OpsHub per caricare il file di immagine della macchina virtuale. Per ulteriori informazioni, consulta [Importazione di un'immagine nel dispositivo come EC2 AMI compatibile con Amazon](#) in questa guida.

Argomenti

- [Passaggio 1: preparare l'immagine della macchina virtuale e caricarla sul dispositivo Snowball Edge](#)
- [Fase 2: configurare le autorizzazioni necessarie su Snowball Edge](#)
- [Fase 3: Importazione dell'immagine della macchina virtuale come istantanea su Snowball Edge](#)
- [Fase 4: Registrare l'istantanea come AMI su Snowball Edge](#)
- [Fase 5: Avviare un'istanza dall'AMI su Snowball Edge](#)
- [Azioni AMI aggiuntive per Snowball Edge](#)

Passaggio 1: preparare l'immagine della macchina virtuale e caricarla sul dispositivo Snowball Edge

Prepara l'immagine della macchina virtuale esportando un'immagine della macchina virtuale da un' EC2 ami Amazon o da un'istanza nella macchina virtuale in Cloud AWS uso o generando l'immagine della macchina virtuale Import/Export localmente utilizzando la piattaforma di virtualizzazione che preferisci.

Per esportare un' EC2 istanza Amazon come immagine di macchina virtuale utilizzando VM Import/Export, consulta Esportazione di [un'istanza come macchina virtuale utilizzando VM Import/Export](#)

[nella VM User Guide](#). Import/Export Per esportare un' EC2 AMI Amazon come immagine di macchina virtuale utilizzando VM Import/Export, consulta Esportazione di [una macchina virtuale direttamente da un'Amazon Machine Image \(AMI\) nella VM](#) User Guide. Import/Export

Se generi un'immagine VM dal tuo ambiente locale, assicurati che l'immagine sia configurata per l'uso come AMI sul dispositivo Snowball Edge. Potrebbe essere necessario configurare i seguenti elementi, a seconda dell'ambiente.

- Configurare e aggiornare il sistema operativo.
- Imposta un nome host.
- Assicurati che il Network Time Protocol (NTP) sia configurato.
- Includi le chiavi pubbliche SSH, se necessario. Crea copie locali delle coppie di chiavi. Per ulteriori informazioni, consulta [Uso di SSH per connettersi alle istanze di calcolo su Snowball Edge](#).
- Installa e configura qualsiasi software che utilizzerai sul dispositivo Snowball Edge.

Note

Tieni presente le seguenti limitazioni quando prepari un'istantanea del disco per un dispositivo Snowball Edge.

- Attualmente Snowball Edge supporta solo l'importazione di istantanee in formato immagine RAW.
- Attualmente Snowball Edge supporta solo l'importazione di istantanee con dimensioni da 1 GB a 1 TB.

Caricamento di un'immagine di macchina virtuale in un bucket Amazon S3 sul dispositivo Snowball Edge

Dopo aver preparato un'immagine della macchina virtuale, caricala in un bucket S3 sul dispositivo o sul cluster Snowball Edge. Puoi utilizzare l'adattatore S3 o lo storage compatibile con Amazon S3 su Snowball Edge per caricare lo snapshot.

Per caricare l'immagine della macchina virtuale utilizzando l'adattatore S3

- Usa il `cp` comando per copiare il file di immagine della macchina virtuale in un bucket sul dispositivo.

```
aws s3 cp image-path s3://S3-bucket-name --endpoint http://S3-object-API-endpoint:443 --profile profile-name
```

Per ulteriori informazioni, consulta [AWS CLI Comandi supportati](#) in questa guida.

Per caricare l'immagine della macchina virtuale utilizzando lo storage compatibile con Amazon S3 su Snowball Edge

- Usa il `put-object` comando per copiare il file di istantanea in un bucket sul dispositivo.

```
aws s3api put-object --bucket bucket-name --key path-to-snapshot-file --body snapshot-file --endpoint-url s3api-endpoint-ip --profile your-profile
```

Per ulteriori informazioni, consulta [Lavorare con oggetti S3 su un dispositivo Snowball](#) Edge.

Fase 2: configurare le autorizzazioni necessarie su Snowball Edge

Affinché l'importazione abbia esito positivo, è necessario configurare le autorizzazioni per la macchina virtuale Import/Export sul dispositivo Snowball Edge, su Amazon EC2 e sull'utente.

Note

I ruoli di servizio e le politiche che forniscono queste autorizzazioni si trovano sul dispositivo Snowball Edge.

Autorizzazioni richieste per la macchina virtuale Import/Export su uno Snowball Edge

Prima di iniziare il processo di importazione, devi creare un ruolo IAM con una policy di fiducia che consenta alla macchina virtuale Import/Export sul dispositivo Snowball Edge di assumere il ruolo. Al ruolo vengono concesse autorizzazioni aggiuntive per consentire alla macchina virtuale Import/Export sul dispositivo di accedere all'immagine memorizzata nel bucket S3 sul dispositivo.

Crea un file json di policy di fiducia

Di seguito è riportato un esempio di policy di fiducia da allegare al ruolo in modo che VM Import/Export possa accedere allo snapshot che deve essere importato dal bucket S3.

JSON

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

Crea un ruolo con il file json della policy di fiducia

Il nome del ruolo può essere vmimport. Puoi cambiarlo usando l'opzione `--role-name` nel comando:

```
aws iam create-role --role-name role-name --assume-role-policy-document file:///trust-  
policy-json-path --endpoint http://snowball-ip:6078 --region snow --profile profile-  
name
```

Di seguito è riportato un esempio di output del comando. `create-role`

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

```

    },
    "MaxSessionDuration":3600,
    "RoleId":"AROACEMGEZDGNBVG3TQ0JQGEZAAAABQBB6NSGNAAAABPSVLTREPY3FPAFOLKJ3",
    "CreateDate":"2022-04-19T22:17:19.823Z",
    "RoleName":"vmimport",
    "Path":"/",
    "Arn":"arn:aws:iam::123456789012:role/vmimport"
  }
}

```

Creare una politica per il ruolo

La seguente policy di esempio ha le autorizzazioni minime richieste per accedere ad Amazon S3. Cambia il nome del bucket Amazon S3 con quello che contiene le tue immagini. Per un dispositivo Snowball Edge autonomo, *snow-id* passa al tuo Job ID. Per un cluster di dispositivi, passa *snow-id* all'ID del cluster. Puoi anche utilizzare i prefissi per restringere ulteriormente la posizione da cui VM Import/Export può importare le istantanee. Crea un file json di policy come questo.

JSON

```

{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetMetadata"
      ],
      "Resource":[
        "arn:aws:s3:snow:account-id:snow/snow-id/bucket/import-snapshot-  
bucket-name",
        "arn:aws:s3:snow:account-id:snow/snow-id/bucket/import-snapshot-  
bucket-name/*"
      ]
    }
  ]
}

```

Crea una politica con il file di policy:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-  
file-path --endpoint http://snowball-ip:6078 --region snow --profile profile-name
```

Di seguito è riportato un esempio di output del comando create-policy.

```
{  
  "Policy":{  
    "PolicyName":"vmimport-resource-policy",  
    "PolicyId":"ANPACEMGEZDGNBVG3TQ0JQGEZAAAAB00EE3IIHAAAABWZJPI2VW4UUTFEDBC2R",  
    "Arn":"arn:aws:iam::123456789012:policy/vmimport-resource-policy",  
    "Path":"/",  
    "DefaultVersionId":"v1",  
    "AttachmentCount":0,  
    "IsAttachable":true,  
    "CreateDate":"2020-07-25T23:27:35.690000+00:00",  
    "UpdateDate":"2020-07-25T23:27:35.690000+00:00"  
  }  
}
```

Allega la policy al ruolo

Allega una policy al ruolo precedente e concedi le autorizzazioni per accedere alle risorse richieste. Ciò consente al Import/Export servizio VM locale di scaricare lo snapshot da Amazon S3 sul dispositivo.

```
aws iam attach-role-policy --role-name role-name --policy-arn  
arn:aws:iam::123456789012:policy/policy-name --endpoint http://snowball-ip:6078 --  
region snow --profile profile-name
```

Autorizzazioni richieste dal chiamante su Snowball Edge

Oltre al ruolo che deve assumere la macchina virtuale Snowball Edge, è necessario assicurarsi che l'utente disponga delle autorizzazioni che gli consentano di passare il ruolo a Import/Export VMIE. Se si utilizza l'utente root predefinito per eseguire l'importazione, l'utente root dispone già di tutte le autorizzazioni necessarie, quindi è possibile saltare questo passaggio e andare al passaggio 3.

Associa le seguenti due autorizzazioni IAM all'utente che esegue l'importazione.

- `pass-role`

- get-role

Crea una politica per il ruolo

Di seguito è riportato un esempio di policy che consente a un utente di eseguire le pass-role azioni get-role and per il ruolo IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:GetRole",
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::*:role/snowball*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "importexport.amazonaws.com"
        }
      }
    }
  ]
}
```

Crea una policy con il file di policy:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-  
file-path --endpoint http://snowball-ip:6078 --region snow --profile profile-name
```

Di seguito è riportato un esempio di output del comando create-policy.

```
{
  "Policy": {
```

```

    "PolicyName": "caller-policy",
    "PolicyId": "ANPACEMGEZDGNBVG3TQ0JQGEZAAAAAB000TU0E3AAAAAAPPBEUM7Q7ARPUE53C6R",
    "Arn": "arn:aws:iam::123456789012:policy/caller-policy",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "CreateDate": "2020-07-30T00:58:25.309000+00:00",
    "UpdateDate": "2020-07-30T00:58:25.309000+00:00"
  }
}

```

Una volta generata la policy, collega la policy agli utenti IAM che chiameranno l' EC2 API Amazon o l'operazione CLI per importare lo snapshot.

```

aws iam attach-user-policy --user-name your-user-name --policy-arn
arn:aws:iam::123456789012:policy/policy-name --endpoint http://snowball-ip:6078 --
region snow --profile profile-name

```

Autorizzazioni necessarie per chiamare Amazon EC2 APIs su Snowball Edge

Per importare uno snapshot, l'utente IAM deve disporre delle autorizzazioni. `ec2:ImportSnapshot`. Se non è necessario limitare l'accesso all'utente, puoi utilizzare le `ec2:*` autorizzazioni per concedere l'accesso completo ad Amazon EC2. Di seguito sono elencate le autorizzazioni che possono essere concesse o limitate per Amazon EC2 sul tuo dispositivo. Crea un file di policy con il contenuto mostrato:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ImportSnapshot",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:CancelImportTask",
        "ec2:DescribeSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:RegisterImage",

```

```

        "ec2:DescribeImages",
        "ec2:DeregisterImage"
    ],
    "Resource": "*"
}
]
}

```

Crea un criterio con il file di policy:

```
aws iam create-policy --policy-name policy-name --policy-document file:///policy-json-  
file-path --endpoint http://snowball-ip:6078 --region snow --profile profile-name
```

Di seguito è riportato un esempio di output del comando create-policy.

```

{
  "Policy":
    {
      "PolicyName": "ec2-import.json",
      "PolicyId":
        "ANPACEMGEZDGNBVG3TQ0JQGEZAAAABQBGPDQC5AAAAATYN62UNBFYTF5WVCSCZS",
      "Arn": "arn:aws:iam::123456789012:policy/ec2-import.json",
      "Path": "/",
      "DefaultVersionId": "v1",
      "AttachmentCount": 0,
      "IsAttachable": true,
      "CreateDate": "2022-04-21T16:25:53.504000+00:00",
      "UpdateDate": "2022-04-21T16:25:53.504000+00:00"
    }
}

```

Una volta generata la policy, collega la policy agli utenti IAM che chiameranno l' EC2 API Amazon o l'operazione CLI per importare lo snapshot.

```
aws iam attach-user-policy --user-name your-user-name --policy-arn  
arn:aws:iam::123456789012:policy/policy-name --endpoint http://snowball-ip:6078 --  
region snow --profile profile-name
```

Fase 3: Importazione dell'immagine della macchina virtuale come istantanea su Snowball Edge

Il passaggio successivo consiste nell'importare l'immagine della macchina virtuale come istantanea sul dispositivo. Il valore del S3Bucket parametro è il nome del bucket che contiene l'immagine della macchina virtuale. Il valore del S3Key parametro è il percorso del file di immagine della macchina virtuale in questo bucket.

```
aws ec2 import-snapshot --disk-container "Format=RAW,UserBucket={S3Bucket=bucket-name,S3Key=image-file}" --endpoint http://snowball-ip:8008 --region snow --profile profile-name
```

Per ulteriori informazioni, vedere [import-snapshot](#) nel Command Reference. AWS CLI

Questo comando non supporta le seguenti opzioni.

- [--client-data value]
- [--client-token] value
- [--dry-run]
- [--no-dry-run]
- [--encrypted]
- [--no-encrypted]
- [--kms-key-id value]
- [--tag-specificazioni] value

Example uscita del comando **import-snapshot**

```
{
  "ImportTaskId": "s.import-snap-1234567890abc",
  "SnapshotTaskDetail": {
    "DiskImageSize": 2.0,
    "Encrypted": false,
    "Format": "RAW",
    "Progress": "3",
    "Status": "active",
    "StatusMessage": "pending",
```

```
"UserBucket":{
  "S3Bucket":"bucket",
  "S3Key":"vmimport/image01"
}
}
```

Note

Attualmente Snowball Edge consente l'esecuzione di un solo processo di importazione attivo alla volta, per dispositivo. Per iniziare una nuova attività di importazione, attendi il completamento dell'operazione corrente o scegli un altro nodo disponibile in un cluster. Puoi anche scegliere di annullare l'importazione corrente, se lo desideri. Per evitare ritardi, non riavviare il dispositivo Snowball Edge mentre l'importazione è in corso. Se riavvii il dispositivo, l'importazione avrà esito negativo e l'avanzamento verrà eliminato quando il dispositivo diventa accessibile. Per verificare lo stato dell'operazione di importazione delle istantanee, utilizzate il seguente comando:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids id --endpoint
http://snowball-ip:8008 --region snow --profile profile-name
```

Fase 4: Registrare l'istananea come AMI su Snowball Edge

Quando l'importazione dell'istananea sul dispositivo ha esito positivo, puoi registrarla utilizzando il comando `register-image`

Note

È possibile registrare un'AMI solo quando tutte le relative istantanee sono disponibili.

Per ulteriori informazioni, consulta [register-image](#) nel Command Reference. AWS CLI

Example del comando **register-image**

```
aws ec2 register-image \
--name ami-01 \
```



```
--description my-ami-01 \
--block-device-mappings "[{\"DeviceName\": \"/dev/sda1\", \"Ebs\": {\"Encrypted\": false,
\"DeleteOnTermination\": true, \"SnapshotId\": \"snapshot-id\", \"VolumeSize\": 30}}]" \
--root-device-name /dev/sda1 \
--endpoint http://snowball-ip:8008 \
--region snow \
--profile profile-name
```

Di seguito è riportato un esempio di mappatura dei dispositivi a blocchi in formato JSON. Per ulteriori informazioni, vedete il [block-device-mapping parametro register-image nel Command Reference](#).

AWS CLI

```
[
  {
    "DeviceName": "/dev/sda",
    "Ebs": {
      "Encrypted": false,
      "DeleteOnTermination": true,
      "SnapshotId": "snapshot-id",
      "VolumeSize": 30
    }
  }
]
```

Example del comando **register-image**

```
{
  "ImageId": "s.ami-8de47d2e397937318"
}
```

Fase 5: Avviare un'istanza dall'AMI su Snowball Edge

Per avviare un'istanza, consulta [run-instances](#) nel Command Reference. AWS CLI

Il valore del `image-id` parametro è il valore del ImageId nome come output del comando. `register-image`

```
aws ec2 run-instances --image-id image-id --instance-type instance-type --endpoint
http://snowball-ip:8008 --region snow --profile profile-name
```

```
{
  "Instances":[
    {
      "SourceDestCheck":false,
      "CpuOptions":{
        "CoreCount":1,
        "ThreadsPerCore":2
      },
      "InstanceId":"s.i-12345a73123456d1",
      "EnaSupport":false,
      "ImageId":"s.ami-1234567890abcdefg",
      "State":{
        "Code":0,
        "Name":"pending"
      },
      "EbsOptimized":false,
      "SecurityGroups":[
        {
          "GroupName":"default",
          "GroupId":"s.sg-1234567890abc"
        }
      ],
      "RootDeviceName":"/dev/sda1",
      "AmiLaunchIndex":0,
      "InstanceType":"sbe-c.large"
    }
  ],
  "ReservationId":"s.r-1234567890abc"
}
```

Note

Puoi anche usarlo AWS OpsHub per avviare l'istanza. Per ulteriori informazioni, consulta [Avvio di un'istanza EC2 compatibile con Amazon](#) in questa guida.

Azioni AMI aggiuntive per Snowball Edge

È possibile utilizzare AWS CLI comandi aggiuntivi per monitorare lo stato di importazione delle istantanee, ottenere dettagli sulle istantanee importate, annullare l'importazione di un'istanza ed eliminare o annullare la registrazione delle istantanee dopo l'importazione.

Monitoraggio dello stato di importazione delle istantanee su Snowball Edge

Per vedere lo stato attuale dell'avanzamento dell'importazione, puoi eseguire il `EC2 describe-import-snapshot-tasks` comando Amazon. Questo comando supporta l'impaginazione e il filtraggio su `task-state`

Example del comando **describe-import-snapshot-tasks**

```
aws ec2 describe-import-snapshot-tasks --import-task-ids id --endpoint http://snowball-ip:8008 --region snow --profile profile-name
```

Example dell'output del **describe-import-snapshot-tasks** comando

```
{
  "ImportSnapshotTasks": [
    {
      "ImportTaskId": "s.import-snap-8f6bfd7fc9ead9aca",
      "SnapshotTaskDetail": {
        "Description": "Created by AWS-Snowball-VMImport service for s.import-snap-8f6bfd7fc9ead9aca",
        "DiskImageSize": 8.0,
        "Encrypted": false,
        "Format": "RAW",
        "Progress": "3",
        "SnapshotId": "s.snap-848a22d7518ad442b",
        "Status": "active",
        "StatusMessage": "pending",
        "UserBucket": {
          "S3Bucket": "bucket1",
          "S3Key": "image1"
        }
      }
    }
  ]
}
```

Note

Questo comando mostra solo l'output delle attività che sono state completate con successo o che sono state contrassegnate come eliminate negli ultimi 7 giorni. Il filtraggio supporta `Name=task-state` solo, `Values=active | deleting | deleted | completed`

Questo comando non supporta i seguenti parametri.

- [--dry-run]
- [--no-dry-run]

Annullamento di un'operazione di importazione su Snowball Edge

Per annullare un'operazione di importazione, esegui il comando. `cancel-import-task`

Example del **cancel-import-task** comando

```
aws ec2 cancel-import-task --import-task-id import-task-id --endpoint http://snowball-  
ip:8008 --region snow --profile profile-name
```

Example dell'output del **cancel-import-task** comando

```
{  
  "ImportTaskId": "s.import-snap-8234ef2a01cc3b0c6",  
  "PreviousState": "active",  
  "State": "deleting"  
}
```

Note

È possibile annullare solo le attività che non sono in uno stato completato.

Questo comando non supporta i seguenti parametri.

- [--dry-run]
- [--no-dry-run]

Descrizione delle istantanee su Snowball Edge

Dopo aver importato un'istanza, puoi utilizzare questo comando per descriverla. Per filtrare le istantanee, è possibile inviarle l'ID dell'istanza della precedente risposta all'attività di importazione. `snapshot-ids` Questo comando supporta l'impaginazione e il filtro `suvolume-id`, `status` e `start-time`

Example del **describe-snapshots** comando

```
aws ec2 describe-snapshots --snapshot-ids snapshot-id --endpoint http://snowball-ip:8008 --region snow --profile profile-name
```

Example dell'output del **describe-snapshots** comando

```
{
  "Snapshots": [
    {
      "Description": "Created by AWS-Snowball-VMImport service for s.import-snap-8f6bfd7fc9ead9aca",
      "Encrypted": false,
      "OwnerId": "123456789012",
      "SnapshotId": "s.snap-848a22d7518ad442b",
      "StartTime": "2020-07-30T04:31:05.032000+00:00",
      "State": "completed",
      "VolumeSize": 8
    }
  ]
}
```

Questo comando non supporta i seguenti parametri.

- [--restorable-by-user-ids value]
- [--dry-run]
- [--no-dry-run]

Eliminazione di un'istantanea da un dispositivo Snowball Edge

Per rimuovere le istantanee che possiedi e che non ti servono più, puoi usare il comando. **delete-snapshot**

Example del comando **delete-snapshot**

```
aws ec2 delete-snapshot --snapshot-id snapshot-id --endpoint http://snowball-ip:8008 --region snow --profile profile-name
```

 Note

Snowball Edge non supporta l'eliminazione di istantanee che si trovano in stato PENDING o che sono designate come dispositivo root per un'AMI.

Questo comando non supporta i seguenti parametri.

- [--dry-run]
- [--no-dry-run]

Annullamento della registrazione di un'AMI su Snowball Edge

Per annullare la registrazione AMIs che non ti serve più, puoi eseguire il comando. `deregister-image` L'annullamento della registrazione di un AMI che si trova nello stato In sospeso non è attualmente supportato.

Example del comando **deregister-image**

```
aws ec2 deregister-image --image-id image-id --endpoint http://snowball-ip:8008 --  
region snow --profile profile-name
```

Questo comando non supporta i seguenti parametri.

- [--dry-run]
- [--no-dry-run]

Utilizzo delle operazioni AWS CLI e dell'API sul dispositivo Snowball Edge

Quando utilizzi le operazioni AWS Command Line Interface (AWS CLI) o API per emettere EC2 comandi IAM, Amazon S3 e Amazon su Snowball Edge, devi specificare come "» `region snow` È possibile eseguire questa operazione utilizzando `aws configure` o all'interno del comando stesso, come negli esempi seguenti.

```
aws configure --profile ProfileName
```

```
AWS Access Key ID [None]: defgh
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Or

```
aws s3 ls --endpoint http://192.0.2.0:8080 --region snow --profile ProfileName
```

Configurazioni di rete per istanze di calcolo su Snowball Edge

Dopo aver avviato l'istanza di calcolo su Snowball Edge, è necessario fornirle un indirizzo IP creando un'interfaccia di rete. Snowball Edges supporta due tipi di interfacce di rete, un'interfaccia di rete virtuale e un'interfaccia di rete diretta.

Interfaccia di rete virtuale (VNI): un'interfaccia di rete virtuale è l'interfaccia di rete standard per la connessione a un'istanza EC2 compatibile su Snowball Edge. È necessario creare un VNI per ciascuna delle istanze EC2 compatibili, indipendentemente dal fatto che si utilizzi o meno anche un'interfaccia di rete diretta. Il traffico che attraversa un VNI è protetto dai gruppi di sicurezza che hai impostato. È possibile eseguire l'associazione solo VNIs alla porta di rete fisica utilizzata per controllare Snowball Edge.

Note

VNI utilizzerà la stessa interfaccia fisica (RJ45SFP+ o QSFP) utilizzata per gestire Snowball Edge. La creazione di un VNI su un'interfaccia fisica diversa da quella utilizzata per la gestione dei dispositivi potrebbe portare a risultati imprevisti.

Interfaccia di rete diretta (DNI): un'interfaccia di rete diretta (DNI) è una funzionalità di rete avanzata che consente casi d'uso come flussi multicast, routing transitivo e bilanciamento del carico. Fornendo istanze con accesso alla rete di livello 2 senza alcuna traduzione o filtro intermediario, è possibile ottenere una maggiore flessibilità nella configurazione di rete di Snowball Edge e migliorare le prestazioni di rete. DNIs supporta i tag VLAN e la personalizzazione dell'indirizzo MAC. Il traffico attivo non DNIs è protetto dai gruppi di sicurezza.

Sui dispositivi Snowball Edge, DNI può essere associato alle RJ45 porte SFP o QSFP. Ogni porta fisica ne supporta un massimo di 63. DNI non devono essere associati alla stessa porta di rete fisica utilizzata per gestire Snowball Edge.

Note

I dispositivi ottimizzati per lo storage Snowball Edge (con funzionalità di EC2 elaborazione) non sono supportati. DNI

Argomenti

- [Prerequisiti per DNI o VNI su Snowball Edge](#)
- [Configurazione di un'interfaccia di rete virtuale \(VNI\) su Snowball Edge](#)
- [Configurazione di un'interfaccia di rete diretta \(DNI\) su Snowball Edge](#)

Prerequisiti per DNI o VNI su Snowball Edge

Prima di configurare un VNI o un DNI, assicurati di aver soddisfatto i seguenti prerequisiti.

1. Assicurati che il dispositivo sia alimentato e che una delle interfacce di rete fisiche, come la RJ45 porta, sia connessa con un indirizzo IP.
2. Ottieni l'indirizzo IP associato all'interfaccia di rete fisica che stai utilizzando su Snowball Edge.
3. Configurare il client Snowball Edge. Per ulteriori informazioni, consulta [Configurazione di un profilo per il client Snowball Edge](#).
4. Configurare AWS CLI. Per ulteriori informazioni, consulta Guida [introduttiva a the AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.
5. Sbloccare il dispositivo.
 - Utilizzare AWS OpsHub per sbloccare il dispositivo. Per ulteriori informazioni, consulta [Snowball Edge](#). AWS OpsHub
 - Usa il client Snowball Edge per sbloccare il dispositivo. Per ulteriori informazioni, consulta [Sbloccare Snowball Edge](#).
6. Avvia un'istanza EC2 compatibile sul dispositivo. Assocerai il VNI a questa istanza.

7. Utilizzate il client Snowball Edge per eseguire il `describe-device` comando. L'output del comando fornirà un elenco di interfacce IDs di rete fisiche. Per ulteriori informazioni, consulta [Visualizzazione dello stato di uno Snowball Edge](#).
8. Identificare l'ID dell'interfaccia di rete fisica da utilizzare e prenderne nota.

Configurazione di un'interfaccia di rete virtuale (VNI) su Snowball Edge

Dopo aver identificato l'ID dell'interfaccia di rete fisica, puoi configurare un'interfaccia di rete virtuale (VNI) con quell'interfaccia fisica. Utilizzare la seguente procedura per configurare un VNI. Assicurati di eseguire le attività preliminari prima di creare un VNI.

Creare un VNI e associare un indirizzo IP

1. Utilizzate il client Snowball Edge per eseguire il `create-virtual-network-interface` comando. Gli esempi seguenti mostrano l'esecuzione di questo comando con i due diversi metodi di assegnazione di indirizzi IP, DHCP e STATIC. Il metodo DHCP utilizza DHCP (Dynamic Host Configuration Protocol).

```
snowballEdge create-virtual-network-interface \  
--physical-network-interface-id s.ni-abcd1234 \  
--ip-address-assignment DHCP \  
--profile profile-name \  
//OR//  
  
snowballEdge create-virtual-network-interface \  
--physical-network-interface-id s.ni-abcd1234 \  
--ip-address-assignment STATIC \  
--static-ip-address-configuration IpAddress=192.0.2.0,Netmask=255.255.255.0 \  
--profile profile-name
```

Il comando restituisce una struttura JSON che include l'indirizzo IP. Prendi nota di quell'indirizzo IP da utilizzare con il `ec2 associate-address` AWS CLI comando più avanti nel processo.

Ogni volta che è necessario questo indirizzo IP, è possibile utilizzare il comando Snowball Edge Client, il comando `describe-virtual-network-interfaces` Snowball Edge client, o AWS CLI il `aws ec2 describe-addresses` comando per ottenerlo.

2. Utilizzate il AWS CLI per associare l'indirizzo IP all'istanza EC2 -compatible, sostituendo il testo rosso con i vostri valori:

```
aws ec2 associate-address --public-ip 192.0.2.0 --instance-id s.i-01234567890123456  
--endpoint http://Snowball Edge physical IP address:8008
```

Configurazione di un'interfaccia di rete diretta (DNI) su Snowball Edge

Note

La funzionalità di interfaccia di rete diretta è disponibile a partire dal 12 gennaio 2021 ed è disponibile in tutte le Regioni AWS ovunque sia disponibile Snowball Edge.

Prerequisiti per un DNI su Snowball Edge

Prima di configurare un'interfaccia di rete diretta (DNI), è necessario eseguire le attività indicate nella sezione dei prerequisiti.

1. Eseguite le attività preliminari prima di configurare il DNI. Per istruzioni, consultare [Prerequisiti per DNIs o VNIs su Snowball Edge](#).
2. Inoltre, è necessario avviare un'istanza sul dispositivo, creare un VNI e associarlo all'istanza. Per istruzioni, consultare [Configurazione di un'interfaccia di rete virtuale \(VNI\) su Snowball Edge](#).

Note

Se hai aggiunto la rete diretta al tuo dispositivo esistente eseguendo un aggiornamento in-the-field software, devi riavviare il dispositivo due volte per abilitare completamente la funzionalità.

Crea un DNI e associa l'indirizzo IP

1. Crea un'interfaccia di rete diretta e collegala all'istanza EC2 compatibile con Amazon eseguendo il comando seguente. Avrai bisogno dell'indirizzo MAC del dispositivo per il passaggio successivo.

```
create-direct-network-interface [--endpoint endpoint] [--instance-id instanceId]  
[--mac macAddress]
```

```

--physical-network-interface-
id physicalNetworkInterfaceId
--unlock-code unlockCode [--vlan vlanId]

```

OPTIONS

--endpoint <endpoint> L'endpoint a cui inviare questa richiesta. L'endpoint per i tuoi dispositivi sarà un URL che utilizza lo `https` schema seguito da un indirizzo IP. Ad esempio, se l'indirizzo IP del dispositivo è 123.0.1.2, l'endpoint del dispositivo sarà `https://123.0.1.2`.

--instance-id <instanceId> L'ID dell'istanza EC2 -compatible a cui collegare l'interfaccia (opzionale).

--mac <macAddress> Imposta l'indirizzo MAC dell'interfaccia di rete (opzionale).

--physical-network-interface-id <physicalNetworkInterfaceId> L'ID dell'interfaccia di rete fisica su cui creare una nuova interfaccia di rete virtuale. È possibile determinare le interfacce di rete fisiche disponibili su Snowball Edge utilizzando `describe-device` il comando.

--vlan <vlanId> Imposta la VLAN assegnata per l'interfaccia (opzionale). Quando specificato, tutto il traffico inviato dall'interfaccia viene etichettato con l'ID VLAN specificato. Il traffico in entrata viene filtrato in base all'ID VLAN specificato e tutti i tag VLAN vengono rimossi prima di essere passato all'istanza.

2. Dopo aver creato un DNI e averlo associato alla tua istanza EC2 compatibile, devi apportare due modifiche alla configurazione all'interno dell'istanza compatibile con Amazon EC2.
 - La prima consiste nel fare in modo che i pacchetti destinati al VNI associato all'istanza EC2 - compatible vengano inviati tramite `eth0`.
 - La seconda modifica configura l'interfaccia di rete diretta per utilizzare DHCP o IP statico all'avvio.

Di seguito sono riportati alcuni esempi di script di shell per Amazon Linux 2 e CentOS Linux che apportano queste modifiche alla configurazione.

Amazon Linux 2

```

# Mac address of the direct network interface.
# You got this when you created the direct network interface.

```

```

DNI_MAC=[MAC ADDRESS FROM CREATED DNI]

# Configure routing so that packets meant for the VNI always are sent through
eth0.
PRIVATE_IP=$(curl -s http://169.254.169.254/latest/meta-data/local-ipv4)
PRIVATE_GATEWAY=$(ip route show to match 0/0 dev eth0 | awk '{print $3}')
ROUTE_TABLE=10001
echo "from $PRIVATE_IP table $ROUTE_TABLE" > /etc/sysconfig/network-scripts/
rule-eth0
echo "default via $PRIVATE_GATEWAY dev eth0 table $ROUTE_TABLE" > /etc/
sysconfig/network-scripts/route-eth0
echo "169.254.169.254 dev eth0" >> /etc/sysconfig/network-scripts/route-eth0

# Query the persistent DNI name, assigned by udev via ec2net helper.
#   changable in /etc/udev/rules.d/70-persistent-net.rules
DNI=$(ip --oneline link | grep -i $DNI_MAC | awk -F ':' '{ print $2 }')

# Configure DNI to use DHCP on boot.
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-$DNI
DEVICE="$DNI"
NAME="$DNI"
HWADDR=$DNI_MAC
ONBOOT=yes
NOZEROCONF=yes
BOOTPROTO=dhcp
TYPE=Ethernet
MAINROUTETABLE=no
EOF

# Make all changes live.
systemctl restart network

```

CentOS Linux

```

# Mac address of the direct network interface. You got this when you created the
direct network interface.
DNI_MAC=[MAC ADDRESS FROM CREATED DNI]
# The name to use for the direct network interface. You can pick any name that
isn't already in use.
DNI=eth1

```

```
# Configure routing so that packets meant for the VNIC always are sent through
eth0
PRIVATE_IP=$(curl -s http://169.254.169.254/latest/meta-data/local-ipv4)
PRIVATE_GATEWAY=$(ip route show to match 0/0 dev eth0 | awk '{print $3}')
ROUTE_TABLE=10001
echo from $PRIVATE_IP table $ROUTE_TABLE > /etc/sysconfig/network-scripts/rule-
eth0
echo default via $PRIVATE_GATEWAY dev eth0 table $ROUTE_TABLE > /etc/sysconfig/
network-scripts/route-eth0

# Configure your direct network interface to use DHCP on boot.
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-$DNI
DEVICE="$DNI"
NAME="$DNI"
HWADDR="$DNI_MAC"
ONBOOT=yes
NOZEROCONF=yes
BOOTPROTO=dhcp
TYPE=Ethernet
EOF

# Rename DNI device if needed.
CURRENT_DEVICE_NAME=$(LANG=C ip -o link | awk -F ':' -v IGNORECASE=1 '!/link\/
ieee802\.\11/ && /'"$DNI_MAC"'/ { print $2 })
ip link set $CURRENT_DEVICE_NAME name $DNI

# Make all changes live.
systemctl restart network
```

Utilizzo di SSH per connettersi alle istanze di calcolo su uno Snowball Edge

Per utilizzare Secure Shell (SSH) per connettersi alle istanze di calcolo su uno Snowball Edge, sono disponibili le seguenti opzioni per fornire o creare una chiave SSH.

- Puoi fornire la chiave SSH per Amazon Machine Image (AMI) quando crei un lavoro per ordinare un dispositivo. Per ulteriori informazioni, consulta [Creazione di un lavoro per ordinare uno Snowball Edge](#).

- Puoi fornire la chiave SSH per l'AMI quando crei un'immagine di macchina virtuale da importare su Snowball Edge. Per ulteriori informazioni, consulta [Importazione dell'immagine di una macchina virtuale su un dispositivo Snowball Edge](#).
- Puoi creare una coppia di chiavi su Snowball Edge e scegliere di avviare un'istanza con quella chiave pubblica generata localmente. Per ulteriori informazioni, consulta [Create a key pair using Amazon EC2](#) nella Amazon EC2 User Guide.

Per connettersi a un'istanza tramite SSH

1. Assicurati che il dispositivo sia acceso, connesso alla rete e sbloccato. Per ulteriori informazioni, consulta [Connessione di uno Snowball Edge alla rete locale](#).
2. Verifica che le impostazioni di rete siano configurate per le istanze di calcolo. Per ulteriori informazioni, consulta [Configurazioni di rete per istanze di calcolo su Snowball Edge](#).
3. Controlla le tue note per trovare il PEM o la coppia di chiavi PPK utilizzate per questa istanza specifica. Creare una copia di quei file da qualche parte nel tuo computer. Prendere nota del percorso del file PEM.
4. Connettersi all'istanza tramite SSH come mostrato nell'esempio di comando seguente. L'indirizzo IP è quello dell'interfaccia di rete virtuale (VNIC) impostata in [Configurazioni di rete per istanze di calcolo su Snowball Edge](#).

```
ssh -i path/to/PEM/key/file instance-user-name@192.0.2.0
```

Per ulteriori informazioni, consulta [Connessione all'istanza Linux tramite SSH](#) nella Amazon EC2 User Guide.

Trasferimento di dati da istanze EC2 di calcolo compatibili a bucket S3 sullo stesso Snowball Edge

Puoi trasferire dati tra istanze di calcolo e bucket Amazon S3 sullo stesso dispositivo Snowball Edge. A tale scopo, utilizza i AWS CLI comandi supportati e gli endpoint appropriati. Ad esempio, supponiamo di voler spostare i dati da una directory nella mia `sbe1.xlarge` istanza al bucket Amazon S3, `amzn-s3-demo-bucket` sullo stesso dispositivo. Supponiamo di utilizzare lo storage compatibile con Amazon S3 sull'endpoint Snowball Edge. `https://S3-object-API-endpoint:443` Attenersi alla seguente procedura:

Per trasferire dati tra un'istanza di calcolo e un bucket sullo stesso Snowball Edge

1. Utilizzare SSH per connettersi all'istanza di calcolo.
2. Scarica e installa il. AWS CLI Se l'istanza non dispone della AWS CLI, dovrai scaricarla e installarla. Per ulteriori informazioni, consulta l'argomento relativo all'[installazione di AWS Command Line Interface](#).
3. Configura l' AWS CLI istanza di calcolo in modo che funzioni con l'endpoint Amazon S3 su Snowball Edge. Per ulteriori informazioni, consulta [Acquisizione e utilizzo delle credenziali locali di Amazon S3 su Snowball Edge](#).
4. Utilizza lo storage compatibile con Amazon S3 supportato sui comandi Snowball Edge per trasferire dati. Per esempio:

```
aws s3 cp ~/june2018/results s3://amzn-s3-demo-bucket/june2018/results --recursive  
--endpoint https://S3-object-API-endpoint:443
```

Avvio automatico di EC2 istanze compatibili

Il client Snowball Edge è un'applicazione CLI (Command Line Interface) autonoma che puoi eseguire nel tuo ambiente. È possibile utilizzarlo per eseguire alcune attività amministrative sul dispositivo Snowball Edge o sul cluster di dispositivi. Per ulteriori informazioni su come utilizzare il client Snowball Edge, incluso come avviare e interrompere i servizi con esso, consulta. [Configurazione e utilizzo del client Snowball Edge](#)

Di seguito, puoi trovare informazioni sui comandi del client Snowball Edge specifici per le istanze di calcolo, inclusi esempi di utilizzo.

Per un elenco dei comandi EC2 compatibili con Amazon che puoi utilizzare sul tuo AWS Snowball Edge dispositivo, consulta [AWS CLI Comandi EC2 compatibili con Amazon supportati su Snowball Edge](#).

Creazione di una configurazione EC2 di avvio compatibile su Snowball Edge

Per avviare automaticamente le istanze EC2 di calcolo compatibili con Amazon sul tuo AWS Snowball Edge dispositivo dopo lo sblocco, puoi creare una configurazione di avvio. A tale scopo, usa il `snowballEdge create-autostart-configuration` comando, come illustrato di seguito.

Utilizzo

```
snowballEdge create-autostart-configuration --physical-connector-type [SFP_PLUS or RJ45 or QSFP] --ip-address-assignment [DHCP or STATIC] [--static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]] --launch-template-id [--launch-template-version]
```

Aggiornamento di una configurazione EC2 di avvio compatibile su Snowball Edge

Per aggiornare una configurazione di avvio esistente su Snowball Edge, usa il `snowballEdge update-autostart-configuration` comando. Di seguito è riportato il suo utilizzo. Per attivare o disattivare una configurazione di avvio, specificare il parametro `--enabled`.

Utilizzo

```
snowballEdge update-autostart-configuration --autostart-configuration-arn [--physical-connector-type [SFP_PLUS or RJ45 or QSFP]] [--ip-address-assignment [DHCP or STATIC]] [--static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]] [--launch-template-id] [--launch-template-version] [--enabled]
```

Eliminazione di una configurazione EC2 di avvio compatibile su Snowball Edge

Per eliminare una configurazione di avvio che non è più in uso, utilizzate il `snowballEdge delete-autostart-configuration` comando, come segue.

Utilizzo

```
snowballEdge delete-autostart-configuration --autostart-configuration-arn
```

Elenco delle configurazioni di avvio EC2 compatibili su Snowball Edge

Per elencare le configurazioni di avvio che hai creato su Snowball Edge, usa `describe-autostart-configurations` il comando, come segue.

Utilizzo

```
snowballEdge describe-autostart-configurations
```


Creazione di un'interfaccia di rete virtuale su Snowball Edge

Per eseguire un'istanza di calcolo o avviare l'interfaccia NFS su Snowball Edge, crea prima un'interfaccia di rete virtuale (VNI). Ogni Snowball Edge dispone di tre interfacce di rete (NICs), i controller di interfaccia di rete fisici per il dispositivo. Queste sono le RJ45 porte SFP e QSFP sul retro del dispositivo.

Ogni VNI è basato su un VNI fisico ed è possibile avere un numero qualsiasi di VNI associato a ciascuna NIC. Per creare un'interfaccia di rete virtuale utilizzando il comando `snowballEdge create-virtual-network-interface`.

Note

Il parametro `--static-ip-address-configuration` è valido solo quando si usa l'opzione `STATIC` per il parametro `--ip-address-assignment`.

Utilizzo

È possibile utilizzare questo comando in due modi: con il client Snowball Edge configurato o senza il client Snowball Edge configurato. L'esempio di utilizzo seguente mostra il metodo con il client Snowball Edge configurato.

```
snowballEdge create-virtual-network-interface --ip-address-assignment [DHCP or STATIC]
--physical-network-interface-id [physical network interface id] --static-ip-address-
configuration IpAddress=[IP address],NetMask=[Netmask]
```

L'esempio di utilizzo seguente mostra il metodo senza il client Snowball Edge configurato.

```
snowballEdge create-virtual-network-interface --endpoint https://[ip address]
--manifest-file /path/to/manifest --unlock-code [unlock code] --ip-address-
assignment [DHCP or STATIC] --physical-network-interface-id [physical network interface
id] --static-ip-address-configuration IpAddress=[IP address],NetMask=[Netmask]
```

Example Esempio: creazione VNICs (utilizzando DHCP)

```
snowballEdge create-virtual-network-interface --ip-address-assignment dhcp --physical-
network-interface-id s.ni-8EXAMPLEaEXAMPLEd
{
  "VirtualNetworkInterface" : {
```

```

    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/
s.ni-8EXAMPLE8EXAMPLEf",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.0",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "EX:AM:PL:E1:23:45",
    "MtuSize" : "1500"
  }
}

```

Descrizione delle interfacce di rete virtuali

Per descrivere VNICs quello che hai creato in precedenza sul tuo dispositivo, usa il `snowballEdge describe-virtual-network-interfaces` comando. Di seguito è riportato il suo utilizzo.

Utilizzo

È possibile utilizzare questo comando in due modi: con il client Snowball Edge configurato o senza il client Snowball Edge configurato. L'esempio di utilizzo seguente mostra il metodo con il client Snowball Edge configurato.

```
snowballEdge describe-virtual-network-interfaces
```

L'esempio di utilizzo seguente mostra il metodo senza il client Snowball Edge configurato.

```
snowballEdge describe-virtual-network-interfaces --endpoint https://[ip address] --
manifest-file /path/to/manifest --unlock-code [unlock code]
```

Example Esempio: descrizione VNICs

```

snowballEdge describe-virtual-network-interfaces
[
  {
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/
s.ni-8EXAMPLE8EXAMPLE8",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.0",
    "Netmask" : "255.255.255.0",

```

```

    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "EX:AM:PL:E1:23:45",
    "MtuSize" : "1500"
  },{
    "VirtualNetworkInterfaceArn" : "arn:aws:snowball-device::interface/
s.ni-1EXAMPLE1EXAMPLE1",
    "PhysicalNetworkInterfaceId" : "s.ni-8EXAMPLEaEXAMPLEd",
    "IpAddressAssignment" : "DHCP",
    "IpAddress" : "192.0.2.2",
    "Netmask" : "255.255.255.0",
    "DefaultGateway" : "192.0.2.1",
    "MacAddress" : "12:34:5E:XA:MP:LE",
    "MtuSize" : "1500"
  }
]

```

Aggiornamento di un'interfaccia di rete virtuale su Snowball Edge

Dopo aver creato un'interfaccia di rete virtuale (VNI), puoi aggiornarne la configurazione utilizzando il `snowballEdge update-virtual-network-interface` comando. Dopo aver fornito l'Amazon Resource Name (ARN) per un determinato VNI, fornisci valori solo per gli elementi che stai aggiornando.

Utilizzo

È possibile utilizzare questo comando in due modi: con il client Snowball Edge configurato o senza il client Snowball Edge configurato. L'esempio di utilizzo seguente mostra il metodo con il client Snowball Edge configurato.

```

snowballEdge update-virtual-network-interface --virtual-network-interface-arn [virtual
network-interface-arn] --ip-address-assignment [DHCP or STATIC] --physical-network-
interface-id [physical network interface id] --static-ip-address-configuration
IpAddress=[IP address],NetMask=[Netmask]

```

L'esempio di utilizzo seguente mostra il metodo senza il client Snowball Edge configurato.

```

snowballEdge update-virtual-network-interface --endpoint https://[ip address] --
manifest-file /path/to/manifest --unlock-code [unlock code] --virtual-network-
interface-arn [virtual network-interface-arn] --ip-address-assignment [DHCP or STATIC]
--physical-network-interface-id [physical network interface id] --static-ip-address-
configuration IpAddress=[IP address],NetMask=[Netmask]

```

Example Esempio: aggiornamento di una VNIC (usando DHCP)

```
snowballEdge update-virtual-network-interface --virtual-network-interface-arn  
arn:aws:snowball-device:::interface/s.ni-8EXAMPLEbEXAMPLEd --ip-address-assignment  
dhcp
```

Eliminazione di un'interfaccia di rete virtuale su Snowball Edge

Per eliminare un'interfaccia di rete virtuale (VNI), puoi usare il comando. `snowballEdge delete-virtual-network-interface`

Utilizzo

È possibile utilizzare questo comando in due modi: con il client Snowball Edge configurato o senza il client Snowball Edge configurato. L'esempio di utilizzo seguente mostra il metodo con il client Snowball Edge configurato.

```
snowballEdge delete-virtual-network-interface --virtual-network-interface-arn [virtual  
network-interface-arn]
```

L'esempio di utilizzo seguente mostra il metodo senza il client Snowball Edge configurato.

```
snowballEdge delete-virtual-network-interface --endpoint https://[ip address] --  
manifest-file /path/to/manifest --unlock-code [unlock code] --virtual-network-  
interface-arn [virtual network-interface-arn]
```

Example Esempio: eliminazione di una VNIC

```
snowballEdge delete-virtual-network-interface --virtual-network-interface-arn  
arn:aws:snowball-device:::interface/s.ni-8EXAMPLEbEXAMPLEd
```

Utilizzo dell'endpoint EC2 compatibile con Amazon su Snowball Edge

Di seguito, puoi trovare una panoramica degli endpoint EC2 compatibili con Amazon. Utilizzando questo endpoint, puoi gestire Amazon Machine Images (AMIs) e calcolare le istanze in modo programmatico utilizzando operazioni API compatibili con Amazon EC2.

Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge

Quando usi per inviare un comando AWS CLI al AWS Snowball Edge dispositivo, puoi specificare che l'endpoint è un endpoint EC2 compatibile con Amazon. Puoi scegliere di utilizzare l'endpoint HTTPS o un endpoint HTTP non protetto, come mostrato di seguito.

Endpoint protetto HTTPS

```
aws ec2 describe-instances --endpoint https://192.0.2.0:8243 --ca-bundle path/to/certificate
```

Endpoint non protetto HTTP

```
aws ec2 describe-instances --endpoint http://192.0.2.0:8008
```

Se utilizzi l'endpoint HTTPS 8243, i dati in transito sono crittografati. Questa crittografia è garantita da un certificato generato da Snowball Edge quando viene sbloccato. Dopo aver ottenuto il certificato, puoi salvarlo in un file `ca-bundle.pem` locale. Puoi, quindi, configurare il profilo AWS CLI per includere il percorso al certificato, come descritto di seguito.

Per associare il certificato all'endpoint EC2 compatibile con Amazon

1. Connect Snowball Edge all'alimentazione e alla rete e accendilo.
2. Al termine della procedura di sblocco, prendere nota del relativo indirizzo IP sulla rete locale.
3. Da un terminale della rete, assicurati di poter eseguire il ping di Snowball Edge.
4. Eseguire il comando `snowballEdge get-certificate` nel terminale. Per ulteriori informazioni su questo comando, consulta [Gestione dei certificati a chiave pubblica su Snowball Edge](#).
5. Salvare l'output del comando `snowballEdge get-certificate` in un file, ad esempio `ca-bundle.pem`.
6. Eseguire il seguente comando dal terminale.

```
aws configure set profile.snowballEdge.ca_bundle /path/to/ca-bundle.pem
```

Al termine della procedura, puoi eseguire comandi CLI con queste credenziali locali, il certificato e l'endpoint specificato.

AWS CLI Comandi EC2 compatibili con Amazon supportati su Snowball Edge

Puoi gestire le istanze di calcolo su un dispositivo Snowball Edge tramite un endpoint compatibile con Amazon. EC2 Questo tipo di endpoint supporta molti dei comandi e delle azioni di Amazon EC2 CLI di. AWS SDKs [Per informazioni sull'installazione e la configurazione di AWS CLI, inclusa la definizione del destinatario delle AWS CLI chiamate, consulta la Guida per l' Regioni AWSAWS Command Line Interface utente.](#)

Elenco dei AWS CLI comandi EC2 compatibili supportati su Snowball Edge

Di seguito, puoi trovare una descrizione del sottoinsieme di AWS CLI comandi e opzioni per Amazon EC2 supportati sui dispositivi Snowball Edge. Un comando o un'opzione non incluso nell'elenco seguente non è supportato. Insieme al comando, puoi dichiarare alcune opzioni non supportate. Tuttavia, queste vengono ignorate.

- [associate-address](#): associa un indirizzo IP virtuale a un'istanza per l'uso in una delle tre interfacce di rete fisiche nel dispositivo:
 - `--instance-id`: ID di una singola istanza sbe.
 - `--public-ip`: indirizzo IP virtuale da utilizzare per accedere all'istanza.
- [attach-volume](#): collega un volume Amazon EBS a un'istanza interrotta o in esecuzione sul dispositivo e lo espone all'istanza con il nome del dispositivo specificato.
 - `--device value` Il nome del dispositivo.
 - `--instance-id` — L'ID di un'istanza di destinazione compatibile con Amazon. EC2
 - `value--volume-id` — L'ID del volume EBS.
- [authorize-security-group-egress](#)— Aggiunge una o più regole di uscita a un gruppo di sicurezza da utilizzare con un dispositivo Snowball Edge. In particolare, questa azione consente alle istanze di inviare traffico a uno o più intervalli di indirizzi CIDR di destinazione IPv4 . Per ulteriori informazioni, consulta [Controllo del traffico di rete con gruppi di sicurezza su Snowball Edge](#).
 - `--group-id value` — L'ID del gruppo di sicurezza
 - `[--ip-permissionsvalue]` — Uno o più set di autorizzazioni IP.

- [authorize-security-group-ingress](#) — Aggiunge una o più regole di ingresso a un gruppo di sicurezza. Quando chiami `authorize-security-group-ingress`, devi specificare un valore per `group-name` o `group-id`.
 - `--group-name value` — Il nome del gruppo di sicurezza.
 - `--group-id value` — L'ID del gruppo di sicurezza
 - `--ip-permissions value` — Uno o più set di autorizzazioni IP.
 - `--protocol value` Il protocollo IP. I valori possibili sono `tcp`, `udp` e `icmp`. L'argomento `--port` è obbligatorio, a meno che non sia stato specificato il valore "all protocols" (-1).
 - `--port value` — Per TCP o UDP, l'intervallo di porte da consentire. Questo valore può essere un numero intero singolo o un intervallo (minimo-massimo).

Per ICMP, un numero intero o un intervallo (`type-code`) in cui `type` rappresenta il numero del tipo ICMP e `code` rappresenta il numero del codice ICMP. Il valore -1 indica tutti i codici ICMP per tutti i tipi di ICMP. Il valore -1 solo per `type` indica tutti i codici ICMP per il tipo di ICMP specificato.

- `--cidr value` — L'intervallo IP CIDR.
- [create-launch-template](#) — Crea un modello di lancio. Un modello di lancio contiene i parametri per avviare un'istanza. Quando avvii un'istanza utilizzando `RunInstances`, puoi specificare un modello di lancio invece di fornire i parametri di lancio nella richiesta. È possibile creare fino a 100 modelli per dispositivo.
 - `-- launch-template-name string` — Un nome per il modello di lancio.
 - `-- launch-template-data structure` — Le informazioni per il modello di lancio. Sono supportati gli attributi seguenti:
 - `ImageId`
 - `InstanceType`
 - `SecurityGroupIds`
 - `TagSpecifications`
 - `UserData`

Sintassi JSON:

```
{
  "ImageId": "string",
  "InstanceType": "sbe-c.large",
  "SecurityGroupIds": ["string", ...],
```

```

    "TagSpecifications":[{"ResourceType":"instance","Tags":
    [{"Key":"Name","Value":"Test"},
      {"Key":"Stack","Value":"Gamma"}]},
    "UserData":"this is my user data"
  }

```

- `--version-descriptionstring` — Una descrizione per la prima versione del modello di lancio.
- `--endpoint snowballEndpoint` — Un valore che consente di gestire le istanze di calcolo in modo programmatico utilizzando operazioni API compatibili con Amazon. EC2 Per ulteriori informazioni, consulta [Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge](#).
- [create-launch-template-version](#) — Crea una nuova versione per un modello di lancio. È possibile specificare una versione esistente di un modello di lancio su cui basare la nuova versione. Le versioni del modello di avvio sono numerate nell'ordine in cui sono state create. Non è possibile specificare, modificare o sostituire la numerazione delle versioni del modello di lancio. È possibile creare fino a 100 versioni di ogni modello di lancio.

Specificare l'ID o il nome del modello di lancio nella richiesta.

- `-- launch-template-id string` — L'ID del modello di lancio.
- `-- launch-template-name string` — Un nome per il modello di lancio.
- `-- launch-template-data structure` — Le informazioni per il modello di lancio. Sono supportati gli attributi seguenti:
 - ImageId
 - InstanceType
 - SecurityGroupIds
 - TagSpecifications
 - UserData

Sintassi JSON:

```

{
  "ImageId":"string",
  "InstanceType":"sbe-c.large",
  "SecurityGroupIds":["string", ...],
  "TagSpecifications":[{"ResourceType":"instance","Tags":
  [{"Key":"Name","Value":"Test"},
    {"Key":"Stack","Value":"Gamma"}]},
  "UserData":"this is my user data"
}

```


}

- `--source-versionstring` — Il numero di versione del modello di lancio su cui basare la nuova versione. La nuova versione eredita gli stessi parametri di lancio della versione di origine, ad eccezione dei parametri specificati in `launch-template-data`.
- `--version-descriptionstring` — Una descrizione per la prima versione del modello di lancio.
- `--endpoint snowballEndpoint` — Un valore che consente di gestire le istanze di calcolo in modo programmatico utilizzando operazioni API compatibili con Amazon. EC2 Per ulteriori informazioni, consulta [Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge](#).
- [create-tags](#) — Aggiunge o sovrascrive uno o più tag per la risorsa specificata. Ogni risorsa può avere un massimo di 50 tag. Ciascun tag è formato da una chiave e da un valore opzionale. Le chiavi del tag devono essere univoche per una risorsa. Sono supportate le seguenti risorse :
 - AMI
 - Istanza
 - Modello di avvio
 - Gruppo di sicurezza
 - Coppia di chiavi
- [create-security-group](#) — Crea un gruppo di sicurezza su Snowball Edge. Puoi creare fino a 50 gruppi di sicurezza. Quando crei un gruppo di sicurezza, devi specificare un nome di tua scelta:
 - `--group-name value` — Il nome del gruppo di sicurezza.
 - `--description value` — Una descrizione del gruppo di sicurezza. Questo messaggio è solo informativo. Questo valore deve contenere al massimo 255 caratteri.
- [create-volume](#): crea un volume Amazon EBS che può essere collegato a un'istanza sul tuo dispositivo.
 - `--sizevalue` — La dimensione del volume in GiBs, che può essere compresa tra 1 GiB e 1 TB (GiBs1000).
 - `--snapshot-idvalue` — L'istantanea da cui creare il volume.
 - `--volume-type value` — Il tipo di volume. Se nessun valore è specificato, il valore predefinito è `sbg1`. I valori possibili sono:
 - `sbg1` per volumi magnetici
 - `sbp1` per volumi SSD
 - `--tag-specificationsvalue` — Un elenco di tag da applicare al volume durante la creazione.

- [delete-launch-template](#)— Elimina un modello di avvio. L'eliminazione di un modello di avvio ne elimina tutte le versioni.

Specificare l'ID o il nome del modello di lancio nella richiesta.

- `-- launch-template-id string` — L'ID del modello di lancio.
- `-- launch-template-name string` — Un nome per il modello di lancio.
- `--endpoint snowballEndpoint` — Un valore che consente di gestire le istanze di calcolo in modo programmatico utilizzando operazioni API compatibili con Amazon. EC2 Per ulteriori informazioni, consulta [Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge](#).
- [delete-launch-template-version](#)— Elimina una o più versioni di un modello di lancio. Non è possibile eliminare la versione predefinita di un modello di lancio; è necessario prima assegnare una versione diversa come predefinita. Se la versione predefinita è l'unica versione del modello di lancio, eliminare l'intero modello di lancio usando il comando `delete-launch-template`.

Specificare l'ID o il nome del modello di lancio nella richiesta.

- `-- launch-template-id string` — L'ID del modello di lancio.
- `-- launch-template-name string` — Un nome per il modello di lancio.
- `--versions (list) "string" "string"` — I numeri di versione di una o più versioni del template di avvio da eliminare.
- `--endpoint snowballEndpoint` — Un valore che consente di gestire le istanze di calcolo in modo programmatico utilizzando operazioni API compatibili con Amazon. EC2 Per ulteriori informazioni, consulta [Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge](#).
- [delete-security-group](#)— Elimina un gruppo di sicurezza.

Se tenti di eliminare un gruppo di sicurezza associato a un'istanza o a cui fa riferimento un altro gruppo di sicurezza, l'operazione ha esito negativo con `DependencyViolation`.

- `--group-name value` — Il nome del gruppo di sicurezza.
- `--description value` — Una descrizione del gruppo di sicurezza. Questo messaggio è solo informativo. Questo valore deve contenere al massimo 255 caratteri.
- [delete-tags](#) — Elimina il set di tag specificato dalla risorsa specificata (AMI, istanza di calcolo, modello di avvio o gruppo di sicurezza).
- [delete-volume](#) — Elimina il volume Amazon EBS specificato. Il volume deve essere nello stato `available` (non collegato a un'istanza).

- `value--volume-id` — L'ID del volume.
- [describe-addresses](#): descrive uno o più indirizzi IP virtuali associati allo stesso numero di istanze sul dispositivo. sbe
 - `--public-ips`: uno o più degli indirizzi IP virtuali associati alle proprie istanze in uso.
- [describe-images](#) — Descrive una o più immagini () disponibili. AMIs Le immagini disponibili vengono aggiunte al dispositivo Snowball Edge durante la creazione del lavoro.
 - `--image-id` — L'ID Snowball AMI dell'AMI.
- [describe-instance-attribute](#) — Descrive l'attributo specificato dell'istanza specificata. Puoi specificare solo un attributo per volta. Sono supportati gli attributi seguenti:
 - `instanceInitiatedShutdownBehavior`
 - `instanceType`
 - `userData`
- [describe-instances](#): descrive una o più delle istanze. La risposta indica tutti i gruppi di sicurezza assegnati per le istanze.
 - `--instance-ids` — L'elenco IDs di una o più sbe istanze che sono state interrotte sul dispositivo.
 - `--page-size` — La dimensione di ogni pagina da inserire nella chiamata. Questo valore non influisce sul numero di elementi restituiti nell'output del comando. Impostando dimensioni minori per la pagina, vengono effettuate più chiamate al dispositivo e recuperati meno elementi in ogni chiamata. Questo contribuisce a prevenire il timeout delle chiamate.
 - `--max-items` — Il numero totale di elementi da restituire nell'output del comando. Se il numero totale di elementi disponibili supera il valore specificato, viene fornito un `NextToken` nell'output del comando. Per riprendere la paginazione, specifica il valore `NextToken` nell'argomento `starting-token` di un comando successivo.
 - `--starting-token` — Un token per specificare dove iniziare l'impaginazione. Questo token è il valore `NextToken` proveniente da una risposta troncata in precedenza.
- [describe-instance-status](#) — Descrive lo stato delle istanze specificate o di tutte le istanze. Per impostazione predefinita, vengono descritte solo le istanze in esecuzione, a meno che non si indichi specificamente di restituire lo stato di tutte le istanze. Lo stato dell'istanza include i seguenti componenti:
 - Controlli dello stato: il dispositivo Snow esegue controlli dello stato su istanze EC2 compatibili con Amazon in esecuzione per identificare problemi hardware e software.
 - Stato dell'istanza: puoi gestire le istanze dal momento in cui le avvii fino alla loro chiusura.

Con questo comando sono supportati i seguenti filtri.

- `[--filters](elenco)`

I filtri.

- `instance-state-code`— Il codice per lo stato dell'istanza, come numero intero senza segno a 16 bit. Il byte high viene utilizzato per scopi di reporting interno dei servizi e deve essere ignorato. Il byte basso viene impostato in base allo stato rappresentato. I valori validi sono 0 (in sospeso), 16 (in esecuzione), 32 (arresto), 48 (terminato), 64 (arresto) e 80 (interrotto).
- `instance-state-name`— Lo stato dell'istanza (`pending` | `running`). `shutting-down` `terminated` `stopping` `stopped`
- `instance-status.reachability`— Filtra in base allo stato dell'istanza in cui il nome è `reachability` (`passed` | `failed` | `initializing` | `insufficient-data`).
- `instance-status.status`— Lo stato dell'istanza (`ok` | `impaired` | `initializing` | `insufficient-data` | `not-applicable`).
- `system-status.reachability`— Filtri sullo stato del sistema in cui il nome è raggiungibilità (`passed` | `failed` | `initializing` | `insufficient-data`).
- `system-status.status`— Lo stato del sistema dell'istanza (`ok` | `impaired` | `initializing` | `insufficient-data` | `not-applicable`).
- Sintassi JSON:

```
[
  {
    "Name": "string",
    "Values": ["string", ...]
  }
  ...
]
```

- `[--instance-ids](elenco)`

L'istanza IDs.

Predefinito: descrive tutte le istanze.

- `[--dry-run | --no-dry-run](booleano)`

Verifica se si dispone delle autorizzazioni necessarie per l'azione, senza effettuare effettivamente la richiesta, e fornisce una risposta di errore. Se si dispone delle autorizzazioni richieste, la risposta di errore è `DryRunOperation`.

In caso contrario è `UnauthorizedOperation`.

- `[--include-all-instances | --no-include-all-instances]`(booleano)

Quando `true`, include lo stato di salute per tutte le istanze. Quando `false`, include lo stato di integrità solo per le istanze in esecuzione.

Impostazione predefinita: `false`

- `[--page-size]`(numero intero): la dimensione di ogni pagina da inserire nella chiamata. Questo valore non influisce sul numero di elementi restituiti nell'output del comando. Impostando dimensioni minori per la pagina, vengono effettuate più chiamate al dispositivo e recuperati meno elementi in ogni chiamata. Questo contribuisce a prevenire il timeout delle chiamate.
- `[--max-items]`(intero) — Il numero totale di elementi da restituire nell'output del comando. Se il numero totale di elementi disponibili supera il valore specificato, viene fornito un `NextToken` nell'output del comando. Per riprendere la paginazione, specifica il valore `NextToken` nell'argomento `starting-token` di un comando successivo.
- `[--starting-token]`(stringa) — Un token per specificare dove iniziare l'impaginazione. Questo token è il valore `NextToken` proveniente da una risposta troncata in precedenza.
- [describe-launch-templates](#) — Descrive uno o più modelli di avvio. Il comando `describe-launch-templates` è un'operazione paginata. Puoi effettuare più chiamate per recuperare l'intero set di dati dei risultati.

Specificate il modello di lancio IDs o i nomi dei modelli di lancio nella richiesta.

- `--launch-template-ids` (elenco) "string" "string" — Un elenco IDs dei modelli di lancio.
- `--launch-template-names` (elenco) "string" "string" — Un elenco di nomi per i modelli di lancio.
- `--page-size` — La dimensione di ogni pagina da inserire nella chiamata. Questo valore non influisce sul numero di elementi restituiti nell'output del comando. Impostando dimensioni minori per la pagina, vengono effettuate più chiamate al dispositivo e recuperati meno elementi in ogni chiamata. Questo contribuisce a prevenire il timeout delle chiamate.
- `--max-items` — Il numero totale di elementi da restituire nell'output del comando. Se il numero totale di elementi disponibili supera il valore specificato, viene fornito un `NextToken` nell'output

del comando. Per riprendere la paginazione, specifica il valore `NextToken` nell'argomento `starting-token` di un comando successivo.

- `--starting-token` — Un token per specificare dove iniziare l'impaginazione. Questo token è il valore `NextToken` proveniente da una risposta troncata in precedenza.
- `--endpoint snowballEndpoint` — Un valore che consente di gestire le istanze di calcolo in modo programmatico utilizzando operazioni API compatibili con Amazon. EC2 Per ulteriori informazioni, consulta [Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge](#).
- [`describe-launch-template-versions`](#) — Descrive una o più versioni di un modello di lancio specificato. È possibile descrivere tutte le versioni, versioni singole o un intervallo di versioni. Il comando `describe-launch-template-versions` è un'operazione paginata. Puoi effettuare più chiamate per recuperare l'intero set di dati dei risultati.

Specificate il modello di lancio IDs o i nomi dei modelli di lancio nella richiesta.

- `-- launch-template-id string` — L'ID del modello di lancio.
- `-- launch-template-name string` — Un nome per il modello di lancio.
- `[--versions (list)"string" "string"]` — I numeri di versione di una o più versioni del template di lancio da eliminare.
- `[--min-versionstring]` — Il numero di versione dopo il quale descrivere le versioni del modello di lancio.
- `[--max-versionstring]` — Il numero di versione fino al quale descrivere le versioni dei modelli di lancio.
- `--page-size` — La dimensione di ogni pagina da inserire nella chiamata. Questo valore non influisce sul numero di elementi restituiti nell'output del comando. Impostando dimensioni minori per la pagina, vengono effettuate più chiamate al dispositivo e recuperati meno elementi in ogni chiamata. Questo contribuisce a prevenire il timeout delle chiamate.
- `--max-items` — Il numero totale di elementi da restituire nell'output del comando. Se il numero totale di elementi disponibili supera il valore specificato, viene fornito un `NextToken` nell'output del comando. Per riprendere la paginazione, specifica il valore `NextToken` nell'argomento `starting-token` di un comando successivo.
- `--starting-token` — Un token per specificare dove iniziare l'impaginazione. Questo token è il valore `NextToken` proveniente da una risposta troncata in precedenza.
- `--endpoint snowballEndpoint` — Un valore che consente di gestire le istanze di calcolo in modo programmatico utilizzando operazioni API compatibili con Amazon. EC2 Per ulteriori

informazioni, consulta [Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge](#).

- [describe-security-groups](#)— Descrive uno o più dei tuoi gruppi di sicurezza.

Il comando `describe-security-groups` è un'operazione paginata. È possibile effettuare più chiamate API per recuperare l'intero set di dati dei risultati.

- `--group-namevalue` — Il nome del gruppo di sicurezza.
- `--group-idvalue` — L'ID del gruppo di sicurezza.
- `--page-sizevalue` — La dimensione di ogni pagina da inserire nella chiamata di servizio. AWS Questa dimensione non influisce sul numero di elementi restituiti nell'output del comando. L'impostazione di una dimensione di pagina più piccola comporta un maggior numero di chiamate al AWS servizio e il recupero di un minor numero di elementi in ogni chiamata. Questo approccio può aiutare a evitare il timeout delle chiamate di AWS servizio. Per esempi di utilizzo, consulta [Pagination nella Guida](#) per l'AWS Command Line Interface utente.
- `--max-itemsvalue` — Il numero totale di elementi da restituire nell'output del comando. Se il numero totale di elementi disponibili supera il valore specificato, viene fornito un `NextToken` nell'output del comando. Per riprendere la paginazione, specifica il valore `NextToken` nell'argomento `starting-token` di un comando successivo. Non utilizzare l'elemento di `NextToken` risposta direttamente all'esterno di. AWS CLI Per esempi di utilizzo, consulta [Pagination](#) nella Guida per l'AWS Command Line Interface utente.
- `--starting-tokenvalue` — Un token per specificare da dove iniziare l'impaginazione. Questo token è il valore `NextToken` proveniente da una risposta troncata in precedenza. Per esempi di utilizzo, consulta [Pagination](#) nella Guida per l'utente.AWS Command Line Interface
- [describe-tags](#): descrive uno o più tag per la risorsa (image o il gruppo di sicurezza) specificato. `instance` Con questo comando, i seguenti filtri sono supportati:
 - `launch-template`
 - `resource-id`
 - `resource-type` – `image` o `instance`
 - Chiave
 - `value`
- [describe-volumes: descrive i volumi](#) Amazon EBS specificati.
 - `--max-itemsvalue` — Il numero totale di elementi da restituire nell'output del comando. Se il numero totale di elementi disponibili supera il valore specificato, viene fornito un `NextToken`

nell'output del comando. Per riprendere la paginazione, specifica il valore `NextToken` nell'argomento `starting-token` di un comando successivo.

- `[--starting-token value]` — Un token per specificare dove iniziare l'impaginazione. Questo token è il valore `NextToken` proveniente da una risposta troncata in precedenza.
- `[--volume-ids]` — Uno o più `volumeId`. IDs
- [`detach-volume`](#): scollega un volume Amazon EBS da un'istanza interrotta o in esecuzione.
 - `[--device value]` — Il nome del dispositivo.
 - `[--instance-id]` — L'ID di un'istanza Amazon di destinazione. EC2
 - `value--volume-id` — L'ID del volume.
- [`disassociate-address`](#): annulla l'associazione di un indirizzo IP virtuale all'istanza a cui è associato.
 - `--public-ip` — L'indirizzo IP virtuale che desideri dissociare dall'istanza.
- [`get-launch-template-data`](#) — Recupera i dati di configurazione dell'istanza specificata. È possibile utilizzare questi dati per creare un modello di lancio.
 - `--instance-id`: ID di una singola istanza sbe.
 - `--endpoint snowballEndpoint` — Un valore che consente di gestire le istanze di calcolo in modo programmatico utilizzando operazioni API compatibili con Amazon. EC2 Per ulteriori informazioni, consulta [Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge](#).
- [`modify-launch-template`](#) — Modifica un modello di avvio. È possibile specificare quale versione del modello di lancio impostare come versione predefinita. Quando si avvia un'istanza senza specificare una versione del modello di lancio, si applica la versione predefinita.

Specificare l'ID o il nome del modello di lancio nella richiesta.

- `-- launch-template-id string` — L'ID del modello di lancio.
- `-- launch-template-name string` — Un nome per il modello di lancio.
- `--default-version string` — Il numero di versione del modello di avvio da impostare come versione predefinita.
- `--endpoint snowballEndpoint` — Un valore che consente di gestire le istanze di calcolo in modo programmatico utilizzando operazioni API compatibili con Amazon. EC2 Per ulteriori informazioni, consulta [Specificazione dell'endpoint EC2 compatibile come endpoint AWS CLI su Snowball Edge](#).
- [`modify-instance-attribute`](#) — Modifica un attributo dell'istanza specificata. Sono supportati gli attributi

seguenti:

- `instanceInitiatedShutdownBehavior`
- `userData`
- [revoke-security-group-egress](#)— Rimuove una o più regole di uscita da un gruppo di sicurezza:
 - `[--group-idvalue]` — L'ID del gruppo di sicurezza
 - `[--ip-permissionsvalue]` — Uno o più set di autorizzazioni IP.
- [revoke-security-group-ingress](#)— Revoca una o più regole di ingresso a un gruppo di sicurezza. Quando chiami `revoke-security-group-ingress`, devi specificare un valore per `group-name` o `group-id`.
 - `[--group-namevalue]` — Il nome del gruppo di sicurezza.
 - `[--group-idvalue]` — L'ID del gruppo di sicurezza.
 - `[--ip-permissionsvalue]` — Uno o più set di autorizzazioni IP.
 - `[--protocol value]` Il protocollo IP. I valori possibili sono `tcp`, `udp` e `icmp`. L'argomento `--port` è obbligatorio, a meno che non sia stato specificato il valore "all protocols" (-1).
 - `[--portvalue]` — Per TCP o UDP, l'intervallo di porte da consentire. Un singolo numero intero o un intervallo (minimo-massimo).

Per ICMP, un numero intero o un intervallo (`type-code`) in cui `type` rappresenta il numero del tipo ICMP e `code` rappresenta il numero del codice ICMP. Il valore -1 indica tutti i codici ICMP per tutti i tipi di ICMP. Il valore -1 solo per `type` indica tutti i codici ICMP per il tipo di ICMP specificato.

- `[--cidrvalue]` — L'intervallo IP CIDR.
- [run-instances](#): avvia una serie di istanze di calcolo utilizzando un ID AMI Snowball per un'AMI.

Note

L'avvio di un'istanza di calcolo su Snowball Edge può richiedere fino a un'ora e mezza, a seconda delle dimensioni e del tipo di istanza.

- `[-- block-device-mappings (list)]` — Le voci di mappatura del dispositivo a blocchi. I parametri `DeleteOnTermination`, `VolumeSize` e `VolumeType` sono supportati. I volumi di avvio devono essere di tipo `sbg1`.

La sintassi JSON per questo comando è la seguente.

```
{
  "DeviceName": "/dev/sdh",
  "Ebs":
  {
    "DeleteOnTermination": true|false,
    "VolumeSize": 100,
    "VolumeType": "sbp1"|"sbg1"
  }
}
```

- `--count` — Numero di istanze da avviare. Specificando un numero singolo, questo viene considerato il numero minimo di istanze da avviare (il valore predefinito è 1). Specificando un intervallo nel formato `min:max`, il primo numero viene interpretato come il numero minimo e il secondo viene interpretato come il numero massimo di istanze da avviare.
- `--image-id` — L'ID Snowball AMI dell'AMI, che puoi ottenere chiamando `describe-images`. Per avviare un'istanza è necessaria un'AMI.
- `--InstanceInitiatedShutdownBehavior` — Per impostazione predefinita, quando si avvia uno spegnimento dall'istanza (utilizzando un comando come `shutdown` o `poweroff`), l'istanza si arresta. Puoi modificare questo comportamento in modo che l'istanza venga terminata anziché arrestata. I parametri `stop` e `terminate` sono supportati. Il valore predefinito è `stop`. Per ulteriori informazioni, consulta [Modifica del comportamento di arresto avviato dall'istanza nella Amazon EC2 User Guide for Linux Instances](#).
- `--instance-type`: tipo di istanza `sbe`.
- `--launch-template structure` — Il modello di avvio da utilizzare per avviare le istanze. I parametri specificati nel comando `run-instances` sostituiscono gli stessi parametri nel modello di lancio. È possibile specificare il nome o l'ID di un modello di lancio, ma non entrambi.

```
{
  "LaunchTemplateId": "string",
  "LaunchTemplateName": "string",
  "Version": "string"
}
```

- `--security-group-ids` — Uno o più gruppi di sicurezza. IDs È possibile creare un gruppo di sicurezza utilizzando [CreateSecurityGroup](#). Se non viene specificato alcun valore, viene assegnato l'ID per il gruppo di sicurezza di default per creare istanze.

- `--tag-specifications` — I tag da applicare alle risorse durante il lancio. Puoi assegnare un tag alle istanze al lancio. I tag specificati vengono applicati a tutti i volumi o le istanze creati durante il lancio. Per applicare tag a una risorsa dopo che è stata creata, utilizza `create-tags`.
- `--user-data` — I dati utente da rendere disponibili all'istanza. Se si utilizza la AWS CLI codifica base64 viene eseguita automaticamente ed è possibile caricare il testo da un file. In caso contrario, è necessario fornire testo con codifica base64.
- `--key-name (string)` — Il nome della coppia di chiavi. È possibile creare una key pair utilizzando `CreateKeyPair` o `ImportKeyPair`.

Warning

Se non specifichi una coppia di key pair, non puoi connetterti all'istanza a meno che non scegli un AMI configurato per consentire agli utenti un altro modo di accedere.

- [start-instances](#): avvia un'istanza che hai interrotto in precedenza. Tutte le risorse collegate all'istanza persistono attraverso avvii e arresti, ma vengono cancellate se l'istanza viene terminata.
 - `--instance-ids` — L'elenco IDs di una o più sbe istanze che sono state interrotte sul dispositivo.
- [stop-instances](#) — [Arresta un'istanza](#) in esecuzione. sbe Tutte le risorse collegate all'istanza persistono attraverso avvii e arresti, ma vengono cancellate se l'istanza viene terminata.
 - `--instance-ids` — L'elenco IDs di una o più sbe istanze da arrestare sul dispositivo.
- [terminate-instances](#) — [Chiude una o più istanze](#). Questa operazione è idempotente: terminando un'istanza più di una volta, ogni chiamata va a buon fine. Tutte le risorse collegate all'istanza persistono attraverso avvii e arresti, ma i dati vengono cancellati se l'istanza viene terminata.

Note

Per impostazione predefinita, quando si utilizza un comando simile a `shutdown` o `poweroff` per avviare un arresto dall'istanza, l'istanza si arresta. Tuttavia, puoi utilizzare l'`InstanceInitiatedShutdownBehavior` attributo per modificare questo comportamento in modo che questi comandi interrompano l'istanza. Per ulteriori informazioni, consulta [Modifica del comportamento di arresto avviato dall'istanza nella Amazon EC2 User Guide for Linux Instances](#).

- `--instance-ids` — Indica una o più sbe istanze da terminare sul IDs dispositivo. Tutti i dati collegati, archiviati per tali istanze, andranno persi.

- [create-key-pair](#)— Crea una coppia di chiavi RSA a 2048 bit con il nome specificato. Amazon EC2 archivia la chiave pubblica e visualizza la chiave privata per consentirti di salvarla in un file. La chiave privata viene restituita come chiave privata PKCS #1 non crittografata con codifica PEM. Se esiste già una chiave con il nome specificato, Amazon EC2 restituisce un errore.
- `--key-name (string)` — Un nome univoco per la coppia di chiavi.

Vincoli: fino a 255 caratteri ASCII.

- `[--tag-specifications] (list)` — I tag da applicare alla nuova key pair.

```
{
  "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
    ...
  ]
}
...
```

- [import-key-pair](#) —

- `--key-name (string)` — Un nome univoco per la coppia di chiavi.

Vincoli: fino a 255 caratteri ASCII.

- `--public-key-material (blob)` — La chiave pubblica. Per le chiamate API, il testo deve essere codificato in base 64. Per gli strumenti da riga di comando, la codifica base64 viene eseguita automaticamente.
- `[--tag-specifications] (list)` — I tag da applicare alla nuova key pair.

```
{
  "ResourceType": "image"|"instance"|"key-pair"|"launch-template"|"security-group",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
    ...
  ]
}
```

}

- [describe-key-pairs](#) –

[--filters] (list) — I filtri.

- key-pair-id — L'ID della key pair.
- key-name — Il nome della coppia di chiavi.
- tag-key — La chiave di un tag assegnato alla risorsa. Usa questo filtro per trovare tutte le risorse a cui è stato assegnato un tag con una chiave specifica, indipendentemente dal valore del tag.
- [--tag-specifications] (list) — I tag da applicare alla nuova key pair.
- tag:key — La key/value combinazione di un tag assegnato alla risorsa. Usa la chiave del tag nel nome del filtro e il valore del tag come valore del filtro. Ad esempio, per trovare tutte le risorse che hanno un tag con la chiave Owner e il valore Team A, specifica tag:Owner per il nome del filtro e Team A per il valore del filtro.

```
{
  "Name": "string",
  "Values": ["string", ...]
}
...
```

- [--key-names] (list) — I nomi delle coppie di chiavi.

Predefinito: descrive tutte le coppie di chiavi.

- [--key-pair-ids] (elenco) — Le coppie IDs di chiavi.
- [delete-key-pair](#) –
 - [--key-name] (string) — Il nome della coppia di chiavi.
 - [--key-pair-id] (string) — L'ID della coppia di key pair.

Operazioni API EC2 compatibili con Amazon supportate su Snowball Edge

Di seguito, puoi trovare le operazioni API EC2 compatibili con Amazon che puoi utilizzare con Snowball Edge, con collegamenti alle relative descrizioni nell' EC2 Amazon API Reference. Le chiamate API EC2 compatibili con Amazon richiedono la firma Signature Version 4 (SigV4). Se utilizzi AWS CLI o un AWS SDK per effettuare queste chiamate API, la firma SigV4 viene gestita automaticamente. In caso contrario, devi implementare la tua soluzione di firma SigV4. Per ulteriori informazioni, consulta [Acquisizione e utilizzo delle credenziali locali di Amazon S3 su Snowball Edge](#).

- [AssociateAddress](#)— Associa un indirizzo IP elastico a un'istanza o un'interfaccia di rete.
- [AttachVolume](#)— Sono supportati i seguenti parametri di richiesta:
 - Device
 - InstanceId
 - VolumeId
- [AuthorizeSecurityGroupEgress](#)— Aggiunge una o più regole di uscita a un gruppo di sicurezza da utilizzare con un dispositivo Snowball Edge. In particolare, questa azione consente alle istanze di inviare traffico a uno o più intervalli di indirizzi CIDR di destinazione IPv4 .
- [AuthorizeSecurityGroupIngress](#)— Aggiunge una o più regole di ingresso a un gruppo di sicurezza. Quando si chiama `AuthorizeSecurityGroupIngress`, è necessario specificare un valore per `GroupName` o `GroupId`.
- [CreateVolume](#)— Sono supportati i seguenti parametri di richiesta:
 - SnapshotId
 - Size
 - VolumeType
 - TagSpecification.N
- [CreateLaunchTemplate](#)— Sono supportati i seguenti parametri di richiesta:
 - ImageId
 - InstanceType
 - SecurityGroupIds
 - TagSpecifications
 - UserData
- [CreateLaunchTemplateVersion](#)
- [CreateTags](#)— Sono supportati i seguenti parametri di richiesta:
 - AMI
 - Instance
 - Launch template
 - Security group
- [CreateSecurityGroup](#)— Crea un gruppo di sicurezza su Snowball Edge. Puoi creare fino a 50 gruppi di sicurezza. Quando crei un gruppo di sicurezza, devi specificare un nome di tua scelta.
- [DeleteLaunchTemplate](#)

- [DeleteLaunchTemplateVersions](#)
- [DeleteSecurityGroup](#)— Elimina un gruppo di sicurezza. Se tenti di eliminare un gruppo di sicurezza associato a un'istanza o a cui fa riferimento un altro gruppo di sicurezza, l'operazione ha esito negativo con `DependencyViolation`.
- [DeleteTags](#)— Elimina il set di tag specificato dal set di risorse specificato.
- [DeleteVolume](#)— Sono supportati i seguenti parametri di richiesta:
 - `VolumeId`
- [DescribeAddresses](#)
- [DescribeImages](#)
- [DescribeInstanceAttribute](#)— Sono supportati i seguenti attributi:
 - `instanceType`
 - `userData`
- [DescribeInstanceStatus](#)
- [DescribeLaunchTemplates](#)
- [DescribeLaunchTemplateVersions](#)
- [DescribeInstances](#)
- [DescribeSecurityGroups](#)— Descrive uno o più gruppi di sicurezza. `DescribeSecurityGroups` è un'operazione impaginata. È possibile effettuare più chiamate API per recuperare l'intero set di dati dei risultati.
- [DescribeTags](#)— Con questo comando, sono supportati i seguenti filtri:
 - `resource-id`
 - `resource-type`— Solo AMI o istanze di calcolo
 - `key`
 - `value`
- [DescribeVolume](#)— Sono supportati i seguenti parametri di richiesta:
 - `MaxResults`
 - `NextToken`
 - `VolumeId.N`
- [DetachVolume](#)— Sono supportati i seguenti parametri di richiesta:
 - `Device`
 - `InstanceId`

- `VolumeId`
- [DisassociateAddress](#)
- [GetLaunchTemplateData](#)
- [ModifyLaunchTemplate](#)
- [ModifyInstanceAttribute](#)— È supportato solo l'`userData` attributo.
- [RevokeSecurityGroupEgress](#)— Rimuove una o più regole di uscita da un gruppo di sicurezza.
- [RevokeSecurityGroupIngress](#)— Revoca una o più regole di ingresso a un gruppo di sicurezza. Quando si chiama `RevokeSecurityGroupIngress`, è necessario specificare un valore per `o. group-name` `group-id`
- [RunInstances](#) –

 Note

L'avvio di un'istanza di calcolo su Snowball Edge può richiedere fino a un'ora e mezza, a seconda delle dimensioni e del tipo di istanza.

- [StartInstances](#)
- [StopInstances](#)— Le risorse associate a un'istanza interrotta persistono. È possibile terminare l'istanza per liberare queste risorse. Tuttavia, i relativi dati vengono eliminati.
- [TerminateInstances](#)

Istanze EC2 compatibili con avvio automatico con modelli di avvio su Snowball Edge

Puoi avviare automaticamente le istanze EC2 compatibili con Amazon sul tuo AWS Snowball Edge dispositivo utilizzando modelli di avvio e comandi di configurazione di avvio del client Snowball Edge.

Un modello di avvio contiene le informazioni di configurazione necessarie per creare un'istanza EC2 compatibile con Amazon su Snowball Edge. Puoi utilizzare un modello di avvio per memorizzare i parametri di avvio in modo da non doverli specificare ogni volta che avvii un'istanza EC2 compatibile su Snowball Edge.

Quando utilizzi le configurazioni di avvio automatico su Snowball Edge, configuri i parametri con cui desideri che inizi l'istanza compatibile con Amazon EC2. Dopo aver configurato Snowball Edge, al riavvio e allo sblocco utilizza la configurazione di avvio automatico per avviare un'istanza con i

parametri specificati. Se un'istanza avviata utilizzando una configurazione di avvio automatico viene arrestata, l'istanza si avvia quando si sblocca il dispositivo.

Note

Dopo aver configurato per la prima volta una configurazione di avvio automatico, riavviare il dispositivo per lanciarla. Tutti gli avvii successivi dell'istanza (dopo riavvii pianificati o non pianificati) avvengono automaticamente dopo lo sblocco del dispositivo.

Un modello di avvio può specificare l'ID Amazon Machine Image (AMI), il tipo di istanza, i dati utente, i gruppi di sicurezza e i tag per un'istanza EC2 compatibile con Amazon al momento del lancio dell'istanza. Per una lista di tipi di istanze supportate, consulta [Quote per le istanze di calcolo su un dispositivo Snowball Edge](#).

Per avviare automaticamente le istanze EC2 compatibili su Snowball Edge, procedi nel seguente modo:

1. Quando ordini il tuo AWS Snowball Edge dispositivo, crea un lavoro per ordinare un dispositivo Snowball Edge con istanze di calcolo. Per ulteriori informazioni, consulta [Creazione di un lavoro per ordinare uno Snowball Edge](#).
2. Dopo aver ricevuto Snowball Edge, sbloccalo.
3. Utilizzate il comando API EC2 `-compatible aws ec2 create-launch-template` per creare un modello di lancio.
4. Utilizzate il comando client Snowball Edge `snowballEdge create-autostart-configuration` per associare il modello di avvio dell'istanza EC2 compatibile alla configurazione di rete. Per ulteriori informazioni, consulta [Creazione di una configurazione EC2 di avvio compatibile su Snowball Edge](#).
5. Riavvia, quindi sblocca il dispositivo. Le istanze EC2 compatibili vengono avviate automaticamente utilizzando gli attributi specificati nel modello di avvio e nel comando client Snowball Edge `create-autostart-configuration`.

Per visualizzare lo stato delle istanze in esecuzione, utilizza il EC2 comando API `-compatible describe-autostart-configurations`.

 Note

Non esiste una console o un'API di gestione dei lavori per il AWS Snowball Edge supporto dei modelli di avvio. I comandi CLI del client EC2 -compatible e Snowball Edge vengono utilizzati per EC2 avviare automaticamente le istanze compatibili sul dispositivo. AWS Snowball Edge

Utilizzo di Instance Metadata Service for Snow con istanze EC2 compatibili con Amazon su Snowball Edge

IMDS for Snow fornisce Instance Metadata Service (IMDS) per istanze EC2 compatibili con Amazon su Snow. I metadati delle istanze sono categorie di informazioni sulle istanze. Include categorie come nome host, eventi e gruppi di sicurezza. Utilizzando IMDS for Snow, puoi utilizzare i metadati dell'istanza per accedere ai dati utente che hai specificato al momento del lancio dell'istanza compatibile con Amazon EC2. Ad esempio, puoi utilizzare IMDS for Snow per specificare i parametri per la configurazione dell'istanza o includere questi parametri in un semplice script. È possibile creare dati generici AMIs e utilizzare dati utente per modificare i file di configurazione forniti al momento dell'avvio.

Per ulteriori informazioni sui metadati delle istanze e sui dati utente e sulle istanze EC2 compatibili con Snow, consulta [Metadati delle istanze e dati utente supportati](#) in questa guida.

 Important

Anche se puoi accedere ai metadati dell'istanza e ai dati utente solo dall'interno dell'istanza stessa, i dati non sono protetti mediante metodi di autenticazione o crittografia. Chiunque disponga dell'accesso diretto all'istanza, e potenzialmente qualsiasi software in esecuzione sull'istanza, può visualizzare i propri metadati. Pertanto, è opportuno non memorizzare dati sensibili, ad esempio password o chiavi di crittografia di lunga durata, come dati utente.

 Note

Gli esempi di questa sezione utilizzano l' IPv4 indirizzo del servizio di metadati dell'istanza: 169.254.169.254. Non supportiamo il recupero dei metadati dell'istanza utilizzando l'indirizzo locale del collegamento. IPv6

Argomenti

- [Versioni IMDS su Snowball Edge](#)
- [Esempi di recupero dei metadati delle istanze utilizzando IMDSv1 e su Snowball IMDSv2 Edge](#)

Versioni IMDS su Snowball Edge

È possibile accedere ai metadati dell'istanza da un'istanza in esecuzione utilizzando IMDS versione 2 o IMDS versione 1:

- Instance Metadata Service versione 2 (IMDSv2), un metodo orientato alla sessione
- Instance Metadata Service versione 1 (IMDSv1), un metodo di richiesta-risposta

A seconda della versione del software Snow, puoi utilizzare o IMDSv1 entrambi IMDSv2. Ciò dipende anche dal tipo di AMI in esecuzione nell'istanza EC2 -compatible. Alcune AMIs, come quelle che eseguono Ubuntu 20.04, richiedono. IMDSv2 Il servizio di metadati delle istanze distingue tra IMDSv1 e IMDSv2 richieste in base alla presenza o alle intestazioniPUT. GET IMDSv2utilizza entrambe queste intestazioni. IMDSv1 utilizza solo l'GETintestazione.

AWS incoraggia l'uso di IMDSv2 piuttosto che IMDSv1 perché IMDSv2 include una maggiore sicurezza. Per ulteriori informazioni, consulta [Aggiungere una difesa approfondita contro firewall aperti, reverse proxy e vulnerabilità SSRF con](#) miglioramenti all'Instance Metadata Service. EC2

IMDSv2 su uno Snowball Edge

Quando si utilizza IMDSv2 per richiedere i metadati dell'istanza, la richiesta deve seguire queste regole:

1. Utilizza una richiesta PUT per inizializzare una sessione al servizio di metadati dell'istanza. La PUT richiesta restituisce un token di sessione che deve essere incluso nelle GET richieste successive al servizio di metadati dell'istanza. Il token di sessione che definisce la durata della sessione. La

durata della sessione può essere compresa tra un minimo di un secondo e un massimo di sei ore. Durante questa durata, puoi utilizzare lo stesso token di sessione per le richieste successive. Dopo la scadenza di questa durata, è necessario creare un nuovo token di sessione per le richieste future. Il token è necessario per accedere ai metadati utilizzando. IMDSv2

2. Includi il token in tutte le richieste GET al servizio di metadati dell'istanza.

- a. Il token è una chiave specifica dell'istanza. Il token non è valido su altre istanze EC2 compatibili e verrà rifiutato se si tenta di utilizzarlo al di fuori dell'istanza su cui è stato generato.
- b. La richiesta PUT deve includere un'intestazione che specifica il Time To Live (TTL) per il token, in secondi, fino a un massimo di sei ore (21.600 secondi). Il token rappresenta una sessione logica. Il TTL specifica la durata di validità del token e, pertanto, la durata della sessione.
- c. Dopo che un token scade, per continuare ad accedere ai metadati dell'istanza, devi creare una nuova sessione utilizzando un'altra richiesta PUT.
- d. Puoi scegliere di riutilizzare un token o creare un nuovo token con ogni richiesta. Per un piccolo numero di richieste, potrebbe essere più semplice generare e utilizzare immediatamente un token ogni volta che occorre accedere al servizio di metadati dell'istanza. Per maggior efficienza, tuttavia, puoi specificare una durata maggiore per il token e riutilizzarlo, piuttosto che dover riscrivere una richiesta PUT ogni volta che devi richiedere metadati dell'istanza. Non esiste un limite effettivo al numero di token simultanei, ciascuno dei quali rappresenta la propria sessione.

HTTP GET e HEAD metodi sono consentiti nelle richieste di metadati delle IMDSv2 istanze. PUT le richieste vengono rifiutate se contengono un X-Forwarded-For intestazione.

Per impostazione predefinita, la risposta alle PUT richieste ha un limite di risposta (time to live) di 1 a livello di protocollo IP. IMDS for Snow non è in grado di modificare il limite di hop per le PUT risposte.

L'esempio seguente utilizza uno script di shell Linux e IMDSv2 recupera gli elementi di metadati dell'istanza di primo livello. Questo esempio:

1. Crea un token di sessione della durata di sei ore (21.600 secondi) utilizzando la PUT richiesta.
2. Memorizza l'intestazione del token di sessione in una variabile denominata. TOKEN
3. Richiede gli elementi di metadati di primo livello utilizzando il token.

Usa due comandi per generare il EC2 token compatibile. È possibile eseguire i comandi separatamente o come un unico comando.

Innanzitutto, generare un token utilizzando il comando riportato di seguito.

Note

X-aws-ec2-metadata-token-ttl-seconds è un'intestazione obbligatoria. Se questa intestazione non è inclusa, riceverai un codice di errore 400 - Parametri mancanti o non validi.

```
[ec2-user ~]$ TOKEN=$(curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600")
```

Quindi, utilizzate il token per generare elementi di metadati di primo livello utilizzando il seguente comando.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

Note

Se si verifica un errore nella creazione del token, nella variabile viene memorizzato un messaggio di errore anziché un token valido e il comando non funzionerà.

È possibile memorizzare il token e combinare i comandi. L'esempio seguente combina i due comandi precedenti e memorizza l'intestazione del token di sessione in una variabile denominata `TOKEN`.

Example di comandi combinati

```
[ec2-user ~]$ TOKEN=$(curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

Dopo aver creato un token, puoi riutilizzarlo finché non scade. Il comando di esempio seguente ottiene l'ID dell'AMI utilizzato per avviare l'istanza e lo memorizza nell'ID \$TOKEN creato nell'esempio precedente.

Example di riutilizzare un token

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/ami-id
```

IMDSv1 su uno Snowball Edge

IMDSv1 utilizza il modello di richiesta-risposta. Per richiedere i metadati dell'istanza, invii una GET richiesta al servizio di metadati dell'istanza.

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

I metadati dell'istanza sono disponibili dall'istanza in esecuzione, quindi non è necessario utilizzare la EC2 AWS CLI console Amazon o accedervi. Ciò può risultare utile quando sta scrivendo script da eseguire dall'istanza. Ad esempio, puoi accedere all'indirizzo IP locale dell'istanza dai metadati dell'istanza per gestire una connessione a un'applicazione esterna. I metadati dell'istanza sono suddivisi in categorie. Per una descrizione di ciascuna categoria di metadati di istanza, consulta [Metadati delle istanze supportate e dati utente](#) in questa guida.

Per visualizzare tutte le categorie di metadati di istanza dall'interno di un'istanza in esecuzione, utilizza il seguente URI: IPv4

```
http://169.254.169.254/latest/meta-data/
```

Gli indirizzi IP sono indirizzi link-local e sono validi solo dall'istanza. Per ulteriori informazioni, consultare [Indirizzo link-local](#) su Wikipedia.

Tutti i metadati dell'istanza vengono restituiti come testo (tipo di contenuto HTTP text/plain).

Una richiesta per una specifica risorsa di metadati restituisce il valore appropriato o un codice di errore HTTP 404 - Not Found, se la risorsa non è disponibile.

Una richiesta per una risorsa di metadati generale (quando l'URI termina con un / carattere) restituisce un elenco di risorse disponibili o un codice di errore HTTP 404 - Not Found se tale risorsa non esiste. Gli elementi dell'elenco si trovano su righe separate, terminate da feed di riga (codice di caratteri ASCII 10).

Per le richieste effettuate utilizzando IMDSv1, è possibile restituire i seguenti codici di errore HTTP:

- 400 - Parametri mancanti o non validi: la PUT richiesta non è valida.
- 401 - Non autorizzato: la GET richiesta utilizza un token non valido. L'operazione consigliata è quella di generare un nuovo token.
- 403 - Proibita: la richiesta non è consentita o il servizio di metadati dell'istanza è disattivato.

Esempi di recupero dei metadati delle istanze utilizzando IMDSv1 e su Snowball IMDSv2 Edge

Gli esempi seguenti forniscono comandi che è possibile utilizzare su un'istanza Linux.

Example di come ottenere le versioni disponibili dei metadati dell'istanza

Questo esempio recupera le versioni disponibili dei metadati dell'istanza. Ogni versione fa riferimento a una build dei metadati dell'istanza quando sono state rilasciate nuove categorie di metadati dell'istanza. Le versioni precedenti sono disponibili in presenza di script basati sulla struttura e sulle informazioni presenti in una versione precedente.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
"X-aws-ec2-metadata-token-ttl-seconds: 21600" ` && curl -H "X-aws-ec2-metadata-token:
$TOKEN" -v http://169.254.169.254/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
 Dload  Upload   Total   Spent    Left  Speed
 100      56    100     56      0      0    3733      0 --:--:--
--:--:-- --:--:-- 3733
* Trying 169.254.169.254...
* TCP_NODELAY set
* Connected to 169.254.169.254 (169.254.169.254) port 80 (#0)
> GET / HTTP/1.1
> Host: 169.254.169.254
> User-Agent: curl/7.61.1
```

```
> Accept: */*
> X-aws-ec2-metadata-token:
MDAXcxNFLbAwJIYx8KzgNckcHTdxT4Tt69TzpKExlXKTULHIQnjEtXvD
>
* HTTP 1.0, assume close after body
< HTTP/1.0 200 OK
< Date: Mon, 12 Sep 2022 21:58:03 GMT
< Content-Length: 274
< Content-Type: text/plain
< Server: EC2ws
<
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27
2021-01-03
2021-03-23
* Closing connection 0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/
```



```
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
2016-06-30
2016-09-02
2018-03-28
2018-08-17
2018-09-24
2019-10-01
2020-10-27
2021-01-03
2021-03-23
latest
```

Example di ottenere gli elementi di metadati di primo livello

Questo esempio ottiene gli elementi di metadati di primo livello. Per informazioni sugli elementi di metadati di primo livello, consulta Metadati delle [istanze supportate e dati utente in questa](#) guida.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
"X-aws-ec2-metadata-token-ttl-seconds: 21600" ` && curl -H "X-aws-ec2-metadata-token:
$TOKEN" -v http://169.254.169.254/latest/meta-data/
ami-id
hostname
instance-id
instance-type
local-hostname
```

```
local-ipv4  
mac  
network/  
reservation-id  
security-groups
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/  
ami-id  
hostname  
instance-id  
instance-type  
local-hostname  
local-ipv4  
mac  
network/  
reservation-id  
security-groups
```

Example di ottenere i valori dei metadati di primo livello

Gli esempi seguenti ottengono i valori di alcuni degli elementi di metadati di primo livello ottenuti nell'esempio precedente. Le IMDSv2 richieste utilizzano il token memorizzato creato nel comando di esempio precedente, supponendo che non sia scaduto.

ami-id IMDSv2

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-  
data/ami-id ami-0abcdef1234567890
```

ami-id IMDSv1

```
curl http://169.254.169.254/latest/meta-data/ami-id ami-0abcdef1234567890
```

reservation-id IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/reservation-id r-0efghijk987654321
```

reservation-id IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id \r-0efghijk987654321
```

local-hostname IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/local-hostname ip-00-000-00-00
```

local-hostname IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname ip-00-000-00-00
```

Utilizzo dello storage a blocchi con istanze EC2 compatibili con Amazon su Snowball Edge

Con lo storage a blocchi su Snowball Edge, puoi aggiungere o rimuovere lo storage a blocchi in base alle esigenze delle tue applicazioni. I volumi collegati a un'istanza EC2 compatibile con Amazon sono esposti come volumi di storage che persistono indipendentemente dalla durata dell'istanza. Puoi gestire lo storage a blocchi utilizzando la familiare API Amazon EBS.

Alcuni comandi Amazon EBS sono supportati utilizzando l'endpoint EC2 -compatible. I comandi supportati includono attach-volume, create-volume, delete-volume, detach-volume e

`describe-volumes`. Per ulteriori informazioni su questi comandi, consulta [Elenco dei AWS CLI comandi EC2 compatibili supportati su Snowball Edge](#)

 Important

Assicuratevi di smontare tutti i file system del dispositivo all'interno del sistema operativo prima di scollegare il volume. In caso contrario, si potrebbe verificare la perdita di dati.

Di seguito, puoi trovare le quote di volume di Amazon EBS e le differenze tra i volumi Amazon EBS sul tuo dispositivo e i volumi Amazon EBS nel cloud:

- I volumi Amazon EBS sono disponibili solo per le istanze EC2 compatibili in esecuzione sul dispositivo che ospita i volumi.
- I tipi di volume sono limitati a HDD con capacità ottimizzata () o SSD con prestazioni ottimizzate (sbg1, sbp1). Il tipo di volume di default è sbg1.
- Snowball Edge condivide la memoria HDD tra oggetti Amazon S3 e Amazon EBS. Se utilizzi lo storage a blocchi basato su HDD AWS Snowball Edge, riduce la quantità di memoria disponibile per gli oggetti Amazon S3. Allo stesso modo, gli oggetti Amazon S3 riducono la quantità di memoria disponibile per lo storage a blocchi Amazon EBS su volumi HDD.
- I volumi EC2 root compatibili con Amazon utilizzano sempre il driver IDE. I volumi Amazon EBS aggiuntivi utilizzeranno preferibilmente il driver Virtio, se disponibile. Se il driver Virtio non è disponibile, SBE utilizza per impostazione predefinita il driver IDE. Il driver Virtio consente prestazioni migliori ed è consigliato.
- Quando si creano volumi Amazon EBS, il `encrypted` parametro non è supportato. Tuttavia, tutti i dati sul dispositivo sono crittografati per impostazione predefinita.
- La dimensione dei volumi può variare da 1 GB a 10 TB.
- È possibile collegare fino a 10 volumi Amazon EBS a una singola istanza EC2 compatibile.
- Non esiste un limite formale al numero di volumi Amazon EBS che puoi avere sul tuo AWS Snowball Edge dispositivo. Tuttavia, la capacità totale del volume di Amazon EBS è limitata dallo spazio disponibile sul dispositivo.

Controllo del traffico di rete con gruppi di sicurezza su Snowball Edge

Un gruppo di sicurezza funge da firewall virtuale che controlla il traffico di una o più istanze. Quando si avvia un'istanza, vi si associa uno o più gruppi di sicurezza. A ciascun gruppo di sicurezza possono essere aggiunte regole che permettono il traffico da e verso le istanze associate. Per ulteriori informazioni, consulta i [gruppi EC2 di sicurezza Amazon per le istanze Linux](#) nella Amazon EC2 User Guide.

I gruppi di sicurezza sui dispositivi Snowball Edge sono simili ai gruppi di sicurezza nel AWS cloud. I cloud privati virtuali (VPCs) non sono supportati sui dispositivi Snowball Edge.

Di seguito sono riportate le altre differenze tra i gruppi di sicurezza Snowball Edge e i gruppi di sicurezza EC2 VPC:

- Ogni dispositivo Snowball Edge ha un limite di 50 gruppi di sicurezza.
- Il gruppo di sicurezza predefinito consente tutto il traffico in entrata e in uscita.
- Il traffico tra le istanze locali può utilizzare l'indirizzo IP dell'istanza privata o un indirizzo IP pubblico. Ad esempio, supponiamo che tu voglia eseguire la connessione tramite SSH dall'istanza A all'istanza B. In questo caso, il tuo indirizzo IP di destinazione può essere l'IP pubblico o un indirizzo IP privato dell'istanza B, se la regola del gruppo di sicurezza regola consente il traffico.
- Sono supportati solo i parametri elencati per AWS CLI le azioni e le chiamate API. In genere sono un sottoinsieme di quelli supportati nelle istanze EC2 VPC.

Per ulteriori informazioni sulle AWS CLI azioni supportate, consulta [Elenco dei AWS CLI comandi EC2 compatibili supportati su Snowball Edge](#) Per ulteriori informazioni sulle operazioni API supportate, consulta [Operazioni API EC2 compatibili con Amazon supportate su Snowball Edge](#).

Metadati EC2 di istanza e dati utente compatibili supportati su Snowball Edge

I metadati dell'istanza sono dati relativi all'istanza che puoi utilizzare per configurare o gestire un'istanza in esecuzione. Snowball Edge supporta un sottoinsieme di categorie di metadati delle istanze per le istanze di calcolo. Per ulteriori informazioni, consulta [Metadati dell'istanza e dati utente](#) nella Amazon EC2 User Guide.

Sono supportate le categorie seguenti. L'utilizzo di qualsiasi altra categoria genera un messaggio di errore 404.

Categorie di metadati delle istanze supportate su un dispositivo Snowball Edge

Dati	Descrizione
<code>ami-id</code>	ID dell'AMI utilizzata per avviare l'istanza.
<code>hostname</code>	Il nome host IPv4 DNS privato dell'istanza.
<code>instance-id</code>	ID dell'istanza corrente.
<code>instance-type</code>	Tipo di istanza.
<code>local-hostname</code>	Il nome host IPv4 DNS privato dell'istanza.
<code>local-ipv4</code>	L' IPv4 indirizzo privato dell'istanza.
<code>mac</code>	Indirizzo MAC (Media Access Control) dell'istanza.
<code>network/interfaces/macs/ <i>mac</i> /local-hostname</code>	Nome host locale dell'interfaccia.
<code>network/interfaces/macs/ <i>mac</i> /local-ipv4s</code>	IPv4 Gli indirizzi privati associati all'interfaccia.
<code>network/interfaces/macs/ <i>mac</i> /mac</code>	Indirizzo MAC dell'istanza.
<code>network/interfaces/macs/ <i>mac</i> /public-ipv4s</code>	Indirizzi IP elastici associati all'interfaccia.
<code>public-ipv4</code>	L' IPv4 indirizzo pubblico.
<code>public-keys/0/openssh-key</code>	Chiave pubblica. Disponibile solo se viene specificato in fase di avvio dell'istanza.
<code>reservation-id</code>	ID della prenotazione.

Dati	Descrizione
userData	Gli script di shell inviano istruzioni a un'istanza al momento del lancio.

Categorie di dati dinamici delle istanze supportate su un dispositivo Snowball Edge

Dati	Descrizione
instance-identity/document	JSON contenente gli attributi dell'istanza. Solo <code>instanceId</code> , <code>imageId</code> , <code>privateIp</code> e <code>instanceType</code> hanno valori, mentre gli altri attributi restituiti sono null. Per ulteriori informazioni, consulta Instance Identity Documents nella Amazon EC2 User Guide.

Dati utente delle istanze di computer su Snowball Edge

Utilizza gli script di shell per accedere ai dati utente delle istanze di calcolo su un dispositivo Snowball Edge. Utilizzando gli script di shell, puoi inviare istruzioni a un'istanza al momento del lancio. È possibile modificare i dati utente con il `modify-instance-attribute` AWS CLI comando o l'`ModifyInstanceAttribute` API.

Per modificare i dati utente

1. Arresta l'istanza di calcolo con il `stop-instances` AWS CLI comando.
2. Utilizzando il `modify-instance-attribute` AWS CLI comando, modificate l'`userData` attributo.
3. Riavvia l'istanza di calcolo con il `start-instances` AWS CLI comando.

Per le istanze di calcolo sono supportati solo gli script di shell. Non è disponibile alcun supporto per le direttive sui `cloud-init` pacchetti sulle istanze di calcolo in esecuzione su un dispositivo Snowball Edge. [Per ulteriori informazioni sull'utilizzo dei AWS CLI comandi, consulta la Guida ai comandi.AWS CLI](#)

Arresto delle istanze EC2 compatibili in esecuzione su Snowball Edge

Per evitare di eliminare accidentalmente le istanze EC2 compatibili con Amazon che crei su un dispositivo, non chiudere le istanze dal sistema operativo. Ad esempio, non utilizzare i comandi shutdown o reboot. L'arresto di un'istanza dal sistema operativo ha lo stesso effetto di chiamare il comando [terminate-instances](#).

Utilizza invece il comando [stop-instances](#) per sospendere le istanze EC2 compatibili con Amazon che desideri conservare.

Utilizzo AWS IoT Greengrass per eseguire software preinstallato su istanze EC2 compatibili con Amazon su Snowball Edge

AWS IoT Greengrass è un servizio cloud e runtime edge open source per l'Internet of Things (IoT) che ti aiuta a creare, implementare e gestire applicazioni IoT sui tuoi dispositivi. Puoi utilizzarlo AWS IoT Greengrass per creare software che consenta ai tuoi dispositivi di agire localmente sui dati generati, eseguire previsioni basate su modelli di apprendimento automatico e filtrare e aggregare i dati dei dispositivi. Per informazioni dettagliate su AWS IoT Greengrass, consulta [Cos'è? AWS IoT Greengrass](#) nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori.

Utilizzandolo AWS IoT Greengrass sul dispositivo Snowball Edge, consenti al dispositivo di raccogliere e analizzare i dati più vicino a dove vengono generati, reagire in modo autonomo agli eventi locali e comunicare in modo sicuro con altri dispositivi sulla rete locale.

Configurazione di un'istanza EC2 compatibile con Amazon per AWS IoT Greengrass su Snowball Edge

Note

Per eseguire l'installazione AWS IoT Greengrass Version 2 su un dispositivo Snowball Edge, assicurati che il dispositivo sia connesso a Internet. Dopo l'installazione, non è necessario disporre di Internet per il funzionamento di un dispositivo Snowball Edge. AWS IoT Greengrass

Per configurare un'istanza EC2 compatibile per AWS IoT Greengrass V2

1. Avvia l'AMI AWS IoT Greengrass convalidato con un indirizzo IP pubblico e una chiave SSH:
 - a. [Utilizzando le istanze AWS CLI: run-instances.](#)
 - b. Utilizzo AWS OpsHub: [avvio di un'istanza EC2 compatibile con Amazon.](#)

 Note

Prendi nota dell'indirizzo IP pubblico e del nome della chiave SSH associati all'istanza.

2. Connect all'istanza EC2 -compatible usando SSH. A tale scopo, esegui il comando seguente sul computer collegato al dispositivo. Sostituiscilo *ssh-key* con la chiave che hai usato per avviare l'istanza EC2 -compatible. Sostituisci *public-ip-address* con l'indirizzo IP pubblico dell'istanza EC2 -compatible.

```
ssh -i ssh-key ec2-user@ public-ip-address
```

 Important

Se il tuo computer utilizza una versione precedente di Microsoft Windows, potresti non avere il comando SSH oppure potresti avere SSH ma non riesci a connetterti alla tua istanza EC2 compatibile. Per connetterti alla tua istanza EC2 compatibile, puoi installare e configurare PuTTY, un client SSH open source gratuito. È necessario convertire la chiave SSH dal .pem formato al formato PuTTY e connettersi all'istanza. EC2 Per istruzioni su come eseguire la conversione dal .pem formato PuTTY, [consulta Converti la tua chiave privata usando PuTTYgen](#) nella Amazon EC2 User Guide.

Installazione AWS IoT Greengrass su un'istanza EC2 compatibile su Snowball Edge

Successivamente, configuri l'istanza EC2 compatibile come dispositivo AWS IoT Greengrass Core da utilizzare per lo sviluppo locale.

Per installare AWS IoT Greengrass

1. Utilizzare il comando seguente per installare il software prerequisito per AWS IoT Greengrass. Questo comando installa AWS Command Line Interface (AWS CLI) v2, Python 3 e Java 8.

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
&& unzip awscliv2.zip && sudo ./aws/install && sudo yum -y install python3
java-1.8.0-openjdk
```

2. Concedi all'utente root il permesso di eseguire il AWS IoT Greengrass software e modifica l'autorizzazione root da root ALL=(ALL) ALL a root ALL=(ALL:ALL) ALL nel file di configurazione sudoers.

```
sudo sed -in 's/root\tALL=(ALL)/root\tALL=(ALL:ALL)/' /etc/sudoers
```

3. Usa il seguente comando per scaricare il AWS IoT Greengrass software Core.

```
curl -s https://d2s8p88vqu9w66.cloudfront.net/releases/greengrass-nucleus-latest.zip > greengrass-nucleus-latest.zip && unzip greengrass-nucleus-latest.zip -d GreengrassCore && rm greengrass-nucleus-latest.zip
```

4. Utilizzate i seguenti comandi per fornire le credenziali che consentono di installare il software AWS IoT Greengrass Core. Sostituisci i valori di esempio con le tue credenziali:

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE  
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
```

Note

Si tratta di credenziali dell'utente IAM della AWS regione, non del dispositivo Snowball Edge.

5. Usa il seguente comando per installare il software AWS IoT Greengrass Core. Il comando crea AWS le risorse necessarie al software di base per il funzionamento e configura il software di base come servizio di sistema che viene eseguito all'avvio dell'AMI.

Sostituire i seguenti parametri nel comando:

- **region:** La AWS regione in cui trovare o creare risorse.
- **MyGreengrassCore:** Il nome dell' AWS IoT oggetto per il dispositivo AWS IoT Greengrass principale.
- **MyGreengrassCoreGroup:** Il nome del AWS IoT gruppo di oggetti per il dispositivo AWS IoT Greengrass principale.

```
sudo -E java -Droot="/greengrass/v2" -Dlog.store=FILE \  
-jar ./GreengrassInstaller/lib/Greengrass.jar \  
--aws-region region \  
--thing-name MyGreengrassCore \  
--thing-group-name MyGreengrassCoreGroup \  
--thing-policy-name GreengrassV2IoTThingPolicy \  
--tes-role-name GreengrassV2TokenExchangeRole \  
--tes-role-alias-name GreengrassCoreTokenExchangeRoleAlias \  
--component-default-user ggc_user:ggc_group \  
--provision true \  
--setup-system-service true \  
--deploy-dev-tools true
```

Note

Questo comando è per un'istanza EC2 compatibile con Amazon che esegue un'AMI Amazon Linux 2. Per un'AMI Windows, vedi [Installare il software AWS IoT Greengrass Core](#).

Al termine, sul dispositivo Snowball Edge verrà eseguito un AWS IoT Greengrass core per l'uso locale.

Utilizzo AWS Lambda con un AWS Snowball Edge

AWS Lambda powered by AWS IoT Greengrass è un servizio di elaborazione che consente di eseguire codice serverless (funzioni Lambda) localmente sui dispositivi Snowball Edge. Puoi usare Lambda per richiamare funzioni Lambda su un dispositivo Snowball Edge con messaggi MQTT (Message Queuing Telemetry Transport), eseguire codice Python nelle funzioni Lambda e utilizzarle per chiamare gli endpoint del servizio pubblico nel cloud. AWS Per utilizzare le funzioni Lambda con i dispositivi Snowball Edge, è necessario creare i job Snowball Edge in un ambiente supportato da Regione AWS AWS IoT Greengrass Per un elenco di quelli validi Regioni AWS, consulta [AWS IoT Greengrass](#). Riferimenti generali di AWS Lambda on Snowball Edge è disponibile nelle regioni in cui sono disponibili dispositivi Lambda e Snowball Edge.

Note

Se assegni la quantità minima consigliata di 128 MB di memoria per ciascuna delle tue funzioni, puoi avere fino a sette funzioni Lambda in un singolo job.

Argomenti

- [Guida introduttiva a Lambda su Snowball Edge](#)
- [Implementazione di una funzione Lambda su un dispositivo Snowball Edge](#)

Guida introduttiva a Lambda su Snowball Edge

Prima di creare una funzione Lambda in linguaggio Python da eseguire su Snowball Edge, ti consigliamo di acquisire familiarità con i seguenti servizi, concetti e argomenti correlati.

Prerequisiti per AWS IoT Greengrass on Snowball Edge

AWS IoT Greengrass è un software che estende Cloud AWS le funzionalità ai dispositivi locali. AWS IoT Greengrass consente ai dispositivi locali di raccogliere e analizzare i dati in modo più vicino alla fonte delle informazioni, comunicando al contempo in modo sicuro tra loro sulle reti locali. Più specificamente, gli sviluppatori che lo utilizzano AWS IoT Greengrass possono creare codice serverless (funzioni Lambda) in Cloud AWS Possono quindi distribuire efficacemente questo codice sui dispositivi per l'esecuzione locale delle applicazioni.

I seguenti AWS IoT Greengrass concetti sono importanti da comprendere quando si utilizza AWS IoT Greengrass su uno Snowball Edge:

- AWS IoT Greengrass requisiti: per un elenco completo dei AWS IoT Greengrass requisiti, consulta [Requisiti](#) nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori.
- AWS IoT Greengrass core: scarica il software di AWS IoT Greengrass base e installalo su un' EC2 istanza in esecuzione sul dispositivo. Consulta [la sezione Utilizzo AWS IoT Greengrass su EC2 istanze Amazon](#) in questa guida.

Per utilizzare le funzioni Lambda su un dispositivo Snowball Edge, devi prima installare il software AWS IoT Greengrass Core su un' EC2 istanza Amazon sul dispositivo. Le funzioni Lambda che intendi utilizzare sul dispositivo Snowball Edge devono essere create con lo stesso account che utilizzerai per l'installazione sul AWS IoT Greengrass dispositivo Snowball Edge. Per informazioni sull'installazione AWS IoT Greengrass sul dispositivo Snowball Edge, consulta. [Utilizzo AWS IoT Greengrass per eseguire software preinstallato su istanze EC2 compatibili con Amazon su Snowball Edge](#)

- AWS IoT Greengrass gruppo: un dispositivo Snowball Edge fa parte di un AWS IoT Greengrass gruppo come dispositivo principale del gruppo. Per ulteriori informazioni sui gruppi, consulta [AWS Greengrass IoT Groups](#) nella AWS IoT Greengrass Developer Guide.
- MQTT: AWS IoT Greengrass utilizza il protocollo MQTT leggero e standard del settore per comunicare all'interno di un gruppo. Qualsiasi dispositivo o software compatibile con MQTT del gruppo può richiamare messaggi MQTT. AWS IoT Greengrass Questi messaggi possono richiamare funzioni Lambda, se si definisce il relativo messaggio MQTT a tale scopo.

Prerequisiti per AWS Lambda on Snowball Edge

AWS Lambda è un servizio di elaborazione che consente di eseguire codice senza effettuare il provisioning o la gestione di server. I seguenti concetti di Lambda sono importanti da comprendere quando si utilizza Lambda con Snowball Edge:

- Funzioni Lambda: codice personalizzato, caricato e pubblicato su Lambda e utilizzato su Snowball Edge. Per ulteriori informazioni, consulta [Lambda Functions](#) nella AWS Lambda Developer Guide.
- Console Lambda: la console in cui carichi, aggiorni e pubblichi le funzioni Lambda in linguaggio Python da utilizzare su Snowball Edge. Per ulteriori informazioni sulla console [Lambda](#), consulta [Console Lambda nella Developer Guide](#).AWS Lambda

- Python: il linguaggio di programmazione di alto livello utilizzato per le funzioni Lambda con tecnologia su AWS IoT Greengrass Snowball Edge. AWS IoT Greengrass supporta la versione 3.8.x di Python.

Implementazione di una funzione Lambda su un dispositivo Snowball Edge

Per eseguire una funzione Lambda su un dispositivo Snowball Edge in un AWS IoT Greengrass gruppo, importa la funzione come componente. Per informazioni complete sull'importazione di una funzione come componente utilizzando la AWS IoT Greengrass console, consulta [Importare una funzione Lambda come componente \(console\)](#) nella AWS IoT Greengrass Version 2 Developer Guide.

1. Nella console AWS IoT, nella pagina dei componenti di Greengrass, scegli Crea componente.
2. In Origine componente, scegli Importa funzione Lambda. Nella funzione Lambda, scegli il nome della tua funzione. Nella versione della funzione Lambda, scegli la versione della tua funzione.
3. Per sottoscrivere la funzione ai messaggi su cui può agire, scegli Aggiungi origine evento e scegli l'evento. In Timeout (secondi), fornisci un periodo di timeout in secondi.
4. In Pinned, scegli se bloccare o meno la tua funzione.
5. Scegli Crea componente
6. Seleziona Deploy (Implementa).
7. In Deployment, scegli Aggiungi alla distribuzione esistente, quindi scegli il tuo gruppo Greengrass. Scegli Next (Successivo).
8. In Public components, scegli questi componenti:
 - aws.greengrass.cli
 - aws.greengrass. LambdaLauncher
 - aws.greengrass. LambdaManager
 - aws.greengrass. LambdaRuntimes
 - AWS. Greengrass. Nucleus
9. Seleziona Deploy (Implementa).

Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge

Lo storage compatibile con Amazon S3 su Snowball Edge offre uno storage di oggetti sicuro con maggiore resilienza, scalabilità e un set di funzionalità API Amazon S3 esteso per ambienti robusti, mobili, edge e disconnessi. Utilizzando lo storage compatibile con Amazon S3 su Snowball Edge, puoi archiviare dati ed eseguire applicazioni ad alta disponibilità su Snowball Edge per l'edge computing.

Puoi creare bucket Amazon S3 sui dispositivi Snowball Edge per archiviare e recuperare oggetti in locale per applicazioni che richiedono l'accesso locale ai dati, l'elaborazione locale dei dati e la residenza dei dati. Lo storage compatibile con Amazon S3 su Snowball Edge offre una nuova classe di storage che utilizza Amazon S3 ed è progettata per archiviare i dati in modo duraturo e ridondante su più dispositivi APIs Snowball Edge. SNOW Sui bucket Snowball Edge puoi utilizzare le stesse APIs funzionalità che usi su Amazon S3, tra cui le policy del ciclo di vita dei bucket, la crittografia e l'etichettatura. Quando il dispositivo o i dispositivi vengono restituiti AWS, tutti i dati creati o archiviati nello storage compatibile con Amazon S3 su Snowball Edge vengono cancellati. Per ulteriori informazioni, consulta [Local Compute and Storage Only Jobs](#).

Puoi distribuire lo storage compatibile con Amazon S3 su Snowball Edge in configurazione autonoma o in configurazione cluster. Nella configurazione autonoma, puoi fornire la capacità S3 sul dispositivo e il saldo è disponibile come storage a blocchi. Nella configurazione del cluster, tutta la capacità del disco dati viene utilizzata per lo storage S3. Un cluster può essere composto da un minimo di 3 dispositivi fino a un massimo di 16 dispositivi. A seconda delle dimensioni del cluster, il servizio S3 è progettato per mantenere la tolleranza ai guasti del dispositivo di 1 o 2 dispositivi.

Con AWS DataSync, puoi trasferire oggetti tra lo storage compatibile con Amazon S3 su Snowball Edge su un dispositivo Snowball Edge e i servizi di storage. AWS Per ulteriori informazioni, consulta [Configurazione dei trasferimenti con storage compatibile con S3 su Snowball Edge](#) nella Guida per l'utente. AWS DataSync

Di seguito sono riportate la capacità di storage compatibile con Amazon S3 su Snowball Edge e la capacità di storage a blocchi per un dispositivo autonomo che utilizza lo storage compatibile con Amazon S3 su Snowball Edge. Per la tolleranza agli errori e la capacità di storage dei cluster, vedi [this table](#)

Snowball Edge Compute Optimized with NVMe storage

Capacità di storage dello storage compatibile con Amazon S3 su Snowball Edge e dello storage a blocchi di dispositivi Snowball Edge Compute Optimized (Compute Optimized with AMD EPYC Gen2 e) NVMe

Storage compatibile con Amazon S3 con capacità di storage Snowball Edge (in TB)	Capacità di storage a blocchi (in TB)
3	17,5
5.5	14,5
10.5	8,5
12	6,5
13	5.5
16,5	1.5

Snowball Edge storage optimized 210 TB

Capacità di storage dello storage compatibile con Amazon S3 su Snowball Edge e dello storage a blocchi di dispositivi da 210 TB ottimizzati per lo storage Snowball Edge

Storage compatibile con Amazon S3 con capacità di storage Snowball Edge (in TB)	Capacità di storage a blocchi (in TB)
20	206
40	182
60	158
80	134
100	110
120	86

Storage compatibile con Amazon S3 con capacità di storage Snowball Edge (in TB)	Capacità di storage a blocchi (in TB)
140	62
160	38
180	14
190	2

Specifiche dello storage compatibile con Amazon S3 su Snowball Edge:

- Il numero massimo di bucket Snowball Edge è 100 per dispositivo o per cluster.
- L'account proprietario del bucket S3 on Snowball Edge possiede tutti gli oggetti nel bucket.
- Solo l'account proprietario del bucket S3 on Snowball Edge può eseguire operazioni sul bucket.
- Le limitazioni relative alle dimensioni degli oggetti sono coerenti con quelle di Amazon S3.
- Tutti gli oggetti archiviati su S3 su Snowball Edge hanno SNOW come classe di archiviazione.
- Per impostazione predefinita, tutti gli oggetti archiviati nella classe di storage SNOW vengono archiviati utilizzando la crittografia lato server con chiavi di crittografia gestite di Amazon S3 (SSE-S3). Puoi inoltre scegliere di archiviare esplicitamente gli oggetti utilizzando la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C).
- Se non c'è abbastanza spazio per archiviare un oggetto su Snowball Edge, l'API restituisce un'eccezione di capacità insufficiente (ICE).

Argomenti

- [Ordina uno storage compatibile con Amazon S3 su Snowball Edge](#)
- [Configurazione e avvio dello storage compatibile con Amazon S3 su Snowball Edge](#)
- [Utilizzo di bucket S3 con storage compatibile con Amazon S3 su Snowball Edge](#)
- [Determinare se è possibile accedere a uno storage compatibile con Amazon S3 su un bucket Snowball Edge su Snowball Edge](#)
- [Recupero di un elenco di bucket o bucket regionali nello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge](#)
- [Ottenere un bucket con storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge](#)

- [Creazione di un bucket S3 nello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge](#)
- [Eliminazione di un bucket in uno storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge](#)
- [Creazione e gestione di una configurazione del ciclo di vita degli oggetti utilizzando il AWS CLI](#)
- [Copiare un oggetto su uno storage compatibile con Amazon S3 su un bucket Snowball Edge su Snowball Edge](#)
- [Elencare oggetti in un bucket nello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge](#)
- [Recupero di un oggetto da un bucket nello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge](#)
- [Eliminazione di oggetti nei bucket nello storage compatibile con Amazon S3 su Snowball Edge](#)
- [Azioni API REST supportate per lo storage compatibile con Amazon S3 su Snowball Edge](#)
- [Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge con un cluster di dispositivi Snow](#)
- [Configurazione dello storage compatibile con Amazon S3 sulle notifiche degli eventi Snowball Edge](#)
- [Configurazione delle notifiche SMTP locali su Snowball Edge](#)

Ordina uno storage compatibile con Amazon S3 su Snowball Edge

L'ordinazione di un dispositivo per lo storage compatibile con Amazon S3 su Snowball Edge è molto simile alla procedura per ordinare uno Snowball Edge. Per ordinare, consulta questa guida e tieni [Creazione di un lavoro per ordinare un dispositivo Snowball Edge](#) a mente questi articoli durante il processo di ordinazione:

- Per Scegli un tipo di lavoro, scegli Solo elaborazione e archiviazione locali.
- Tra i dispositivi Snow, scegli Snowball Edge Compute Optimized
- In Seleziona il tipo di storage, seleziona lo storage compatibile con Amazon S3 su Snowball Edge.
- Per un dispositivo autonomo, in Capacità di archiviazione, scegli Dispositivo singolo, quindi seleziona la quantità di spazio di archiviazione desiderata.
- Per un cluster, in Capacità di archiviazione seleziona Cluster, quindi seleziona la capacità di archiviazione e la tolleranza di errore desiderate.

Configurazione e avvio dello storage compatibile con Amazon S3 su Snowball Edge

Installa e configura strumenti software dal tuo ambiente locale AWS per interagire con il dispositivo Snowball Edge o il cluster di dispositivi e lo storage compatibile con Amazon S3 su Snowball Edge. Utilizza quindi questi strumenti per configurare il dispositivo o il cluster Snowball Edge e avviare lo storage compatibile con Amazon S3 su Snowball Edge.

Prerequisiti

Lo storage compatibile con Amazon S3 su Snowball Edge richiede che il client Snowball Edge e lo siano installati nell' AWS CLI ambiente locale. Puoi anche utilizzare AWS strumenti SDK per .NET e strumenti per Windows per PowerShell lavorare con lo storage compatibile con Amazon S3 su Snowball Edge. AWS consiglia di utilizzare le seguenti versioni di questi strumenti:

- Snowball Edge Client: utilizza la versione più recente. Per ulteriori informazioni, consulta [Scaricamento e installazione del client Snowball Edge](#) in questa guida.
- AWS CLI— Versione 2.11.15 o successiva. Per ulteriori informazioni, vedere [Installazione, aggiornamento e disinstallazione di AWS CLI nella Guida per l'utente](#). AWS Command Line Interface
- SDK per .NET— AWSSDK .S3Control 3.7.304.8 o versione successiva. Per ulteriori informazioni, consulta [AWS SDK per .NET](#).
- AWS Strumenti per Windows: versione 4.1.476 o successiva. PowerShell Per ulteriori informazioni, consulta la [Guida per l'utente di AWS Strumenti per PowerShell](#).

Configurazione dell'ambiente locale

Questa sezione descrive come configurare il client Snowball Edge e l'ambiente locale per l'utilizzo con lo storage compatibile con Amazon S3 su Snowball Edge.

1. Scarica e installa il client Snowball Edge. Per ulteriori informazioni, consulta [Scaricamento e installazione del client Snowball Edge](#).
2. Configura un profilo per il client Snowball Edge. Per ulteriori informazioni, consulta [Configurazione di un profilo per il client Snowball Edge](#).
3. Se lo stai utilizzando SDK per .NET, imposta il valore del `clientConfig.AuthenticationRegion` parametro come segue:

```
clientConfig.AuthenticationRegion = "snow"
```

Configurazione del dispositivo Snowball Edge

Configurazione di IAM su Snowball Edge

AWS Identity and Access Management (IAM) ti aiuta a abilitare l'accesso granulare alle AWS risorse eseguite sui tuoi dispositivi Snowball Edge. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse.

IAM è supportato localmente su Snowball Edge. Puoi utilizzare il servizio IAM locale per creare ruoli e associare ad essi policy IAM. È possibile utilizzare questi criteri per consentire l'accesso necessario per eseguire le attività assegnate.

L'esempio seguente consente l'accesso completo all'API Amazon S3:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Per altri esempi di policy IAM, consulta la [AWS Snowball Edge Developer Guide](#).

Avvio dello storage compatibile con Amazon S3 sul servizio Snowball Edge

Utilizza le seguenti istruzioni per avviare lo storage compatibile con Amazon S3 sul servizio Snowball Edge su un dispositivo o cluster Snowball Edge.

Se preferisci un'esperienza più intuitiva, puoi avviare lo storage compatibile con Amazon S3 sul servizio Snowball Edge per un dispositivo autonomo o un cluster di dispositivi utilizzando AWS OpsHub Consultare [Configura lo storage compatibile con Amazon S3 su Snowball Edge con AWS OpsHub](#).

1. Sblocca il dispositivo o il cluster di dispositivi Snowball Edge eseguendo il seguente comando:

- Per un singolo dispositivo:

```
snowballEdge unlock-device --endpoint https://snow-device-ip
```

- Per un cluster:

```
snowballEdge unlock-cluster
```

2. Esegui il comando seguente e assicurati che il dispositivo Snowball Edge o il cluster di dispositivi sia sbloccato:

- Per un singolo dispositivo:

```
snowballEdge describe-device --endpoint https://snow-device-ip
```

- Per un cluster:

```
snowballEdge describe-cluster --device-ip-addresses [snow-device-1-ip] [snow-device-2-ip] /  
[snow-device-3-ip] [snow-device-4-ip] [snow-device-5-ip] /  
[snow-device-6-ip]
```

3. Per ogni dispositivo (che tu ne abbia uno o un cluster), per avviare lo storage compatibile con Amazon S3 su Snowball Edge, procedi come segue:

- a. Recupera i dispositivi `PhysicalNetworkInterfaceId` eseguendo il seguente comando:
`describe-device`

```
snowballEdge describe-device --endpoint https://snow-device-ip
```

- b. Esegui il `create-virtual-network-interface` comando seguente due volte per creare le interfacce di rete virtuali (VNI) per gli endpoint `s3control` (per le operazioni sui bucket) e `s3api` (per le operazioni sugli oggetti).

```
snowballEdge create-virtual-network-interface --ip-address-assignment
dhcp --manifest-file manifest --physical-network-interface-id
"PhysicalNetworkInterfaceId" --unlock-code unlockcode --endpoint https://snow-
device-ip
```

Il comando restituisce una struttura JSON che include l'indirizzo IP. Prendere nota di tale indirizzo IP.

Per informazioni dettagliate su questi comandi, consulta [Configurazione di un'interfaccia di rete virtuale \(VNI\) su Snowball Edge](#).

 Note

L'avvio dello storage compatibile con Amazon S3 su Snowball Edge consuma le risorse del dispositivo.

4. Avvia lo storage compatibile con Amazon S3 sul servizio Snowball Edge eseguendo il seguente `start-service` comando, che include gli indirizzi IP dei tuoi dispositivi e gli Amazon Resource Names (ARNs) degli endpoint VNI che hai creato per gli endpoint `s3control` `s3api`

Per avviare il servizio su un singolo dispositivo:

```
snowballEdge start-service --service-id s3-snow --device-ip-addresses snow-
device-1-ip --virtual-network-interface-arns vni-arn-1 vni-arn-2
```

Per avviare il servizio su un cluster:

```
snowballEdge start-service --service-id s3-snow --device-ip-addresses snow-
device-1-ip snow-device-2-ip snow-device-3-ip --virtual-network-interface-arns vni-
arn-1 vni-arn-2 vni-arn-3 vni-arn-4 vni-arn-5 vni-arn-6
```

Per `--virtual-network-interface-arns`, ARNs includi tutto VNIs ciò che hai creato nel passaggio precedente. Separa ogni ARN utilizzando uno spazio.

5. Esegui il `describe-service` comando seguente per un singolo dispositivo:

```
snowballEdge describe-service --service-id s3-snow
```

Attendi che lo stato del servizio sia `Active`.

Esegui il `describe-service` comando seguente per un cluster:

```
snowballEdge describe-service --service-id s3-snow \  
--device-ip-addresses snow-device-1-ip snow-device-2-ip snow-device-3-ip
```

Visualizzazione delle informazioni sullo storage compatibile con Amazon S3 sugli endpoint Snowball Edge

Quando lo storage compatibile con Amazon S3 sul servizio Snowball Edge è in esecuzione, puoi utilizzare il comando `describe-service` Snowball Edge Client per visualizzare gli indirizzi IP associati agli endpoint `s3control` e `s3api`.

```
snowballEdge describe-service --service-id s3-snow --endpoint https://snow-device-ip-address --profile profile-name
```

Example output del comando **describe-service**

In questo esempio, l'indirizzo IP dell'endpoint `s3control` è 192.168.1.222 e l'indirizzo IP dell'endpoint `s3api` è 192.168.1.152.

```
{  
  "ServiceId": "s3-snow",  
  "Autostart": true,  
  "Status": {  
    "State": "ACTIVATING",  
    "Details": "Attaching storage"
```



```

},
"ServiceCapacities": [
  {
    "Name": "S3 Storage",
    "Unit": "Byte",
    "Used": 148599705600,
    "Available": 19351400294400
  }
],
"Endpoints": [
  {
    "Protocol": "https",
    "Port": 443,
    "Host": "192.168.1.222",
    "CertificateAssociation": {
      "CertificateArn": "arn:aws:snowball-
device:::certificate/30c563f1124707705117f57f6c3accd42a4528ed6dba1e35c1822a391a717199d8c49973d3
    },
    "Description": "s3-snow bucket API endpoint (for s3control SDK)",
    "DeviceId": "JID-beta-207429000001-23-12-28-03-51-11",
    "Status": {
      "State": "ACTIVE"
    }
  },
  {
    "Protocol": "https",
    "Port": 443,
    "Host": "192.168.1.152",
    "CertificateAssociation": {
      "CertificateArn": "arn:aws:snowball-
device:::certificate/30c563f1124707705117f57f6c3accd42a4528ed6dba1e35c1822a391a717199d8c49973d3
    },
    "Description": "s3-snow object & bucket API endpoint (for s3api SDK)",
    "DeviceId": "JID-beta-207429000001-23-12-28-03-51-11",
    "Status": {
      "State": "ACTIVATING"
    }
  }
]
}

```

Utilizzo di bucket S3 con storage compatibile con Amazon S3 su Snowball Edge

Con lo storage compatibile con Amazon S3 su Snowball Edge, puoi creare bucket Amazon S3 sui tuoi dispositivi Snowball Edge per archiviare e recuperare oggetti in locale per applicazioni che richiedono accesso ai dati locali, elaborazione locale dei dati e residenza dei dati. Lo storage compatibile con Amazon S3 su Snowball Edge offre una nuova classe di storage che utilizza Amazon S3 ed è progettata per archiviare i dati in modo duraturo e ridondante su più dispositivi APIs Snowball Edge. Sui bucket Snowball Edge puoi utilizzare le stesse API funzionalità che usi su Amazon S3, tra cui le policy del ciclo di vita dei bucket, la crittografia e l'etichettatura.

Puoi utilizzare lo storage compatibile con Amazon S3 su Snowball Edge utilizzando AWS Command Line Interface (AWS CLI) o in modo programmatico tramite Java SDK. AWS Con AWS CLI, puoi configurare un endpoint s3api o s3control e interagire con esso tramite comandi. Ti consigliamo di utilizzare l'endpoint s3api perché lo stesso endpoint può essere utilizzato per operazioni su bucket e oggetti.

Note

L'endpoint s3api è disponibile per la versione 8004 e successive del software Snowball Edge. Per trovare la versione del software Snowball Edge installata su un dispositivo, usa il `snowballEdge check-for-updates` comando. Per aggiornare un dispositivo Snowball Edge, consulta [Aggiornamento del software sui dispositivi Snowball Edge](#).

Utilizzo del AWS CLI

Segui queste istruzioni per utilizzare i bucket Amazon S3 sul tuo dispositivo utilizzando il. AWS CLI

Per configurare il AWS CLI

1. Crea un profilo per gli endpoint degli oggetti in `~/.aws/config`.

```
[profile your-profile]  
aws_access_key_id = your-access-id  
aws_secret_access_key = your-access-key  
region = snow  
ca_bundle = dev/apps/ca-certs/your-ca_bundle
```

2. Ottieni un certificato dal tuo dispositivo. Per informazioni, consulta la [Snowball Edge Developer Guide](#).
3. Se hai installato l'SDK in un ambiente virtuale, attivalo utilizzando il seguente comando:

```
source your-virtual-environment-name/bin/activate
```

Dopo aver configurato le operazioni, puoi utilizzare l'SDK s3api o l'SDK s3control per accedere ai bucket S3 su Snowball Edge con AWS CLI

Example di accedere al bucket S3 utilizzando l'SDK s3api

```
aws s3api list-buckets --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

Example di accedere ai bucket S3 utilizzando l'SDK s3control

```
aws s3control list-regional-buckets --account-id bucket-owner --endpoint-url  
https://s3ctrlapi-endpoint-ip --profile your-profile
```

Example di accedere agli oggetti S3 utilizzando l'SDK s3api

```
aws s3api list-objects-v2 --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

Utilizzo dell'SDK Java

Usa l'esempio seguente per lavorare con i bucket e gli oggetti Amazon S3 utilizzando l'SDK Java.

```
import software.amazon.awssdk.services.s3.S3Client;  
import software.amazon.awssdk.auth.credentials.AwsBasicCredentials;  
import software.amazon.awssdk.auth.credentials.StaticCredentialsProvider;  
import software.amazon.awssdk.http.SdkHttpClient;bg
```

```
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.regions.Region;

import java.net.URI;

AwsBasicCredentials creds = AwsBasicCredentials.create(accessKey, secretKey); // set
creds by getting Access Key and Secret Key from snowball edge
SdkHttpClient httpClient =
    ApacheHttpClient.builder().tlsTrustManagersProvider(trustManagersProvider).build(); //
    set trust managers provider with client certificate from snowball edge
String s3SnowEndpoint = "10.0.0.0"; // set s3-snow object api endpoint from describe
service

S3Client s3Client =
    S3Client.builder().httpClient(httpClient).region(Region.of("snow")).endpointOverride(new
    URI(s3SnowEndpoint)).credentialsProvider(StaticCredentialsProvider.create(creds)).build();
```

Formato Bucket ARN

Puoi utilizzare il formato Amazon Resource Name (ARN) elencato qui per identificare un bucket Amazon S3 su un dispositivo Snowball Edge:

```
arn:partition:s3:snow:account-id:device/device-id/bucket/bucket-name
```

partition Dov'è la partizione della regione in cui è stato ordinato il dispositivo Snowball Edge.
device-id è job_id se il dispositivo è un dispositivo Snowball Edge autonomo o *cluster_id* il se si dispone di un cluster Snowball Edge.

Formato di posizione del bucket

Il formato di posizione del bucket specifica il dispositivo Snowball Edge in cui verrà creato il bucket. La posizione del bucket ha il seguente formato:

```
/device-id/bucket/bucket-name
```

Per ulteriori informazioni, consulta [create-bucket](#) nel Command Reference. AWS CLI

Determinare se è possibile accedere a uno storage compatibile con Amazon S3 su un bucket Snowball Edge su Snowball Edge

L'esempio seguente utilizza il `head-bucket` comando per determinare se esiste un bucket Amazon S3 e se si dispone delle autorizzazioni per accedervi utilizzando. AWS CLI Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

```
aws s3api head-bucket --bucket sample-bucket --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

Recupero di un elenco di bucket o bucket regionali nello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge

Usa `list-regional-buckets` o `list-buckets` per elencare lo storage compatibile con Amazon S3 sui bucket Snowball Edge utilizzando il. AWS CLI

Example di recuperare un elenco di bucket o bucket regionali con AWS CLI

s3api syntax

```
aws s3api list-buckets --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

Per ulteriori informazioni sul `list-buckets` comando, vedere [list-buckets](#) nel Command Reference AWS CLI

s3control syntax

```
aws s3control list-regional-buckets --account-id 123456789012 --endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profiles
```

Per ulteriori informazioni sul `list-regional-buckets` comando, vedere [list-regional-buckets](#) nella Guida ai AWS CLI comandi.

Il seguente esempio di SDK for Java ottiene un elenco di bucket sui dispositivi Snowball Edge. Per ulteriori informazioni, consulta il riferimento [ListBuckets](#) all'API di Amazon Simple Storage Service.

```
import com.amazonaws.services.s3.model.*;
public void listBuckets() {
    ListBucketsRequest reqListBuckets = new ListBucketsRequest()
        .withAccountId(AccountId)
    ListBucketsResult respListBuckets = s3APIClient.RegionalBuckets(reqListBuckets);
    System.out.printf("ListBuckets Response: %s\n", respListBuckets.toString());
}
```

L' PowerShell esempio seguente ottiene un elenco di bucket sui dispositivi Snowball Edge.

```
Get-S3CRegionalBucketList -AccountId 012345678910 -Endpoint "https://snowball_ip" -
Region snow
```

Il seguente esempio.NET ottiene un elenco di bucket sui dispositivi Snowball Edge.

```
using Amazon.S3Control;
using Amazon.S3Control.Model;

namespace SnowTest;

internal class Program
{
    static async Task Main(string[] args)
    {
        var config = new AmazonS3ControlConfig
        {
            ServiceURL = "https://snowball_ip",
            AuthenticationRegion = "snow" // Note that this is not RegionEndpoint
        };

        var client = new AmazonS3ControlClient(config);

        var response = await client.ListRegionalBucketsAsync(new
ListRegionalBucketsRequest()
        {
            AccountId = "012345678910"
        });
    }
}
```

```
}
```

Ottenere un bucket con storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge

L'esempio seguente ottiene uno storage compatibile con Amazon S3 sul bucket Snowball Edge utilizzando il. AWS CLI Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

```
aws s3control get-bucket --account-id 123456789012 --bucket amzn-s3-demo-bucket --  
endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profile
```

Per ulteriori informazioni su questo comando, consulta [get-bucket](#) nel Command Reference. AWS CLI

Il seguente esempio di storage compatibile con Amazon S3 su Snowball Edge ottiene un bucket utilizzando l'SDK for Java. Per ulteriori informazioni, consulta [GetBucket](#) in [Amazon Simple Storage Service API Reference](#) (Guida di riferimento per l'API di Amazon Simple Storage Service).

```
import com.amazonaws.services.s3control.model.*;  
  
public void getBucket(String bucketName) {  
  
    GetBucketRequest reqGetBucket = new GetBucketRequest()  
        .withBucket(bucketName)  
        .withAccountId(AccountId);  
  
    GetBucketResult respGetBucket = s3ControlClient.getBucket(reqGetBucket);  
    System.out.printf("GetBucket Response: %s%n", respGetBucket.toString());  
}
```

Creazione di un bucket S3 nello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge

Puoi creare bucket Amazon S3 sul tuo dispositivo Snowball Edge per archiviare e recuperare oggetti all'edge per applicazioni che richiedono l'accesso locale ai dati, l'elaborazione locale dei dati e la residenza dei dati. Lo storage compatibile con Amazon S3 su Snowball Edge offre una nuova classe di storage che utilizza Amazon S3 ed è progettata per archiviare i dati in modo duraturo e ridondante su più dispositivi. SNOW Puoi utilizzare le stesse API funzionalità dei bucket Amazon S3, tra cui le politiche del ciclo di vita dei bucket, la crittografia e l'etichettatura.

L'esempio seguente crea un bucket Amazon S3 per un dispositivo Snowball Edge utilizzando il. AWS CLI Per eseguire questo comando, sostituisci i segnaposto inseriti dall'utente con le tue informazioni.

Example di creare un bucket S3

s3api syntax

```
aws s3api create-bucket --bucket your-snow-bucket --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

s3control syntax

```
aws s3control create-bucket --bucket your-snow-bucket --endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profile
```

Eliminazione di un bucket in uno storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge

Puoi utilizzare l'SDK s3api o l'SDK s3control per eliminare un bucket nello storage compatibile con Amazon S3 su Snowball Edge.

Important

- Il bucket Account AWS che crea il bucket ne è proprietario ed è l'unico che può eliminarlo.

- I bucket Snowball Edge devono essere vuoti prima di poter essere eliminati.
- Non è possibile recuperare un bucket dopo che è stato eliminato.

I seguenti esempi eliminano uno storage compatibile con Amazon S3 sul bucket Snowball Edge utilizzando il. AWS CLI Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

Example di eliminare un bucket

s3api syntax

```
aws s3api delete-bucket --bucket amzn-s3-demo-bucket --endpoint-url https://s3api-endpoint-ip --profile your-profile
```

Per ulteriori informazioni su questo comando, vedere [delete-bucket](#) nel Command Reference.
AWS CLI

s3control syntax

```
aws s3control delete-bucket --account-id 123456789012 --bucket amzn-s3-demo-bucket --endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profile
```

Per ulteriori informazioni su questo comando, vedere [delete-bucket](#) nel Command Reference.
AWS CLI

Creazione e gestione di una configurazione del ciclo di vita degli oggetti utilizzando il AWS CLI

Puoi utilizzare Amazon S3 Lifecycle per ottimizzare la capacità di storage per lo storage compatibile con Amazon S3 su Snowball Edge. È possibile creare regole del ciclo di vita per far scadere gli oggetti man mano che invecchiano o vengono sostituiti da versioni più recenti. Puoi creare, abilitare, disabilitare o eliminare una regola del ciclo di vita. Per ulteriori informazioni sul ciclo di vita di Amazon S3, consulta [Managing your storage lifecycle](#).

 Note

Chi crea Account AWS il bucket ne è il proprietario ed è l'unico in grado di creare, abilitare, disabilitare o eliminare una regola del ciclo di vita.

Per creare e gestire una configurazione del ciclo di vita per uno storage compatibile con Amazon S3 sul bucket Snowball Edge utilizzando AWS CLI(), consulta AWS Command Line Interface gli esempi seguenti.

INSERISCI una configurazione del ciclo di vita su un bucket Snowball Edge

L' AWS CLI esempio seguente inserisce una policy di configurazione del ciclo di vita in un bucket Snowball Edge. Questa policy specifica che tutti gli oggetti con il prefisso contrassegnato (*myprefix*) e i tag scadono dopo 10 giorni. Per utilizzare questo esempio, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

Innanzitutto, salva la politica di configurazione del ciclo di vita in un file JSON. In questo esempio, il file è denominato. **lifecycle-example.json**

```
{
  "Rules": [{
    "ID": "id-1",
    "Filter": {
      "And": {
        "Prefix": "myprefix",
        "Tags": [{
          "Value": "mytagvalue1",
          "Key": "mytagkey1"
        },
        {
          "Value": "mytagvalue2",
          "Key": "mytagkey2"
        }
      ]
    }
  },
  "Status": "Enabled",
  "Expiration": {
    "Days": 10
  }
}
```

```
}]  
}
```

Dopo aver salvato il file, inviate il file JSON come parte del `put-bucket-lifecycle-configuration` comando. Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

Example del **put-bucket-lifecycle** comando

s3api syntax

```
aws s3api put-bucket-lifecycle-configuration --bucket example-snow-bucket \<\  
--lifecycle-configuration file://lifecycle-example.json --endpoint-url  
https://s3api-endpoint-ip --profile your-profile
```

Per ulteriori informazioni su questo comando, vedere [put-bucket-lifecycle-configuration](#) nella Guida ai AWS CLI comandi.

s3control syntax

```
aws s3control put-bucket-lifecycle-configuration --bucket example-snow-bucket \<\  
--lifecycle-configuration file://lifecycle-example.json \<\  
--endpoint-url https://s3ctrlapi-endpoint-ip --profile your-profile
```

Per ulteriori informazioni su questo comando, vedere [put-bucket-lifecycle-configuration](#) nella Guida ai AWS CLI comandi.

Copiare un oggetto su uno storage compatibile con Amazon S3 su un bucket Snowball Edge su Snowball Edge

L'esempio seguente carica un file denominato su uno storage compatibile con Amazon S3 sul bucket Snowball Edge *sample-object.xml* per il quale disponi delle autorizzazioni di scrittura per l'utilizzo di AWS CLI. Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

```
aws s3api put-object --bucket sample-bucket --key sample-object.xml --body sample-object.xml --endpoint-url s3api-endpoint-ip --profile your-profile
```

Il seguente esempio di storage compatibile con Amazon S3 su Snowball Edge copia un oggetto in un nuovo oggetto nello stesso bucket utilizzando l'SDK for Java. Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;
add : import java.io.IOException;

public class CopyObject {
    public static void main(String[] args) {
        String bucketName = "**** Bucket name ****";
        String sourceKey = "**** Source object key ****";
        String destinationKey = "**** Destination object key ****";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .enableUseArnRegion()
                .build();

            // Copy the object into a new object in the same bucket.
            CopyObjectRequest copyObjectRequest = new CopyObjectRequest(sourceKey,
destinationKey);
            s3Client.copyObject(copyObjectRequest);
            CopyObjectRequest copyObjectRequest = CopyObjectRequest.builder()
                .sourceKey(sourceKey)
                .destinationKey(destKey)
                .build();
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
```

```

        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}

```

Elencare oggetti in un bucket nello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge

L'esempio seguente elenca gli oggetti in uno storage compatibile con Amazon S3 sul bucket Snowball Edge utilizzando il AWS CLI Il comando SDK è. `s3-snow:ListObjectsV2` Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

```
aws s3api list-objects-v2 --bucket sample-bucket --endpoint-url s3api-endpoint-ip --
profile your-profile
```

Per ulteriori informazioni su questo comando, vedere [list-objects-v2](#) nel AWS CLI Command Reference.

Il seguente esempio di storage compatibile con Amazon S3 su Snowball Edge elenca gli oggetti in un bucket utilizzando l'SDK for Java. Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

Questo esempio utilizza la [ListObjectsversione 2](#), che è l'ultima revisione del funzionamento dell'API. ListObjects Si consiglia di utilizzare questa operazione API rivista per lo sviluppo di applicazioni. Per la compatibilità con le versioni precedenti, Amazon S3 continua a supportare la versione precedente di questa operazione API.

```

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListObjectsV2Request;
import com.amazonaws.services.s3.model.ListObjectsV2Result;
import com.amazonaws.services.s3.model.S3ObjectSummary;

public class ListObjectsV2 {

```

```
public static void main(String[] args) {
    String bucketName = "*** Bucket name ***";

    try {
        // This code expects that you have AWS credentials set up per:
        // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
        AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
            .enableUseArnRegion()
            .build();

        System.out.println("Listing objects");

        // maxKeys is set to 2 to demonstrate the use of
        // ListObjectsV2Result.getNextContinuationToken()
        ListObjectsV2Request req = new
ListObjectsV2Request().withBucketName(bucketName).withMaxKeys(2);
        ListObjectsV2Result result;

        do {
            result = s3Client.listObjectsV2(req);

            for (S3ObjectSummary objectSummary : result.getObjectSummaries()) {
                System.out.printf(" - %s (size: %d)\n", objectSummary.getKey(),
objectSummary.getSize());
            }
            // If there are more than maxKeys keys in the bucket, get a
continuation token
            // and list the next objects.
            String token = result.getNextContinuationToken();
            System.out.println("Next Continuation Token: " + token);
            req.setContinuationToken(token);
        } while (result.isTruncated());
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
```

```
}
```

Recupero di un oggetto da un bucket nello storage compatibile con Amazon S3 su Snowball Edge su Snowball Edge

L'esempio seguente ottiene un oggetto denominato *sample-object.xml* da uno storage compatibile con Amazon S3 sul bucket Snowball Edge utilizzando il comando SDK AWS CLI. Il comando è `s3-snow:GetObject`. Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

```
aws s3api get-object --bucket sample-bucket --key sample-object.xml --endpoint-url s3api-endpoint-ip --profile your-profile
```

Per ulteriori informazioni su questo comando, vedere [get-object](#) nel Command Reference AWS CLI.

Il seguente esempio di storage compatibile con Amazon S3 su Snowball Edge ottiene un oggetto utilizzando l'SDK for Java. Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni. Per ulteriori informazioni, consulta [GetObject](#) in [Amazon Simple Storage Service API Reference](#) (Guida di riferimento per l'API di Amazon Simple Storage Service).

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GetObjectRequest;
import com.amazonaws.services.s3.model.ResponseHeaderOverrides;
import com.amazonaws.services.s3.model.S3Object;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;

public class GetObject {
    public static void main(String[] args) throws IOException {
        String bucketName = "**** Bucket name ****";
        String key = "**** Object key ****";
```

```

        S3Object fullObject = null, objectPortion = null, headerOverrideObject = null;
        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .enableUseArnRegion()
                .build();
            GetObjectRequest getObjectRequest = GetObjectRequest.builder()
                .bucket(bucketName)
                .key(key)
                .build();

s3Client.getObject(getObjectRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        } finally {
            // To ensure that the network connection doesn't remain open, close any
open input streams.
            if (fullObject != null) {
                fullObject.close();
            }
            if (objectPortion != null) {
                objectPortion.close();
            }
            if (headerOverrideObject != null) {
                headerOverrideObject.close();
            }
        }
    }

    private static void displayTextInputStream(InputStream input) throws IOException {
        // Read the text input stream one line at a time and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line = null;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
    }

```



```
        System.out.println();
    }
}
```

Eliminazione di oggetti nei bucket nello storage compatibile con Amazon S3 su Snowball Edge

Puoi eliminare uno o più oggetti da uno storage compatibile con Amazon S3 sul bucket Snowball Edge. L'esempio seguente elimina un oggetto denominato utilizzando. *sample-object.xml* AWS CLI Per utilizzare questo comando, sostituisci ogni segnaposto immesso dall'utente con le tue informazioni.

```
aws s3api delete-object --bucket sample-bucket --key key --endpoint-url s3api-endpoint-ip --profile your-profile
```

Per ulteriori informazioni su questo comando, vedere [delete-object](#) nel Command Reference.AWS CLI

Il seguente esempio di storage compatibile con Amazon S3 su Snowball Edge elimina un oggetto in un bucket utilizzando l'SDK for Java. Per utilizzare questo esempio, specifica il nome della chiave per l'oggetto che desideri eliminare. Per ulteriori informazioni, consulta il riferimento [DeleteObject](#) all'API di Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

public class DeleteObject {
    public static void main(String[] args) {
        String bucketName = "*** Bucket name ***";
        String keyName = "*** key name ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-credentials.html
        }
    }
}
```

```
AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
    .enableUseArnRegion()
    .build();

DeleteObjectRequest deleteObjectRequest = DeleteObjectRequest.builder()
    .bucket(bucketName)
    .key(keyName)
    .build());
s3Client.deleteObject(deleteObjectRequest);
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it, so it returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
```

Azioni API REST supportate per lo storage compatibile con Amazon S3 su Snowball Edge

Gli elenchi seguenti mostrano le operazioni API supportate dallo storage compatibile con Amazon S3 su Snowball Edge, inclusi i collegamenti alle operazioni correlate per Amazon S3 in. Regioni AWS

Operazioni API bucket supportate per l'endpoint s3api:

- [CreateBucket](#)
- [DeleteBucket](#)
- [DeleteBucketLifecycle](#)
- [GetBucketLifecycleConfiguration](#)
- [ListBuckets](#)
- [PutBucketLifecycleConfiguration](#)

Operazioni API bucket supportate per l'endpoint s3control:

- [CreateBucket](#)
- [DeleteBucket](#)
- [DeleteBucketLifecycle](#)
- [GetBucket](#)
- [GetBucketLifecycleConfiguration](#)
- [ListBuckets](#)
- [PutBucketLifecycleConfiguration](#)

Operazioni API a oggetti supportate:

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [DeleteObject](#)
- [DeleteObjects](#)
- [DeleteObjectTagging](#)
- [GetObject](#)
- [GetObjectTagging](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListMultipartUploads](#)
- [ListObjects](#)
- [ListObjectsV2](#)
- [ListParts](#)
- [PutObject](#)
- [PutObjectTagging](#)
- [UploadPart](#)
- [UploadPartCopy](#)

Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge con un cluster di dispositivi Snow

Un cluster è una raccolta di tre o più dispositivi Snowball Edge utilizzati come singola unità logica per scopi di archiviazione e calcolo locali. Un cluster offre due vantaggi principali rispetto a un dispositivo Snowball Edge autonomo per l'archiviazione e l'elaborazione locali:

- **Maggiore durabilità:** i dati S3 archiviati in un cluster di dispositivi Snowball Edge godono di una maggiore durabilità dei dati rispetto a un singolo dispositivo. Inoltre, i dati sul cluster rimangono sicuri e utilizzabili, nonostante le possibili interruzioni hardware che interessano il cluster. I cluster sono in grado di sopportare la perdita di un dispositivo in cluster da 3 a 4 dispositivi e fino a due dispositivi in cluster da 5 a 16 dispositivi prima che i dati siano in pericolo. È possibile sostituire i nodi non integri per mantenere la durabilità e la sicurezza dei dati archiviati nel cluster.
- **Maggiore storage:** con i dispositivi ottimizzati per lo storage Snowball Edge, puoi creare un singolo cluster a 16 nodi con un massimo di 2,6 PB di capacità di storage utilizzabile compatibile con S3. Con i dispositivi ottimizzati per l'elaborazione Snowball Edge, puoi creare un singolo cluster a 16 nodi con un massimo di 501 TB di capacità di storage utilizzabile compatibile con S3.

Un cluster di dispositivi Snowball Edge è composto da nodi senza leader. Qualsiasi nodo può scrivere e leggere dati dall'intero cluster e tutti i nodi sono in grado di eseguire la behind-the-scenes gestione del cluster.

Tieni a mente le seguenti considerazioni quando pianifichi di utilizzare un cluster di dispositivi Snowball Edge:

- Si consiglia di fornire una fonte di alimentazione ridondante per tutti i dispositivi del cluster per ridurre i potenziali problemi di prestazioni e stabilità del cluster.
- Come per i processi di elaborazione e archiviazione locali autonomi, i dati archiviati in un cluster non possono essere importati in Amazon S3 senza ordinare dispositivi aggiuntivi come parte di processi di importazione separati. Se ordini dispositivi aggiuntivi come processi di importazione, puoi trasferire i dati dal cluster ai dispositivi di importazione.
- Per trasferire dati in un cluster da Amazon S3, utilizza l'API Amazon S3 per creare bucket Amazon S3 sul cluster per archiviare e recuperare oggetti da S3. Inoltre, puoi utilizzare AWS DataSync per trasferire oggetti tra i servizi di storage e AWS lo storage compatibile con Amazon S3 su Snowball Edge su un dispositivo Snowball Edge. Per ulteriori informazioni, consulta [Configurazione dei trasferimenti con storage compatibile con S3 su Snowball Edge](#).

- Puoi creare un lavoro per ordinare un cluster di dispositivi da, da Console di gestione della famiglia di servizi AWS Snow AWS CLI, o da uno dei. AWS SDKs Per ulteriori informazioni, consulta [Guida introduttiva a Snowball Edge](#).
- Ogni dispositivo del cluster ha un ID di nodo. Un ID di nodo è un identificatore univoco per ogni dispositivo del cluster, come un ID di lavoro per un dispositivo autonomo. Puoi ottenere il nodo IDs dal Console di gestione della famiglia di servizi AWS Snow, dal AWS CLI AWS SDKs, e dal client Snowball Edge. Il client Snowball Edge comanda `describe-device` e `describe-cluster` restituisce il nodo IDs con altre informazioni sui dispositivi o sul cluster.
- La durata di un cluster è limitata dal certificato di sicurezza concesso ai dispositivi del cluster quando viene effettuato il provisioning del cluster. Per impostazione predefinita, i dispositivi Snowball Edge possono essere utilizzati per un massimo di 360 giorni prima di dover essere restituiti. Al termine di tale periodo, i dispositivi smettono di rispondere alle read/write richieste. Se devi conservare uno o più dispositivi per più di 360 giorni, contatta Supporto AWS.
- Quando AWS riceve un dispositivo restituito che faceva parte di un cluster, eseguiamo una cancellazione completa del dispositivo. Questa cancellazione rispetta gli standard 800-88 della National Institute of Standards and Technology (NIST).

Storage compatibile con Amazon S3 su cluster Snowball Edge, tolleranza agli errori e capacità di storage

Dimensione del cluster	Tolleranza ai guasti	Capacità di storage dei dispositivi Snowball Edge Compute Optimized (elaborazione ottimizzata con AMD EPYC NVMe Gen2 e) (in TB)	Capacità di storage dei dispositivi da 210 TB ottimizzati per lo storage Snowball Edge (in TB)
3	Perdita di un massimo di 1 nodo	38	438
4	Perdita di un massimo di 1 nodo	57	657

Dimensione del cluster	Tolleranza ai guasti	Capacità di storage dei dispositivi Snowball Edge Compute Optimized (elaborazione ottimizzata con AMD EPYC NVMe Gen2 e) (in TB)	Capacità di storage dei dispositivi da 210 TB ottimizzati per lo storage Snowball Edge (in TB)
5	Perdita di un massimo di 2 nodi	57	657
6	Perdita di un massimo di 2 nodi	76	904
7	Perdita di un massimo di 2 nodi	95	1096
8	Perdita di un massimo di 2 nodi	114	1315
9	Perdita di un massimo di 2 nodi	133	1534
10	Perdita di un massimo di 2 nodi	152	1754
11	Perdita di un massimo di 2 nodi	165	1970
12	Perdita di un massimo di 2 nodi	171	1973
13	Perdita di un massimo di 2 nodi	190	2192
14	Perdita di un massimo di 2 nodi	209	2411

Dimensione del cluster	Tolleranza ai guasti	Capacità di storage dei dispositivi Snowball Edge Compute Optimized (elaborazione ottimizzata con AMD EPYC NVMe Gen2 e) (in TB)	Capacità di storage dei dispositivi da 210 TB ottimizzati per lo storage Snowball Edge (in TB)
15	Perdita di un massimo di 2 nodi	225	2625
16	Perdita di un massimo di 2 nodi	228	2631

Dopo aver sbloccato un cluster, sei pronto per archiviare e accedere ai dati su quel cluster. Puoi utilizzare l'endpoint compatibile con Amazon S3 per leggere e scrivere dati su un cluster.

Per leggere o scrivere dati su un cluster, devi avere un read/write quorum che non superi il numero consentito di nodi non disponibili nel cluster di dispositivi.

Quorum del cluster Snowball Edge

Un quorum rappresenta il numero minimo di dispositivi Snowball Edge in un cluster che devono comunicare tra loro per mantenere un quorum. read/write

Quando tutti i dispositivi di un cluster sono integri, si dispone di un quorum di lettura/scrittura per il cluster. Se uno o due di questi dispositivi vanno offline, si riduce la capacità operativa del cluster. Tuttavia, puoi ancora eseguire operazioni di lettura e scrittura nel cluster. Con tutti i dispositivi operativi tranne uno o due, il cluster ha ancora un read/write quorum. Il numero di nodi che possono andare offline prima che la capacità operativa del cluster venga compromessa è indicato in. [this table](#)

Quorum può andare perso se un cluster perde più del numero di dispositivi indicato in. [this table](#)

Quando si perde un quorum, il cluster è offline e i dati in esso contenuti non sono disponibili.

A seconda della gravità dell'evento, potresti riuscire a risolvere questo problema o perdere definitivamente i dati. Se si tratta di un evento di alimentazione esterno temporaneo ed è possibile riaccendere i dispositivi Snowball Edge e sbloccare tutti i nodi del cluster, i dati sono nuovamente disponibili.

 Important

Se non esiste un quorum minimo di nodi integri, contatta. Supporto AWS

È possibile utilizzare il `describe-cluster` comando per visualizzare lo stato di blocco e la raggiungibilità della rete di ciascun nodo. Garantire che i dispositivi del cluster siano integri e connessi è una responsabilità amministrativa che ti assumi quando utilizzi lo storage del cluster. Per ulteriori informazioni, consulta [Rilevare lo stato del dispositivo](#).

Se ritieni che uno o più nodi non siano integri, puoi sostituire i nodi del cluster per mantenere il quorum e l'integrità e la stabilità dei dati. Per ulteriori informazioni, consulta [Sostituzione di un nodo in un cluster](#).

Riconnessione di un nodo del cluster non disponibile

Un nodo o un dispositivo all'interno di un cluster può diventare temporaneamente non disponibile a causa di un problema come l'interruzione dell'alimentazione o della rete senza danneggiare i dati sul nodo. Quando si verifica, ciò questo influenza lo stato del cluster. La raggiungibilità della rete e lo stato di blocco di un nodo vengono segnalati nel client Snowball Edge utilizzando `snowballEdge describe-cluster` il comando.

Ti consigliamo di posizionare fisicamente il cluster in modo da accedere alla parte anteriore, posteriore e superiore di tutti i nodi. In questo modo, puoi accedere ai cavi di alimentazione e di rete sul retro, alle etichette di spedizione sulla parte superiore per il nodo IDs e agli schermi LCD sulla parte anteriore dei dispositivi per gli indirizzi IP e altre informazioni amministrative.

Quando rilevi che un nodo non è disponibile, ti consigliamo di provare una delle seguenti procedure, a seconda dello scenario che ha causato la mancata disponibilità del nodo.

Per ristabilire la connessione a un nodo non disponibile

1. Assicurati che il nodo sia acceso.
2. Assicurati che il nodo sia connesso alla stessa rete interna a cui è connesso il resto del cluster.
3. Se devi accendere il nodo, attendi fino a 20 minuti che finisca.
4. Esegui il `snowballEdge unlock-cluster` comando o il `snowballEdge associate-device` comando. Per un esempio, consulta [Sblocco dei dispositivi Snowball Edge](#).

Per ricollegare un nodo non disponibile che ha perso la connettività di rete ma non l'alimentazione

1. Verificare che il nodo sia connesso alla stessa rete interna su cui si trova il resto del cluster.
2. Eseguire il comando `snowballEdge describe-device` per vedere quando il nodo precedentemente non disponibile viene nuovamente aggiunto al cluster. Per un esempio, vedi [Ottenere lo stato del dispositivo](#).

Dopo aver eseguito le procedure precedenti, i nodi dovrebbero funzionare normalmente. È inoltre necessario avere un read/write quorum. In caso contrario, uno o più nodi potrebbero presentare un problema più grave e potrebbe essere necessario rimuoverli dal cluster.

Sostituzione di un nodo in un cluster

Per sostituire un nodo, devi prima ordinarne uno sostitutivo. È possibile ordinare un nodo sostitutivo dalla console, da AWS CLI, o da uno dei AWS SDKs. Se stai ordinando un nodo sostitutivo dalla console, puoi ordinare ricambi per qualsiasi processo che non è stato annullato o completato. Quindi, dissociate il nodo non integro dal cluster, connettete il nodo sostitutivo alla rete e sbloccate il cluster, incluso il nodo sostitutivo, associate il nodo sostitutivo al cluster e riavviate lo storage compatibile con Amazon S3 sul servizio Snowball Edge.

Per ordinare un nodo sostitutivo dalla console

1. Accedi alla [Console di gestione della famiglia di servizi AWS Snow](#).
2. Individuare e scegliere un processo per un nodo che appartiene al cluster creato dal pannello di controllo del processo.
3. Per Actions (Operazioni), selezionare Replace node (Sostituisci nodo).

In questo modo viene aperta la fase finale della creazione guidata processo, in cui tutte le impostazioni sono identiche alla modalità di creazione originale del cluster.

4. Scegli Crea processo.

Lo Snowball Edge sostitutivo è ora in arrivo. Utilizzare la procedura seguente per rimuovere il nodo non integro dal cluster.

Per rimuovere un nodo da un cluster

1. Spegnerne il nodo da rimuovere. Per ulteriori informazioni, consulta [Powering off the Snowball Edge](#).

2. Usa il `describe-cluster` comando per assicurarti che il nodo non integro sia irraggiungibile. Ciò è indicato dal valore di `UNREACHABLE` per il `State` nome dell'oggetto. `NetworkReachability`

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://ip-address-of-device-in-cluster
```

Example dell'`describe-cluster` output

```
{
  "ClusterId": "CID12345678-1234-1234-1234-123456789012",
  "Devices": [
    {
      "DeviceId": "JID12345678-1234-1234-1234-123456789012",
      "UnlockStatus": {
        "State": "UNLOCKED"
      },
      "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.0"
      },
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
      },
      "NetworkReachability": {
        "State": "REACHABLE"
      },
      "Tags": []
    },
    {
      "DeviceId": "JID12345678-1234-1234-1234-123456789013",
      "UnlockStatus": {
        "State": "UNLOCKED"
      },
      "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.1"
      },
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
```

```

        "State": "ASSOCIATED"
      },
      "NetworkReachability": {
        "State": "REACHABLE"
      },
      "Tags": []
    },
    {
      "DeviceId": "JID12345678-1234-1234-1234-123456789014",
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
      },
      "NetworkReachability": {
        "State": "UNREACHABLE"
      }
    }
  ]
}

```

3. Usa il `describe-service` comando per assicurarti che lo stato del `s3-snow` servizio sia `DEGRADED`.

```

snowballEdge describe-service --service-id s3-snow --device-ip-addresses snow-device-1-address snow-device-2-address --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-address

```

Example dell'output del **describe-service** comando

```

{
  "ServiceId": "s3-snow",
  "Autostart": true,
  "Status": {
    "State": "DEGRADED"
  },
  "ServiceCapacities": [
    {
      "Name": "S3 Storage",
      "Unit": "Byte",

```

```

        "Used": 38768180432,
        "Available": 82961231819568
    }
],
"Endpoints": [
    {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.10",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description" : "s3-snow bucket API endpoint (for s3control SDK)",
        "DeviceId": "JID-beta-207012320001-24-02-05-17-17-26",
        "Status": {
            "State": "ACTIVE"
        }
    },
    {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.11",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "Description" : "s3-snow object & bucket API endpoint
(for s3api SDK)",
        "DeviceId": "JID-beta-207012320001-24-02-05-17-17-26",
        "Status": {
            "State": "ACTIVE"
        }
    },
    {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.12",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device:::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "Description" : "s3-snow bucket API endpoint (for
s3control SDK)",
    }
]

```

```

        "DeviceId": "JID-beta-207012240003-24-02-05-17-17-27",
        "Status": {
            "State": "ACTIVE"
        }
    },
    {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.13",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "Description" : "s3-snow object & bucket API endpoint
(for s3api SDK)",
        "DeviceId": "JID-beta-207012320001-24-02-05-17-17-27",
        "Status": {
            "State": "ACTIVE"
        }
    }
]
}

```

4. Usa il `disassociate-device` comando per dissociare e rimuovere il nodo non integro dal cluster.

```

snowballEdge disassociate-device --device-id device-id --manifest-file path/to/
manifest/file.bin --unlock-code unlock-code --endpoint https://ip-address-of-
unhealthy-device

```

Example output del comando **disassociate-device**

Disassociating your Snowball Edge device from the cluster. Your Snowball Edge device will be disassociated from the cluster when it is in the "DISASSOCIATED" state. You can use the `describe-cluster` command to determine the state of your cluster.

5. Usa nuovamente il `describe-cluster` comando per assicurarti che il nodo non integro venga dissociato dal cluster.

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https:ip-address-of-healthy-device
```

Example del **describe-cluster** comando che mostra il nodo è dissociato

```
{
  "ClusterId": "CID12345678-1234-1234-1234-123456789012",
  "Devices": [
    {
      "DeviceId": "JID12345678-1234-1234-1234-123456789012",
      "UnlockStatus": {
        "State": "UNLOCKED"
      },
      "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.0"
      },
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
      },
      "NetworkReachability": {
        "State": "REACHABLE"
      },
      "Tags": []
    },
    {
      "DeviceId": "JID12345678-1234-1234-1234-123456789013",
      "UnlockStatus": {
        "State": "UNLOCKED"
      },
      "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.1"
      },
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
      }
    }
  ]
}
```

```

    },
    "NetworkReachability": {
        "State": "REACHABLE"
    },
    "Tags": []
},
{
    "DeviceId": "JID12345678-1234-1234-1234-123456789014",
    "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "DISASSOCIATED"
    }
}
]
}

```

6. Spegnere e riportare il dispositivo non integro a AWS Per ulteriori informazioni, vedere [Spegnimento del dispositivo Snowball Edge e Restituzione del dispositivo Snowball Edge](#).

Quando arriva il dispositivo sostitutivo, utilizza la procedura seguente per aggiungerlo al cluster.

Per aggiungere un dispositivo sostitutivo

1. Posiziona il dispositivo sostitutivo per il cluster in modo da avere accesso alla parte anteriore, posteriore e superiore di tutti i dispositivi.
2. Accendi il nodo e assicurati che sia connesso alla stessa rete interna del resto del cluster. Per ulteriori informazioni, consulta [Connessione alla rete locale](#).
3. Usa il `unlock-cluster` comando e includi l'indirizzo IP del nuovo nodo.

```

snowballEdge unlock-cluster --manifest-file path/to/manifest/file.bin --unlock-
code unlock-code --endpoint https://ip-address-of-cluster-device --device-ip-
addresses node-1-ip-address node-2-ip-address new-node-ip-address

```

Lo stato del nuovo nodo rimarrà `DEGRADED` invariato finché non lo assocerai al cluster nel passaggio successivo.

4. Usa il `associate-device` comando per associare il nodo sostitutivo al cluster.

```
snowballEdge associate-device --device-ip-address new-node-ip-address
```

Example dell'output del **associate-device** comando

Associating your Snowball Edge device with the cluster. Your Snowball Edge device will be associated with the cluster when it is in the ASSOCIATED state. You can use the describe-device command to determine the state of your devices.

5. Usa il describe-cluster comando per assicurarti che il nuovo nodo sia associato al cluster.

```
snowballEdge describe-cluster --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://node-ip-address
```

Example dell'output del **describe-cluster** comando

```
{
  "ClusterId": "CID12345678-1234-1234-1234-123456789012",
  "Devices": [
    {
      "DeviceId": "JID12345678-1234-1234-1234-123456789012",
      "UnlockStatus": {
        "State": "UNLOCKED"
      },
      "ActiveNetworkInterface": {
        "IpAddress": "10.0.0.0"
      },
      "ClusterAssociation": {
        "ClusterId": "CID12345678-1234-1234-1234-123456789012",
        "State": "ASSOCIATED"
      },
      "NetworkReachability": {
        "State": "REACHABLE"
      },
    },
  ],
}
```



```

        "Tags": []
    },
    {
        "DeviceId": "JID-CID12345678-1234-1234-1234-123456789013",
        "UnlockStatus": {
            "State": "UNLOCKED"
        },
        "ActiveNetworkInterface": {
            "IpAddress": "10.0.0.1"
        },
        "ClusterAssociation": {
            "ClusterId": "CID12345678-1234-1234-1234-123456789012",
            "State": "ASSOCIATED"
        },
        "NetworkReachability": {
            "State": "REACHABLE"
        },
        "Tags": []
    },
    {
        "DeviceId": "JID-CID12345678-1234-1234-1234-123456789015",
        "UnlockStatus": {
            "State": "UNLOCKED"
        },
        "ActiveNetworkInterface": {
            "IpAddress": "10.0.0.2"
        },
        "ClusterAssociation": {
            "ClusterId": "CID12345678-1234-1234-1234-123456789012",
            "State": "ASSOCIATED"
        },
        "NetworkReachability": {
            "State": "REACHABLE"
        },
        "Tags": []
    }
}
]
}

```

6. Sul nuovo nodo, crea due interfacce di rete virtuali (VNI). Per ulteriori informazioni, consulta [Avvio dello storage compatibile con Amazon S3 sul servizio Snowball Edge](#)

7. Utilizzate il `stop-service` comando per interrompere il servizio s3-snow.

```
snowballEdge stop-service --service-id s3-snow --device-ip-addresses cluster-device-1-ip-address cluster-device-2-ip-address cluster-device-3-ip-address --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-address
```

Example dell'output del comando **stop-service**

Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS service using the `describe-service` command.

8. Usa il `start-service` comando per avviare il servizio s3-snow dopo aver aggiunto il nuovo nodo al cluster.

```
snowballEdge start-service --service-id s3-snow --device-ip-addresses cluster-device-1-ip-address cluster-device-2-ip-address cluster-device-3-ip-address --virtual-network-interface-arns "device-1-vni-ip-address-a device-1-vni-ip-address-b device-2-vni-ip-address-a device-2-vni-ip-address-b device-3-vni-ip-address-a device-3-vni-ip-address-b" --manifest-file path/to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-address
```

Example dell'output del comando **start-service**

Starting the AWS service on your Snowball Edge. You can determine the status of the AWS service using the `describe-service` command.

9. Usa il `describe-service` comando per assicurarti che il servizio s3-snow sia avviato.

```
snowballEdge describe-service --service-id s3-snow --device-ip-addresses snow-  
device-1-address snow-device-2-address snow-device-3-address --manifest-file path/  
to/manifest/file.bin --unlock-code unlock-code --endpoint https://snow-device-ip-  
address
```

Example dell'output del comando **describe-service**

```
{
  "ServiceId": "s3-snow",
  "Autostart": true,
  "Status": {
    "State": "ACTIVE"
  },
  "ServiceCapacities": [{
    "Name": "S3 Storage",
    "Unit": "Byte",
    "Used": 38768180432,
    "Available": 82961231819568
  }],
  "Endpoints": [{
    "Protocol": "https",
    "Port": 443,
    "Host": "10.0.0.10",
    "CertificateAssociation": {
      "CertificateArn": "arn:aws:snowball-  
device::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
    },
    "Description": "s3-snow bucket API endpoint (for s3control SDK)",
    "DeviceId": "JID12345678-1234-1234-1234-123456789012",
    "Status": {
      "State": "ACTIVE"
    }
  }, {
    "Protocol": "https",
    "Port": 443,
    "Host": "10.0.0.11",
    "CertificateAssociation": {
      "CertificateArn": "arn:aws:snowball-  
device::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
    },
    "Description": "s3-snow object & bucket API endpoint (for s3api SDK)",
```

```

        "DeviceId": "JID12345678-1234-1234-1234-123456789013",
        "Status": {
            "State": "ACTIVE"
        }
    }, {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.12",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "s3-snow bucket API endpoint (for s3control SDK)",
        "DeviceId": "JID12345678-1234-1234-1234-123456789015",
        "Status": {
            "State": "ACTIVE"
        }
    }, {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.13",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "s3-snow object & bucket API endpoint (for s3api SDK)",
        "DeviceId": "JID-beta-207012320001-24-02-05-17-17-27",
        "Status": {
            "State": "ACTIVE"
        }
    }, {
        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.14",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "s3-snow bucket API endpoint (for s3control SDK)",
        "DeviceId": "JID-beta-207012240003-24-02-05-17-17-28",
        "Status": {
            "State": "ACTIVE"
        }
    }, {

```

```

        "Protocol": "https",
        "Port": 443,
        "Host": "10.0.0.15",
        "CertificateAssociation": {
            "CertificateArn": "arn:aws:snowball-
device::certificate/7Rg2lP9tQaHnW4sC6xUzF1vGyD3jB5kN8MwEiYpT"
        },
        "Description": "s3-snow object & bucket API endpoint (for s3api SDK),
        "DeviceId": "JID-beta-207012320001-24-02-05-17-17-28",
        "Status": {
            "State": "ACTIVE"
        }
    }
}
}]
}

```

Configurazione dello storage compatibile con Amazon S3 sulle notifiche degli eventi Snowball Edge

Lo storage compatibile con Amazon S3 su Snowball Edge supporta le notifiche di eventi di Amazon S3 per le chiamate API a oggetti basate sul protocollo Message Queuing Telemetry Transport (MQTT).

Puoi utilizzare lo storage compatibile con Amazon S3 su Snowball Edge per ricevere notifiche quando si verificano determinati eventi nel tuo bucket S3. Per abilitare le notifiche, aggiungi una configurazione di notifica che identifichi gli eventi che desideri vengano pubblicati dal servizio.

Lo storage compatibile con Amazon S3 su Snowball Edge supporta i seguenti tipi di notifica:

- Eventi di creazione nuovo oggetto
- Eventi di rimozione di oggetti
- Eventi di assegnazione di tag agli oggetti

Configurazione delle notifiche degli eventi di Amazon S3

1. Prima di iniziare, è necessario disporre di un'infrastruttura MQTT nella rete.

2. Nel client Snowball Edge, esegui il `snowballEdge configure` comando per configurare il dispositivo Snowball Edge.

Quando richiesto, inserisci le seguenti informazioni:

- Il percorso del file manifesto.
 - Il codice di sblocco del dispositivo.
 - L'endpoint del dispositivo (ad esempio, *https://10.0.0.1*).
3. Esegui il `put-notification-configuration` comando seguente per inviare notifiche a un broker esterno.

```
snowballEdge put-notification-configuration --broker-endpoint ssl://mqtt-broker-ip-address:8883 --enabled true --service-id s3-snow --ca-certificate file:path-to-mqtt-broker-ca-cert
```

4. Esegui il `get-notification-configuration` comando seguente per verificare che tutto sia configurato correttamente:

```
snowballEdge get-notification-configuration --service-id s3-snow
```

Ciò restituisce l'endpoint del broker e il campo abilitato.

Dopo aver configurato l'intero cluster per l'invio di notifiche al broker MQTT in rete, ogni chiamata all'API dell'oggetto genererà una notifica di evento.

Note

Devi iscriverti all'argomento `s3SnowEvents/Device ID` (o *Cluster Id* se si tratta di un cluster) `/bucketName`. Puoi anche usare caratteri jolly, ad esempio il nome dell'argomento può essere o. *# s3SnowEvents/#*

Di seguito è riportato un esempio di storage compatibile con Amazon S3 nel registro eventi Snowball Edge:

```
{  
  "eventDetails": {
```

```

    "additionalEventData": {
      "AuthenticationMethod": "AuthHeader",
      "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "SignatureVersion": "SigV4",
      "bytesTransferredIn": 1205,
      "bytesTransferredOut": 0,
      "x-amz-id-2": "uLdTfvdGTKlX6TBgCZtDd9Beef8wzUurA+Wpht7rKtfdaNsnxeLILg=="
    },
    "eventName": "PutObject",
    "eventTime": "2023-01-30T14:13:24.772Z",
    "requestAuthLatencyMillis": 40,
    "requestBandwidthKBs": 35,
    "requestID": "140CD93455CB62B4",
    "requestLatencyMillis": 77,
    "requestLockLatencyNanos": 1169953,
    "requestParameters": {
      "Content-Length": "1205",
      "Content-MD5": "GZdTU0hYHvHgQgmaw2gl4w==",
      "Host": "10.0.2.251",
      "bucketName": "bucket",
      "key": "file-key"
    },
    "requestTTFBLatencyMillis": 77,
    "responseElements": {
      "ETag": "\"19975350e8581ef1e042099ac36825e3\"",
      "Server": "AmazonS3",
      "x-amz-id-2": "uLdTfvdGTKlX6TBgCZtDd9Beef8wzUurA+Wpht7rKtfdaNsnxeLILg==",
      "x-amz-request-id": "140CD93455CB62B4"
    },
    "responseStatusCode": 200,
    "sourceIPAddress": "172.31.37.21",
    "userAgent": "aws-cli/1.27.23 Python/3.7.16 Linux/4.14.301-224.520.amzn2.x86_64
botocore/1.29.23",
    "userIdentity": {
      "identityType": "IAMUser",
      "principalId": "531520547609",
      "arn": "arn:aws:iam::531520547609:root",
      "userName": "root"
    }
  }
}

```

Per ulteriori informazioni sulle notifiche degli eventi di Amazon S3, consulta [Amazon S3 Event Notifications](#).

Configurazione delle notifiche SMTP locali su Snowball Edge

Puoi configurare notifiche locali per i dispositivi Snowball Edge con Simple Mail Transfer Protocol (SMTP). Le notifiche locali inviano e-mail ai server configurati quando lo stato del servizio (Attivo, Degradato, Inattivo) cambia o se si superano le soglie di utilizzo della capacità dell'80%, 90% o 100%.

Prima di iniziare, verifica che:

- Hai accesso al client Snowball Edge più recente.
- Il dispositivo è sbloccato e pronto all'uso.
- Il dispositivo può connettersi a Internet (se utilizza Amazon Simple Email Service o un server SMTP esterno) o a un server SMTP locale.

Configurazione di Snowball Edge per le notifiche locali

Configura Snowball Edge per inviare notifiche e-mail.

Per configurare il dispositivo per le notifiche SMTP

1. Esegui il comando seguente per aggiungere una configurazione SMTP al tuo dispositivo:

```
# If you don't specify a port, port 587 is the default.
SMTP_ENDPOINT=your-local-smtp-server-endpoint:port

# For multiple email recipients, separate with commas
RECIPIENTS_LIST=your-email-address

snowballEdge put-notification-configuration \
  --service-id local-monitoring \
  --enabled true \
  --type smtp \
  --broker-endpoint "$SMTP_ENDPOINT" \
  --sender example-sender@domain.com \
  --recipients "$RECIPIENTS_LIST"
```

Se hai successo, riceverai un'email di prova da *example-sender@domain.com*.

2. Verifica la configurazione eseguendo il `get-notification-configuration` comando seguente:

```
snowballEdge get-notification-configuration \  
--service-id local-monitoring
```

La risposta non include una password o un certificato, anche se li fornisci tu.

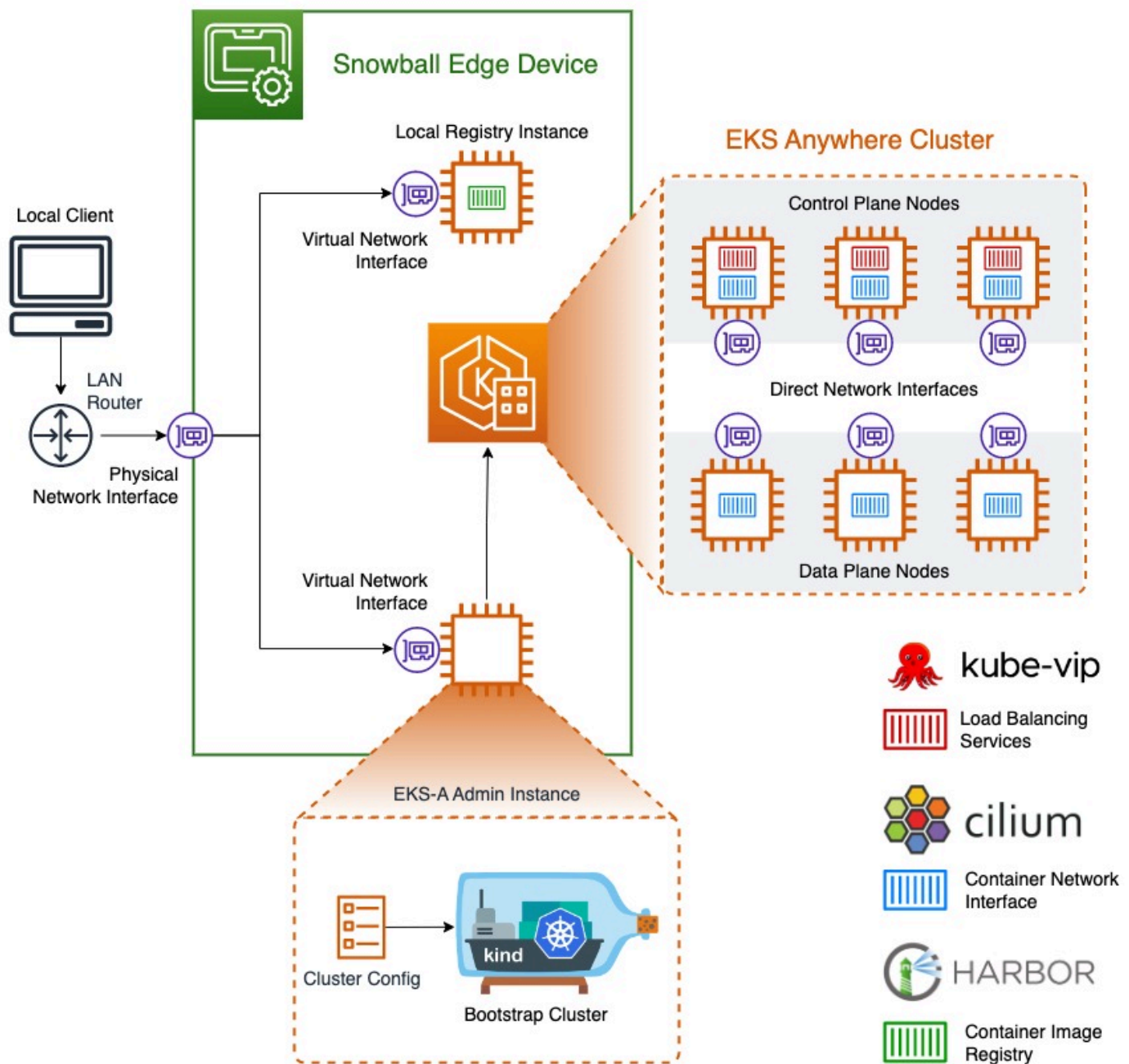
Utilizzo di Amazon EKS Anywhere sulla AWS neve

Amazon EKS Anywhere on AWS Snow ti aiuta a creare e gestire cluster Kubernetes su Snowball Edge. Kubernetes è un software open source utilizzato per automatizzare l'implementazione, la scalabilità e la gestione di applicazioni containerizzate. Puoi usare Amazon EKS Anywhere su un dispositivo Snowball Edge con o senza una connessione di rete esterna. Per utilizzare Amazon EKS Anywhere su un dispositivo senza una connessione di rete esterna, fornisci un registro container da eseguire sul dispositivo Snowball Edge. Per informazioni generali su Amazon EKS Anywhere, consulta la [documentazione di Amazon EKS Anywhere](#).

L'uso di Amazon EKS Anywhere on AWS Snow offre le seguenti funzionalità:

- Effettua il provisioning di un cluster Kubernetes (K8s) con Amazon EKS Anywhere CLI (eksctl anywhere) su dispositivi ottimizzati per il calcolo Snowball Edge. Puoi effettuare il provisioning di Amazon EKS Anywhere su un singolo dispositivo Snowball Edge o su tre o più dispositivi per un'elevata disponibilità.
- Support per Cilium Container Network Interface (CNI).
- Support per Ubuntu 20.04 come sistema operativo del nodo.

Questo diagramma illustra un cluster Amazon EKS Anywhere distribuito su un dispositivo Snowball Edge.



Ti consigliamo di creare il tuo cluster Kubernetes con l'ultima versione di Kubernetes disponibile supportata da Amazon EKS Anywhere. Per ulteriori informazioni, consulta [Amazon EKS-Anywhere Versioning](#). Se la tua applicazione richiede una versione specifica di Kubernetes, utilizza qualsiasi versione di Kubernetes offerta con supporto standard o esteso da Amazon EKS. Considera le date di rilascio e supporto delle versioni di Kubernetes quando pianifichi il ciclo di vita della tua implementazione. Questo ti aiuterà a evitare la potenziale perdita del supporto per la versione di

Kubernetes che intendi utilizzare. Per ulteriori informazioni, consulta il calendario delle release di [Amazon EKS Kubernetes](#).

Per ulteriori informazioni su Amazon EKS Anywhere on AWS Snow, consulta la [documentazione di Amazon EKS Anywhere](#).

Argomenti

- [Azioni da completare prima di ordinare un dispositivo Snowball Edge per Amazon EKS Anywhere on Snow AWS](#)
- [Ordinazione di un dispositivo Snowball Edge da utilizzare con Amazon EKS Anywhere on Snow AWS](#)
- [Configurazione ed esecuzione di Amazon EKS Anywhere su dispositivi Snowball Edge](#)
- [Configurazione di Amazon EKS Anywhere on AWS Snow per il funzionamento disconnesso](#)
- [Creazione e manutenzione di cluster su dispositivi Snowball Edge](#)

Azioni da completare prima di ordinare un dispositivo Snowball Edge per Amazon EKS Anywhere on Snow AWS

Al momento, Amazon EKS Anywhere è compatibile con i dispositivi ottimizzati per il calcolo Snowball Edge. Prima di ordinare un dispositivo Snowball Edge, ci sono alcune cose da fare per prepararsi.

- Crea e fornisci un'immagine del sistema operativo da utilizzare per creare macchine virtuali sul dispositivo.
- La rete deve avere un indirizzo IP statico disponibile per l'endpoint del piano di controllo K8s e consentire l'Address Resolution Protocol (ARP).
- Il dispositivo Snowball Edge deve avere porte specifiche aperte. Per ulteriori informazioni sulle porte, consulta [Porte e protocolli](#) nella documentazione di Amazon EKS Anywhere.

Argomenti

- [Creare un'AMI Ubuntu EKS Distro per Snowball Edge](#)
- [Crea un'AMI Harbor per Snowball Edge](#)

Creare un'AMI Ubuntu EKS Distro per Snowball Edge

Per creare l'AMI Ubuntu EKS Distro, consulta [Build Snow node images](#).

Il nome dell'AMI generato seguirà lo schema `capa-ami-ubuntu-20.04-version-timestamp`. Ad esempio, `capa-ami-ubuntu-20.04-v1.24-1672424524`.

Crea un'AMI Harbor per Snowball Edge

Configura un'AMI di registro privato Harbor da includere nel dispositivo Snowball Edge in modo da poter utilizzare Amazon EKS Anywhere sul dispositivo senza una connessione di rete esterna. Se non utilizzerai Amazon EKS Anywhere mentre il dispositivo Snowball Edge è disconnesso dalla rete esterna o se disponi di un registro Kubernetes privato in un'AMI da utilizzare sul dispositivo, puoi saltare questa sezione.

Per creare l'AMI del registro locale Harbor, consulta [Creare un AMI Harbor](#).

Ordinazione di un dispositivo Snowball Edge da utilizzare con Amazon EKS Anywhere on Snow AWS

Per ordinare uno Snowball Edge ottimizzato per l'elaborazione, consulta questa guida e tieni [Creazione di un lavoro per ordinare un dispositivo Snowball Edge](#) a mente questi elementi durante il processo di ordinazione:

- Nel passaggio 1, scegli il tipo di lavoro solo per elaborazione e archiviazione locali.
- Nel passaggio 2, scegli il tipo di dispositivo Snowball Edge Compute Optimized.
- Nel passaggio 3, scegli Amazon EKS Anywhere on AWS Snow, quindi scegli la versione di Kubernetes di cui hai bisogno.

Note

Per fornire il software più recente, possiamo configurare il dispositivo con una versione di ESK Anywhere più recente di quella attualmente disponibile. Per ulteriori informazioni, consulta il [controllo delle versioni](#) nella Amazon EKS User Guide.

Ti consigliamo di creare il tuo cluster Kubernetes con l'ultima versione di Kubernetes disponibile supportata da Amazon EKS Anywhere. Per ulteriori informazioni, consulta [Amazon EKS-Anywhere Versioning](#). Se la tua applicazione richiede una versione specifica

di Kubernetes, utilizza qualsiasi versione di Kubernetes offerta con supporto standard o esteso da Amazon EKS. Considera le date di rilascio e supporto delle versioni di Kubernetes quando pianifichi il ciclo di vita della tua implementazione. Questo ti aiuterà a evitare la potenziale perdita del supporto per la versione di Kubernetes che intendi utilizzare. Per ulteriori informazioni, consulta il calendario delle release di [Amazon EKS Kubernetes](#).

- Scegli AMIs di includere nel tuo dispositivo, tra cui l'AMI EKS Distro (vedi [Creare un'AMI Ubuntu EKS Distro per Snowball Edge](#)) e, facoltativamente, l'AMI Harbor che hai creato (vedi [Crea un'AMI Harbor per Snowball Edge](#)).
- Se hai bisogno di più dispositivi Snowball Edge per l'alta disponibilità, scegli il numero di dispositivi di cui hai bisogno da High Availability.

Dopo aver ricevuto il dispositivo o i dispositivi Snowball Edge, configura Amazon EKS Anywhere in base a. [Configurazione ed esecuzione di Amazon EKS Anywhere su dispositivi Snowball Edge](#)

Configurazione ed esecuzione di Amazon EKS Anywhere su dispositivi Snowball Edge

Segui queste procedure per configurare e avviare Amazon EKS Anywhere sui tuoi dispositivi Snowball Edge. Quindi, per configurare Amazon EKS Anywhere in modo che funzioni su dispositivi disconnessi, completa procedure aggiuntive prima di scollegare tali dispositivi dalla rete esterna. Per ulteriori informazioni, consulta [Configurazione di Amazon EKS Anywhere on AWS Snow per il funzionamento disconnesso](#).

Argomenti

- [Configurazione iniziale per Amazon EKS Anywhere su Snowball Edge](#)
- [Configurazione ed esecuzione automatica di Amazon EKS Anywhere su dispositivi Snowball Edge](#)
- [Configurazione ed esecuzione manuale di Amazon EKS Anywhere su dispositivi Snowball Edge](#)

Configurazione iniziale per Amazon EKS Anywhere su Snowball Edge

Esegui la configurazione iniziale su ogni dispositivo Snowball Edge collegando il dispositivo alla rete locale, scaricando il client Snowball Edge, ottenendo le credenziali e sbloccando il dispositivo.

Esegui la configurazione iniziale

1. Scarica e installa il client Snowball Edge. Per ulteriori informazioni, consulta [Scaricamento e installazione del client Snowball Edge](#).
2. Connect il dispositivo alla rete locale. Per ulteriori informazioni, consulta [Connessione di uno Snowball Edge alla rete locale](#).
3. Ottieni le credenziali per sbloccare il dispositivo. Per ulteriori informazioni, consulta [Ottenere le credenziali per accedere a Snowball Edge](#).
4. Sbloccare il dispositivo. Per ulteriori informazioni, consulta [Sbloccare Snowball Edge](#). Puoi anche utilizzare uno strumento di script invece di sbloccare i dispositivi manualmente. Vedi [Sbloccare i dispositivi](#).

Configurazione ed esecuzione automatica di Amazon EKS Anywhere su dispositivi Snowball Edge

Puoi utilizzare strumenti di script di esempio per configurare l'ambiente ed eseguire un'istanza di amministrazione di Amazon EKS Anywhere oppure puoi farlo manualmente. Per utilizzare gli strumenti di script, consulta [Unlock devices and setup environment for Amazon EKS Anywhere](#). Dopo la configurazione dell'ambiente e l'esecuzione dell'istanza di amministrazione di Amazon EKS Anywhere, se devi configurare Amazon EKS Anywhere per funzionare sul dispositivo Snowball Edge quando non sei connesso da una rete, consulta [Configurazione di Amazon EKS Anywhere on AWS Snow per il funzionamento disconnesso](#). In caso contrario, consulta [Creazione e manutenzione di cluster su dispositivi Snowball Edge](#).

Per configurare manualmente l'ambiente ed eseguire un'istanza di amministrazione di Amazon EKS Anywhere, consulta [Configurazione ed esecuzione manuale di Amazon EKS Anywhere su dispositivi Snowball Edge](#).

Configurazione ed esecuzione manuale di Amazon EKS Anywhere su dispositivi Snowball Edge

Prima di configurare Amazon EKS Anywhere su un dispositivo Snowball Edge, configura un profilo per il client Snowball Edge. Per ulteriori informazioni, consulta [Configurazione e utilizzo del client Snowball Edge](#).

Argomenti

- [Crea un utente locale Amazon EKS Anywhere IAM](#)
- [\(Facoltativo\) Creare e importare una chiave Secure Shell su Snowball Edge](#)
- [Esegui un'istanza di amministrazione di Amazon EKS Anywhere su Snowball Edge e trasferisci i file di credenziali e certificati su di essa](#)

Crea un utente locale Amazon EKS Anywhere IAM

Per le migliori pratiche di sicurezza, crea un utente IAM locale per Amazon EKS Anywhere sul dispositivo Snowball Edge. È possibile eseguire questa operazione manualmente utilizzando le seguenti procedure.

Note

Esegui questa operazione per ogni dispositivo Snowball Edge che utilizzi.

Creare un utente locale su Snowball Edge

Usa il `create-user` comando per creare l'utente IAM di Amazon EKS Anywhere.

```
aws iam create-user --user-name user-name --endpoint http://snowball-ip:6078 --  
profile profile-name  
{  
  "User": {  
    "Path": "/",  
    "UserName": "eks-a-user",  
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",  
    "Arn": "arn:aws:iam::123456789012:user/eks-a-user",  
    "CreateDate": "2022-04-06T00:13:35.665000+00:00"  
  }  
}
```

Creare una policy per l'utente locale su Snowball Edge

Crea un documento di policy, usalo per creare una policy IAM e allega tale policy all'utente locale di Amazon EKS Anywhere.

Per creare un documento di policy e allegarlo all'utente locale di Amazon EKS Anywhere

1. Crea un documento di policy e salvalo sul tuo computer. Copia la politica riportata di seguito nel documento.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "snowball-device:DescribeDevice",
        "snowball-device:CreateDirectNetworkInterface",
        "snowball-device>DeleteDirectNetworkInterface",
        "snowball-device:DescribeDirectNetworkInterfaces",
        "snowball-device:DescribeDeviceSoftware"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:TerminateInstances",
        "ec2:ImportKeyPair",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeImages",
        "ec2>DeleteTags"
      ],
      "Resource": ["*"]
    }
  ]
}
```

2. Utilizza il `create-policy` comando per creare una policy IAM basata sul documento di policy. Il valore del `--policy-document` parametro deve utilizzare il percorso assoluto del file di policy. Ad esempio, `file:///home/user/policy-name.json`

```
aws iam create-policy --policy-name policy-name --policy-document file:///home/  
user/policy-name.json --endpoint http://snowball-ip:6078 --profile profile-name  
{  
  "Policy": {  
    "PolicyName": "policy-name",  
    "PolicyId":  
    "ANPACEMGEZDGNBVG3TQ0JQGEZAAAABP76TE5MKAAAABCCOTR2IJ43NBTJRZBU",  
    "Arn": "arn:aws:iam::123456789012:policy/policy-name",  
    "Path": "/",  
    "DefaultVersionId": "v1",  
    "AttachmentCount": 0,  
    "IsAttachable": true,  
    "CreateDate": "2022-04-06T04:46:56.907000+00:00",  
    "UpdateDate": "2022-04-06T04:46:56.907000+00:00"  
  }  
}
```

3. Utilizza il `attach-user-policy` comando per collegare la policy IAM all'utente locale di Amazon EKS Anywhere.

```
aws iam attach-user-policy --policy-arn policy-arn --user-name user-name --endpoint  
http://snowball-ip:6078 --profile profile-name
```

Creare una chiave di accesso e un file di credenziali su Snowball Edge

Crea una chiave di accesso per l'utente locale Amazon EKS Anywhere IAM. Quindi, crea un file di credenziali e includi in esso i valori `AccessKeyId` e quelli `SecretAccessKey` generati per l'utente locale. Il file delle credenziali verrà utilizzato dall'istanza di amministrazione di Amazon EKS Anywhere in un secondo momento.

1. Usa il `create-access-key` comando per creare una chiave di accesso per l'utente locale di Amazon EKS Anywhere.

```
aws iam create-access-key --user-name user-name --endpoint http://snowball-ip:6078
--profile profile-name
{
  "AccessKey": {
    "UserName": "eks-a-user",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "Status": "Active",
    "SecretAccessKey": "RTT/wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
    "CreateDate": "2022-04-06T04:23:46.139000+00:00"
  }
}
```

2. Crea un file di credenziali. In esso, salva i SecretAccessKey valori AccessKeyId and nel seguente formato.

```
[snowball-ip]
aws_access_key_id = ABCDEFGHIJKLMNOPQR2T
aws_secret_access_key = AfSD7sYz/TBZtzkReB16PuuISzJ2WtNkeePw+nNzJ
region = snow
```

Note

Se lavori con più dispositivi Snowball Edge, l'ordine delle credenziali nel file non ha importanza, ma le credenziali per tutti i dispositivi devono trovarsi in un unico file.

Creare un file di certificati per l'istanza di amministrazione su Snowball Edge

L'istanza di amministrazione di Amazon EKS Anywhere necessita dei certificati dei dispositivi Snowball Edge per funzionare su di essi. Crea un file di certificati contenente il certificato per accedere ai dispositivi Snowball Edge e utilizzarlo successivamente dall'istanza di amministrazione di Amazon EKS Anywhere.

Per creare un file di certificati

1. Usa il `list-certificates` comando per ottenere i certificati per ogni dispositivo Snowball Edge che intendi utilizzare.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge list-certificates --endpoint
https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-
code
{
  "Certificates" : [ {
    "CertificateArn" : "arn:aws:snowball-device::certificate/xxx",
    "SubjectAlternativeNames" : [ "ID:JID-xxx" ]
  } ]
}
```

2. Utilizzate il valore di `CertificateArn` come valore per il `--certificate-arn` parametro del `get-certificate` comando.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge get-certificate --certificate-arn ARN
--endpoint https://snowball-ip --manifest-file path-to-manifest-file --unlock-
code unlock-code
```

3. Crea un file di certificato del dispositivo. Inserisci l'output di `get-certificate` nel file del certificato. Di seguito è riportato un esempio di come salvare l'output.

Note

Se lavori con più dispositivi Snowball Edge, l'ordine delle credenziali nel file non ha importanza, ma le credenziali per tutti i dispositivi devono trovarsi in un unico file.

```
-----BEGIN CERTIFICATE-----
ZWtzYSBzbm93IHRlc3QgY2VydGlmawNhdGUgZWtzYSBzbm93IHRlc3QgY2VydGlm
aWNhdGVla3NhIHhNub3cgdGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vdyB0ZXN0IGNl
cnRpZm1jYXRlZWtzYSBzbm93IHRlc3QgY2VydGlmawNhdGVla3NhIHhNub3cgdGVz
dCBjZXJ0aWZpY2F0ZQMIIDXCcAkSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ
```

```
...
-----END CERTIFICATE-----
```

4. [Crea un utente locale Amazon EKS Anywhere IAM](#) Ripetere l'operazione per creare un utente locale IAM per Amazon EKS Anywhere su tutti i dispositivi Snowball Edge.

(Facoltativo) Creare e importare una chiave Secure Shell su Snowball Edge

Utilizza questa procedura opzionale per creare una chiave Secure Shell (SSH) per accedere a tutte le istanze del nodo Amazon EKS Anywhere e importare la chiave pubblica su tutti i dispositivi Snowball Edge. Conserva e proteggi questo file chiave.

Se salti questa procedura, Amazon EKS Anywhere creerà e importerà automaticamente una chiave SSH quando necessario. Questa chiave verrà archiviata nell'istanza di amministrazione in. `${PWD}/${CLUSTER_NAME}/eks-a-id_rsa`

Crea una chiave SSH e importala nell'istanza Amazon EKS Anywhere

1. Usa il `ssh-keygen` comando per generare una chiave SSH.

```
ssh-keygen -t rsa -C "key-name" -f path-to-key-file
```

2. Usa il `import-key-pair` comando per importare la chiave dal computer al dispositivo Snowball Edge.

Note

Il valore del `key-name` parametro deve essere lo stesso quando si importa la chiave su tutti i dispositivi.

```
aws ec2 import-key-pair --key-name key-name --public-key-material fileb:///path/to/key-file --endpoint http://snowball-ip:8008 --profile profile-name
{
  "KeyFingerprint": "5b:0c:fd:e1:a0:69:05:4c:aa:43:f3:3b:3e:04:7f:51",
  "KeyName": "default",
```

```
"KeyPairId": "s.key-85edb5d820c92a6f8"
}
```

Esegui un'istanza di amministrazione di Amazon EKS Anywhere su Snowball Edge e trasferisci i file di credenziali e certificati su di essa

Esegui un'istanza di amministrazione di Amazon EKS Anywhere su Snowball Edge

Segui questa procedura per eseguire manualmente un'istanza di amministrazione di Amazon EKS Anywhere, configurare un'interfaccia di rete virtuale (VNI) per l'istanza di amministrazione, controllare lo stato dell'istanza, creare una chiave SSH e connetterti all'istanza di amministrazione con essa. Puoi utilizzare uno strumento di script di esempio per automatizzare la creazione di un'istanza di amministrazione di Amazon EKS Anywhere e il trasferimento di file di credenziali e certificati su questa istanza. Vedi [Creazione di un'istanza di amministrazione di Amazon EKS Anywhere](#). Una volta completato lo strumento di script, puoi accedere all'istanza tramite ssh e creare cluster facendo riferimento a [Creazione e manutenzione di cluster su dispositivi Snowball Edge](#). Se desideri configurare manualmente l'istanza Amazon EKS Anywhere, utilizza i seguenti passaggi.

Note

Se utilizzi più di un dispositivo Snowball Edge per il provisioning del cluster, puoi avviare un'istanza di amministrazione di Amazon EKS Anywhere su qualsiasi dispositivo Snowball Edge.

Per eseguire un'istanza di amministrazione di Amazon EKS Anywhere

1. Utilizza il `create-key-pair` comando per creare una chiave SSH per l'istanza di amministrazione di Amazon EKS Anywhere. Il comando salva la chiave in. `$PWD/key-file-name`

```
aws ec2 create-key-pair --key-name key-name --query 'KeyMaterial' --output text --  
endpoint http://snowball ip:8008 > key-file-name --profile profile-name
```

2. Utilizzate il `describe-images` comando per trovare il nome dell'immagine che inizia con `eks-anywhere-admin` l'output.

```
aws ec2 describe-images --endpoint http://snowball-ip:8008 --profile profile-name
```

3. Usa il `run-instance` comando per avviare un'istanza di amministrazione eks-a con l'immagine di amministrazione di Amazon EKS Anywhere.

```
aws ec2 run-instances --image-id eks-a-admin-image-id --key-name key-name --  
instance-type sbe-c.xlarge --endpoint http://snowball-ip:8008 --profile profile-  
name
```

4. Utilizza il `describe-instances` comando per verificare lo stato dell'istanza Amazon EKS Anywhere. Attendi che il comando indichi lo stato dell'istanza `running` prima di continuare.

```
aws ec2 describe-instances --instance-id instance-id --endpoint http://snowball-  
ip:8008 --profile profile-name
```

5. Nell'output del `describe-device` comando, annota il valore dell'interfaccia `PhysicalNetworkInterfaceId` di rete fisica connessa alla rete. Lo userai per creare un VNI.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge describe-device --endpoint  
https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-  
code
```

6. Crea un VNI per l'istanza di amministrazione di Amazon EKS Anywhere. Usa il valore di `PhysicalNetworkInterfaceId` come valore del `physical-network-interface-id` parametro.

```
PATH_TO_Snowball_Edge_CLIENT/bin/snowballEdge create-virtual-network-interface  
--ip-address-assignment dhcp --physical-network-interface-id PNI --endpoint  
https://snowball-ip --manifest-file path-to-manifest-file --unlock-code unlock-  
code
```

7. Utilizza il valore di `IpAddress` come valore del `public-ip` parametro del `associate-address` comando per associare l'indirizzo pubblico all'istanza di amministrazione di Amazon EKS Anywhere.

```
aws ec2 associate-address --instance-id instance-id --public-ip VNI-IP --endpoint
http://snowball-ip:8008 --profile profile-name
```

8. Connettiti all'istanza di amministrazione di Amazon EKS Anywhere tramite SSH.

```
ssh -i path-to-key ec2-user@VNI-IP
```

Trasferimento di file di certificati e credenziali all'istanza di amministrazione su Snowball Edge

Dopo l'esecuzione dell'istanza di amministrazione di Amazon EKS Anywhere, trasferisci le credenziali e i certificati dei tuoi dispositivi Snowball Edge all'istanza di amministrazione. Esegui il comando seguente dalla stessa directory in cui hai salvato i file delle credenziali e dei certificati in `and`. [Creare una chiave di accesso e un file di credenziali su Snowball Edge](#) [Creare un file di certificati per l'istanza di amministrazione su Snowball Edge](#)

```
scp -i path-to-key path-to-credentials-file path-to-certificates-file ec2-user@eks-admin-instance-ip:~
```

Verifica il contenuto dei file sull'istanza di amministrazione di Amazon EKS Anywhere. Di seguito sono riportati alcuni esempi di file di credenziali e certificati.

```
[192.168.1.1]
aws_access_key_id = EMGEZDGNBVGy3TQ0JQGEZB5ULEAAIWHWUJDXEXAMPLE
aws_secret_access_key = AUHpqj00GZQHEYXDbN0neLN1fR0gEXAMPLE
region = snow

[192.168.1.2]
aws_access_key_id = EMGEZDGNBVGy3TQ0JQGEZG507F3FJUCMYRMI4KPIEXAMPLE
aws_secret_access_key = kY4C18+RJA wq/bu28Y8fUJepwqhDEXAMPLE
region = snow
```



```

-----BEGIN CERTIFICATE-----
ZWtzYSBzbm93IHRlc3QgY2VydGlmawNhdGUgZWtzYSBzbm93IHRlc3QgY2VydGlm
aWNhdGVla3NhIHhNub3cgdGVzdCBjZXJ0aWZpY2F0ZWVrc2Egc25vdyB0ZXN0IGNl
cnRpZmljYXRlZWtzYSBzbm93IHRlc3QgY2VydGlmawNhdGVla3NhIHhNub3cgdGVz
dCBjZXJ0aWZpY2F0ZQMIIDXCcAKSgAwIBAgIJAISM0nTVmbj+MA0GCSqGSIb3DQ
...
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
KJ0FP12PAYPEjxr81/PoCXfZeARBzn9WLUH5yz1ta+sYUJouzhzWuLJYA1xqcCPY
mhV1kRsN4hVd1BNRnCCpRF766yjdJeibKVzXQxoXoZBj10kuGwqRy3d3ndjK77h4
OR5Fv9mjGf7CjcaSjk/4iwmZvRSaQacb0YG5GVeb4mfUAuVtuFoMeYfnAgMBAAGj
azBpMAwGA1UdEwQFMAMBAf8wHQYDVR00BBYEFL/bRcnBRuSM5+FcYFa8HfIBomdF
...
-----END CERTIFICATE-----

```

Configurazione di Amazon EKS Anywhere on AWS Snow per il funzionamento disconnesso

Completa questa configurazione aggiuntiva di Amazon EKS Anywhere sul dispositivo Snowball Edge mentre è connesso a una rete per preparare Amazon EKS Anywhere all'esecuzione in un ambiente senza una connessione di rete esterna.

Per configurare Amazon EKS Anywhere per l'uso disconnesso con il tuo registro Kubernetes privato e locale, consulta la [configurazione di Registry Mirror](#) nella documentazione di EKS Anywhere.

Se hai creato un AMI del registro privato Harbor, segui le procedure in questa sezione.

Argomenti

- [Configurazione del registro Harbor su un dispositivo Snowball Edge](#)
- [Usa il registro Harbor sull'istanza di amministrazione di Amazon EKS Anywhere su Snowball Edge](#)

Configurazione del registro Harbor su un dispositivo Snowball Edge

Vedi [Configurazione di Harbor su un dispositivo Snowball Edge](#).

Usa il registro Harbor sull'istanza di amministrazione di Amazon EKS Anywhere su Snowball Edge

Consulta [Importazione di immagini di container Amazon EKS Anywhere nel registro Harbor locale su un dispositivo Snowball Edge](#).

Creazione e manutenzione di cluster su dispositivi Snowball Edge

Procedure consigliate per la creazione di cluster su Snowball Edge

Per creare un cluster Amazon EKS Anywhere, consulta [Create Snow clusters](#).

Tieni a mente le seguenti best practice quando crei cluster Amazon EKS Anywhere su dispositivi Snowball Edge:

- Prima di creare un cluster in un intervallo di indirizzi IP statico, assicurati che non vi siano altri cluster sul dispositivo Snowball Edge che utilizzano lo stesso intervallo di indirizzi IP.
- Prima di creare un cluster con indirizzo DHCP sul dispositivo Snowball Edge, assicurati che tutti gli intervalli di indirizzi IP statici utilizzati per i cluster non si trovino nella sottorete del pool DHCP.
- Quando crei più di un cluster, attendi che un cluster sia correttamente fornito e funzionante prima di crearne un altro.

Aggiornamento dei cluster su Snowball Edge

Per aggiornare un'AMI di amministrazione Amazon EKS Anywhere o un'AMI EKS Distro, contatta Supporto AWS. Supporto fornirà un aggiornamento Snowball Edge contenente l'AMI aggiornata. Quindi, scarica e installa l'aggiornamento Snowball Edge. Consulta [Scaricamento degli aggiornamenti sui dispositivi Snowball Edge](#) e [Installazione degli aggiornamenti sui dispositivi Snowball Edge](#).

Dopo aver aggiornato l'AMI Amazon EKS Anywhere, devi avviare una nuova istanza di amministrazione di Amazon EKS Anywhere. Consultare [Esegui un'istanza di amministrazione di Amazon EKS Anywhere su Snowball Edge](#). Quindi, copia i file chiave, la cartella del cluster, le credenziali e i certificati dall'istanza di amministrazione precedente all'istanza aggiornata. Questi si trovano in una cartella che prende il nome dal cluster.

Pulizia delle risorse del cluster su Snowball Edge

Se crei più cluster sui dispositivi Snowball Edge e non li elimini correttamente o se c'è un problema nel cluster e il cluster crea nodi sostitutivi dopo la ripresa, si verificherà una perdita di risorse. È disponibile uno strumento di script di esempio che puoi modificare e utilizzare per pulire l'istanza di amministrazione di Amazon EKS Anywhere e i tuoi dispositivi Snowball Edge. Consulta [Amazon EKS Anywhere sugli strumenti di pulizia della AWS neve](#).

Utilizzo di IAM localmente su Snowball Edge

AWS Identity and Access Management (IAM) ti aiuta a controllare in modo sicuro l'accesso alle AWS risorse eseguite sul tuo AWS Snowball Edge dispositivo. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse.

IAM è supportato localmente sul tuo dispositivo. Puoi utilizzare il servizio IAM locale per creare nuovi utenti e allegare loro politiche IAM. È possibile utilizzare questi criteri per consentire l'accesso necessario per eseguire le attività assegnate. Ad esempio, puoi dare a un utente la possibilità di trasferire dati, ma limitarne la possibilità di creare nuove istanze EC2 compatibili con Amazon.

Inoltre, puoi creare credenziali locali basate sulla sessione utilizzando AWS Security Token Service (AWS STS) sul tuo dispositivo. Per informazioni sul servizio IAM, consulta la [Guida introduttiva](#) alla IAM User Guide.

Le credenziali root del tuo dispositivo non possono essere disabilitate e non puoi utilizzare le policy all'interno del tuo account per negare esplicitamente l'accesso all'utente root. Account AWS Ti consigliamo di proteggere le chiavi di accesso dell'utente root e di creare credenziali utente IAM per l'interazione quotidiana con il tuo dispositivo.

Important

La documentazione in questa sezione si applica all'utilizzo di IAM localmente su un AWS Snowball Edge dispositivo. Per informazioni sull'utilizzo di IAM in Cloud AWS, consulta [Identity and Access Management in AWS Snowball Edge](#).

AWS Affinché i servizi funzionino correttamente su Snowball Edge, è necessario consentire le porte per i servizi. Per informazioni dettagliate, consultare [Requisiti delle porte per AWS i servizi su Snowball Edge](#).

Argomenti

- [Utilizzo delle operazioni AWS CLI e dell'API su Snowball Edge](#)
- [Elenco dei AWS CLI comandi IAM supportati su Snowball Edge](#)
- [Esempi di policy IAM su Snowball Edge](#)
- [TrustPolicy esempio su Snowball Edge](#)

Utilizzo delle operazioni AWS CLI e dell'API su Snowball Edge

Quando utilizzi le operazioni AWS CLI o API per emettere EC2 comandi IAM AWS STS, Amazon S3 e Amazon su Snowball Edge, devi specificare come "» region snow È possibile eseguire questa operazione utilizzando `aws configure` o all'interno del comando stesso, come negli esempi seguenti.

```
aws configure --profile abc
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Or

```
aws iam list-users --endpoint http://192.0.2.0:6078 --region snow --profile
snowballEdge
```

Note

L'ID della chiave di accesso e la chiave segreta di accesso utilizzate localmente su non AWS Snowball Edge possono essere scambiate con le chiavi di. Cloud AWS

Elenco dei AWS CLI comandi IAM supportati su Snowball Edge

Di seguito è riportata una descrizione del sottoinsieme di AWS CLI comandi e opzioni per IAM supportati sui dispositivi Snowball Edge. Un comando o un'opzione non incluso nell'elenco seguente non è supportato. I parametri non supportati per i comandi sono annotati nella descrizione.

- [attach-role-policy](#)— Allega la policy gestita specificata al ruolo IAM specificato.
- [attach-user-policy](#)— Allega la politica gestita specificata all'utente specificato.
- [create-access-key](#)— Crea una nuova chiave di accesso segreta IAM locale e l'ID della chiave di AWS accesso corrispondente per l'utente specificato.

- [create-policy](#): crea una nuova policy gestita da IAM per il tuo dispositivo.
- [create-role](#): crea un nuovo ruolo IAM locale per il tuo dispositivo. I seguenti parametri non sono supportati:
 - Tags
 - PermissionsBoundary
- [create-user](#): crea un nuovo utente IAM locale per il tuo dispositivo. I seguenti parametri non sono supportati:
 - Tags
 - PermissionsBoundary
- [delete-access-key](#) — Elimina una nuova chiave di accesso segreta IAM locale e l'ID della chiave di AWS accesso corrispondente per l'utente specificato.
- [delete-policy](#) — Elimina la policy gestita specificata.
- [delete-role](#) — [Elimina il ruolo](#) specificato.
- [delete-user](#) — [Elimina l'utente](#) specificato.
- [detach-role-policy](#) — Rimuove la politica gestita specificata dal ruolo specificato.
- [detach-user-policy](#) — Rimuove la politica gestita specificata dall'utente specificato.
- [get-policy](#): recupera le informazioni sulla policy gestita specificata, inclusa la versione predefinita della policy e il numero totale di utenti, gruppi e ruoli IAM locali a cui è associata la policy.
- [get-policy-version](#) — Recupera informazioni sulla versione specificata della policy gestita specificata, incluso il documento relativo alla policy.
- [get-role](#) — Recupera informazioni sul ruolo specificato, inclusi il percorso del ruolo, il GUID, l'ARN e la politica di fiducia del ruolo che concede l'autorizzazione ad assumere il ruolo.
- [get-user](#) — Recupera informazioni sull'utente IAM specificato, tra cui la data di creazione, il percorso, l'ID univoco e l'ARN dell'utente.
- [list-access-keys](#) — Restituisce informazioni sulla chiave di accesso IDs associata all'utente IAM specificato.
- [list-attached-role-policies](#) — Elenca tutte le policy gestite associate al ruolo IAM specificato.
- [list-attached-user-policies](#) — Elenca tutte le policy gestite collegate all'utente IAM specificato.
- [list-entities-for-policy](#) — Elenca tutti gli utenti, i gruppi e i ruoli IAM locali a cui è associata la policy gestita specificata.
 - --EntityFilter: sono supportati solo i valori user e role.

- [list-policies](#): elenca tutte le policy gestite disponibili nel tuo locale. Account AWS Il parametro seguente non è supportato:
 - --PolicyUsageFilter
- [list-roles](#): elenca i ruoli IAM locali con il prefisso di percorso specificato.
- [list-users](#): elenca gli utenti IAM con il prefisso di percorso specificato.
- [update-access-key](#)— Modifica lo stato della chiave di accesso specificata da Attivo a Inattivo o viceversa.
- [update-assume-role-policy](#)— Aggiorna la policy che concede a un'entità IAM l'autorizzazione ad assumere un ruolo.
- [update-role](#): aggiorna la descrizione o l'impostazione della durata massima della sessione di un ruolo.
- [update-user](#): aggiorna il nome e il percorso and/or dell'utente IAM specificato.

Operazioni API IAM supportate su Snowball Edge

Di seguito sono elencate le operazioni dell'API IAM che puoi utilizzare con Snowball Edge, con collegamenti alle relative descrizioni nella Guida di riferimento all'API IAM.

- [AttachRolePolicy](#)— Allega la policy gestita specificata al ruolo IAM specificato.
- [AttachUserPolicy](#)— Allega la politica gestita specificata all'utente specificato.
- [CreateAccessKey](#)— Crea una nuova chiave di accesso segreta IAM locale e l'ID della chiave di AWS accesso corrispondente per l'utente specificato.
- [CreatePolicy](#)— Crea una nuova policy gestita da IAM per il tuo dispositivo.
- [CreateRole](#)— Crea un nuovo ruolo IAM locale per il tuo dispositivo.
- [CreateUser](#)— Crea un nuovo utente IAM locale per il tuo dispositivo.

I seguenti parametri non sono supportati:

- Tags
- PermissionsBoundary
- [DeleteAccessKey](#)— Elimina la chiave di accesso specificata.
- [DeletePolicy](#)— Elimina la politica gestita specificata.
- [DeleteRole](#)— Elimina il ruolo specificato.
- [DeleteUser](#)— Elimina l'utente specificato.

- [DetachRolePolicy](#)— Rimuove la politica gestita specificata dal ruolo specificato.
- [DetachUserPolicy](#)— Rimuove la politica gestita specificata dall'utente specificato.
- [GetPolicy](#)— Recupera le informazioni sulla policy gestita specificata, inclusa la versione predefinita della policy e il numero totale di utenti, gruppi e ruoli IAM locali a cui è associata la policy.
- [GetPolicyVersion](#)— Recupera informazioni sulla versione specificata della policy gestita specificata, incluso il documento relativo alla policy.
- [GetRole](#)— Recupera informazioni sul ruolo specificato, inclusi il percorso del ruolo, il GUID, l'ARN e la politica di fiducia del ruolo che concede l'autorizzazione ad assumere il ruolo.
- [GetUser](#)— Recupera informazioni sull'utente IAM specificato, tra cui la data di creazione, il percorso, l'ID univoco e l'ARN dell'utente.
- [ListAccessKeys](#)— Restituisce informazioni sulla chiave di accesso IDs associata all'utente IAM specificato.
- [ListAttachedRolePolicies](#)— Elenca tutte le policy gestite associate al ruolo IAM specificato.
- [ListAttachedUserPolicies](#)— Elenca tutte le policy gestite collegate all'utente IAM specificato.
- [ListEntitiesForPolicy](#)— Recupera informazioni sull'utente IAM specificato, tra cui la data di creazione, il percorso, l'ID univoco e l'ARN dell'utente.
 - --EntityFilter: sono supportati solo i valori `user` e `role`.
- [ListPolicies](#)— Elenca tutte le politiche gestite disponibili nel tuo locale. Account AWS Il parametro seguente non è supportato:
 - --PolicyUsageFilter
- [ListRoles](#)— Elenca i ruoli IAM locali con il prefisso di percorso specificato.
- [ListUsers](#)— Elenca gli utenti IAM con il prefisso di percorso specificato.
- [UpdateAccessKey](#)— Modifica lo stato della chiave di accesso specificata da Attivo a Inattivo o viceversa.
- [UpdateAssumeRolePolicy](#)— Aggiorna la policy che concede a un'entità IAM l'autorizzazione ad assumere un ruolo.
- [UpdateRole](#)— Aggiorna la descrizione o l'impostazione della durata massima della sessione di un ruolo.
- [UpdateUser](#)— Aggiorna il nome e and/or il percorso dell'utente IAM specificato.

Versione e grammatica delle policy IAM supportate su Snowball Edge

Di seguito è riportata la versione di supporto IAM locale 2012-10-17 del criterio IAM e un sottoinsieme della grammatica dei criteri.

Tipo di policy	Grammatica supportata
Criteri basati sull'identità (criterio utente/ruolo)	"Effect", "Action" e "Resource"  Note IAM locale non supporta "Condition", "NotAction", "NotResource" e "Principal".
Criteri basati sulle risorse (criteri di attendibilità dei ruoli)	"Effect", "Action" e "Principal"  Note Per Principal, è consentito solo Account AWS l'ID o l'ID principale.

Esempi di policy IAM su Snowball Edge

Note

AWS Identity and Access Management Gli utenti (IAM) necessitano "snowballdevice:*" delle autorizzazioni per utilizzare l'[AWS OpsHub for Snow Family applicazione](#) e gestire Snowball Edge.

Di seguito sono riportati alcuni esempi di policy che concedono autorizzazioni a un dispositivo Snowball Edge.

Consentire la GetUser chiamata per un utente campione su Snowball Edge tramite l'API IAM

Utilizza la seguente policy per consentire la GetUser chiamata a un utente campione tramite l'API IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "iam:GetUser",
      "Resource": "arn:aws:iam::user/example-user"
    }
  ]
}
```

Consentire l'accesso completo all'API Amazon S3 su Snowball Edge

Utilizza la seguente policy per consentire l'accesso completo all'API Amazon S3.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Consentire l'accesso in lettura e scrittura a un bucket Amazon S3 su Snowball Edge

Utilizzare il criterio seguente per consentire l'accesso in lettura e scrittura a un bucket specifico.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListObjectsInBucket",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::bucket-name"
    },
    {
      "Sid": "AllObjectActions",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::bucket-name/*"
    }
  ]
}
```

Consentire l'accesso a elenchi, get e put a un bucket Amazon S3 su Snowball Edge

Utilizza la seguente policy per consentire l'accesso a List, Get e Put a un bucket S3 specifico.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "s3:PutObject",
        "s3:GetObject",
        "s3:List*"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
}
]
```

Consentire l'accesso completo all' EC2API Amazon su Snowball Edge

Utilizza la seguente politica per consentire l'accesso completo ad Amazon EC2.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    }
  ]
}
```

Consentire l'accesso per avviare e arrestare istanze EC2 compatibili con Amazon su Snowball Edge

Utilizza la seguente politica per consentire l'accesso all'avvio e all'arresto EC2 delle istanze Amazon.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances"
        ],
        "Resource": "*"
    }
]
```

Negare le chiamate verso uno Snowball Edge, DescribeLaunchTemplates ma consentire DescribeImages a tutte le chiamate di farlo

Utilizzare il seguente criterio per negare le chiamate DescribeLaunchTemplates ma consentire tutte le chiamate a DescribeImages.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    }
  ]
}
```

Criteri per le chiamate API su Snowball Edge

Elenca tutte le policy gestite disponibili sul dispositivo Snow, incluse le policy gestite definite dal cliente. [Maggiori dettagli in list-policies.](#)

```
aws iam list-policies --endpoint http://ip-address:6078 --region snow --profile
snowballEdge
{
  "Policies": [
    {
      "PolicyName": "Administrator",
      "Description": "Root user admin policy for Account 123456789012",
      "CreateDate": "2020-03-04T17:44:59.412Z",
      "AttachmentCount": 1,
      "IsAttachable": true,
      "PolicyId": "policy-id",
      "DefaultVersionId": "v1",
      "Path": "/",
      "Arn": "arn:aws:iam::123456789012:policy/Administrator",
      "UpdateDate": "2020-03-04T19:10:45.620Z"
    }
  ]
}
```

TrustPolicy esempio su Snowball Edge

Una politica di attendibilità restituisce una serie di credenziali di sicurezza temporanee che è possibile utilizzare per accedere a AWS risorse a cui normalmente non si ha accesso. Le credenziali temporanee sono costituite da un ID chiave di accesso, una chiave di accesso segreta e un token di sicurezza. In genere, si utilizza AssumeRole nel proprio account per l'accesso tra account.

Di seguito è illustrato un esempio di policy di attendibilità. Per ulteriori informazioni sulla politica di fiducia, consulta [AssumeRole](#) l'AWS Security Token Service API Reference.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
        "Effect": "Allow",
        "Principal": {
            "AWS": [
                "arn:aws:iam::AccountId:root" //You can use the Principal ID
instead of the account ID.
            ]
        },
        "Action": [
            "sts:AssumeRole"
        ]
    }
]
```

Utilizzo AWS Security Token Service su Snowball Edge

Il AWS Security Token Service (AWS STS) consente di richiedere credenziali temporanee con privilegi limitati per gli utenti IAM.

Important

AWS Affinché i servizi funzionino correttamente su Snowball Edge, è necessario consentire le porte per i servizi. Per informazioni dettagliate, consultare [Requisiti delle porte per AWS i servizi su Snowball Edge](#).

Argomenti

- [Utilizzo delle operazioni AWS CLI e dell'API su Snowball Edge](#)
- [AWS STSAWS CLI Comandi supportati su Snowball Edge](#)
- [Operazioni AWS STS API supportate su Snowball Edge](#)

Utilizzo delle operazioni AWS CLI e dell'API su Snowball Edge

Quando utilizzi le operazioni AWS CLI o API per emettere EC2 comandi IAM AWS STS, Amazon S3 e Amazon su un dispositivo Snowball Edge, devi specificare come "» region snow È possibile eseguire questa operazione utilizzando AWS configure o all'interno del comando stesso, come negli esempi seguenti.

```
aws configure --profile snowballEdge
AWS Access Key ID [None]: defgh
AWS Secret Access Key [None]: 1234567
Default region name [None]: snow
Default output format [None]: json
```

Or

```
aws iam list-users --endpoint http://192.0.2.0:6078 --region snow --profile
snowballEdge
```


 Note

L'ID della chiave di accesso e la chiave segreta di accesso utilizzati localmente su non AWS Snowball Edge possono essere scambiati con le chiavi di Cloud AWS

AWS STSAWS CLI Comandi supportati su Snowball Edge

Solo il comando [assume-role](#) è supportato localmente.

Sono supportati i seguenti parametri per `assume-role`:

- `role-arn`
- `role-session-name`
- `duration-seconds`

Esempio di comando per assumere un ruolo su Snowball Edge

Per assumere un ruolo, utilizzare il comando seguente.

```
aws sts assume-role --role-arn "arn:aws:iam::123456789012:role/example-role" --  
role-session-name AWSCLI-Session --endpoint http://snow-device-IP-address:7078
```

Per ulteriori informazioni sull'utilizzo del `assume-role` comando, vedi [Come si assume un ruolo IAM utilizzando il AWS CLI?](#)

Per ulteriori informazioni sull'utilizzo AWS STS, consulta Using [Temporary Security Credentials](#) nella IAM User Guide.

Operazioni AWS STS API supportate su Snowball Edge

Solo l'[AssumeRole](#) API è supportata localmente.

Sono supportati i seguenti parametri per `AssumeRole`:

- `RoleArn`

- RoleSessionName
- DurationSeconds

Example di assumere un ruolo

```
https://sts.amazonaws.com/  
?Version=2011-06-15  
&Action=AssumeRole  
&RoleSessionName=session-example  
&RoleArn=arn:aws:iam::123456789012:role/demo  
&DurationSeconds=3600
```

Gestione dei certificati a chiave pubblica su Snowball Edge

Puoi interagire in modo sicuro con AWS i servizi in esecuzione su un dispositivo Snowball Edge o su un cluster di dispositivi Snowball Edge tramite il protocollo HTTPS fornendo un certificato a chiave pubblica. Puoi utilizzare il protocollo HTTPS per interagire con AWS servizi come IAM, Amazon, adattatore S3 EC2, storage compatibile con Amazon S3 su Snowball Edge, Amazon EC2 Systems Manager AWS STS e su dispositivi Snowball Edge. Nel caso di un cluster di dispositivi, è richiesto un singolo certificato che può essere generato da qualsiasi dispositivo del cluster. Una volta che un dispositivo Snowball Edge genera il certificato e lo sblocca, puoi utilizzare i comandi del client Snowball Edge per elencare, ottenere ed eliminare il certificato.

Un dispositivo Snowball Edge genera un certificato quando si verificano i seguenti eventi:

- Il dispositivo o il cluster Snowball Edge viene sbloccato per la prima volta.
- Il dispositivo o il cluster Snowball Edge viene sbloccato dopo l'eliminazione del certificato (utilizzando il `delete-certificate` comando o Rinnova certificato in). AWS OpsHub
- Il dispositivo o il cluster Snowball Edge viene riavviato e sbloccato dopo la scadenza del certificato.

Ogni volta che viene generato un nuovo certificato, il vecchio certificato non è più valido. Un certificato è valido per un periodo di un anno dal giorno in cui è stato generato.

È inoltre possibile AWS OpsHub utilizzarlo per gestire i certificati a chiave pubblica. Per ulteriori informazioni, consulta [Gestire l'utilizzo dei certificati a chiave pubblica OpsHub](#) in questa guida.

Argomenti

- [Inserimento del certificato su Snowball Edge](#)
- [Ottenere certificati da Snowball Edge](#)
- [Eliminazione di certificati su Snowball Edge](#)

Inserimento del certificato su Snowball Edge

Usa il `list-certificates` comando per visualizzare Amazon Resource Names (ARNs) per il certificato corrente.

```
snowballEdge list-certificates
```

Example di **list-certificates** output

```
{
  "Certificates" : [ {
    "CertificateArn" : "arn:aws:snowball-
device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7",
    "SubjectAlternativeNames" : [ "192.0.2.0" ]
  } ]
}
```

Ottenere certificati da Snowball Edge

Utilizzare il `get-certificate` comando per visualizzare il contenuto del certificato in base all'ARN fornito. Utilizzare il `list-certificates` comando per ottenere l'ARN del certificato da utilizzare come parametro. `certificate-arn`

```
snowballEdge get-certificate --certificate-arn arn:aws:snowball-
device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
```

Example di **get-certificate** output

```
-----BEGIN CERTIFICATE-----
Certificate
-----END CERTIFICATE-----
```

Per informazioni sulla configurazione del certificato, consulta [Configurazione AWS CLI per utilizzare l'adattatore S3 su uno Snowball Edge come endpoint](#).

Eliminazione di certificati su Snowball Edge

Usa il `delete-certificate` comando per eliminare il certificato corrente. Utilizzare il `list-certificates` comando per ottenere l'ARN del certificato da utilizzare come parametro. `certificate-arn` Per generare un nuovo certificato, riavvia Snowball Edge o ogni Snowball Edge

in un cluster. Visualizza [Riavvio del dispositivo Snowball Edge](#) o usa il comando. `snowballEdge reboot-device`

```
snowballEdge delete-certificate --certificate-arn arn:aws:snowball-  
device::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
```

Example di **delete-certificate** output

```
The certificate has been deleted from your Snow device. Please reboot your Snowball  
Edge or Snowball Edge cluster to generate a new certificate.
```

Requisiti delle porte per AWS i servizi su Snowball Edge

AWS Affinché i servizi funzionino correttamente su un AWS Snowball Edge dispositivo, è necessario consentire le porte di rete del servizio.

Di seguito è riportato un elenco di porte di rete necessarie per ogni AWS servizio.

Porta	Protocollo	Commento
22 (HTTP)	TCP	Controllo dello stato del dispositivo e per EC2 SSH
443 (HTTPS)	TCP	Endpoint HTTPS dell'API S3 e dell'API di controllo S3
2049 (HTTP)	TCP	Endpoint NFS
6078 (HTTP)	TCP	Endpoint IAM HTTP
6089 (HTTPS)	TCP	Endpoint IAM HTTPS
7078 (HTTP)	TCP	Endpoint STS HTTP
7089 (HTTPS)	TCP	Endpoint STS HTTPS
8080 (HTTP)	TCP	Endpoint HTTP dell'adattatore S3
8008 (HTTP)	TCP	EC2 Endpoint HTTP
8243 (HTTPS)	TCP	EC2 Endpoint HTTPS
8443 (HTTPS)	TCP	Endpoint HTTPS dell'adattatore S3
9091 (HTTP)	TCP	Endpoint per la gestione dei dispositivi
9092	TCP	Inbound per EKS Anywhere e controller di dispositivi CAPAS

Porta	Protocollo	Commento
8242	TCP	Endpoint EC2 HTTPS in entrata per EKS Anywhere
6443	TCP	In entrata per l'endpoint dell'API Kubernetes EKS Anywhere
2379	TCP	In entrata per l'endpoint API EKS Anywhere Etcd
2380	TCP	In entrata per l'endpoint API EKS Anywhere Etcd

Utilizzo AWS Snowball Edge Device Management per gestire Snowball Edge

AWS Snowball Edge Device Management consente di gestire da remoto Snowball Edge e AWS i servizi locali. Tutti gli Snowball Edge supportano Snowball Edge Device Management e vengono installati su nuovi dispositivi nella maggior parte dei paesi in cui è disponibile Regioni AWS Snowball Edge.

Con Snowball Edge Device Management, puoi eseguire le seguenti attività:

- Creare un'attività
- Controlla lo stato dell'attività
- Controlla i metadati delle attività
- Annullare un'attività
- Controlla le informazioni sul dispositivo
- Verifica lo stato dell'istanza EC2 compatibile con Amazon
- Elenca i comandi e la sintassi
- Elenca i dispositivi gestibili in remoto
- Elenca lo stato delle attività su tutti i dispositivi
- Elenca le risorse disponibili
- Elenca le attività per stato
- Elenca i tag dei dispositivi o delle attività
- Applica tag
- Rimuovere i tag

Argomenti

- [Scelta dello stato di gestione dei dispositivi Snowball Edge quando si ordina uno Snowball Edge](#)
- [Attivazione della gestione dei dispositivi Snowball Edge su Snowball Edge](#)
- [Aggiungere le autorizzazioni per Snowball Edge Device Management a un ruolo IAM su Snowball Edge](#)
- [Comandi CLI di Snowball Edge Device Management](#)

Scelta dello stato di gestione dei dispositivi Snowball Edge quando si ordina uno Snowball Edge

Quando si crea un lavoro per ordinare un dispositivo Snow, è possibile scegliere lo stato in cui si troverà Snowball Edge Device Management quando si riceve il dispositivo: installato ma non attivato oppure installato e attivato. Se è installato ma non attivato, dovrai utilizzare AWS OpsHub o il client Snowball Edge per attivarlo prima di utilizzarlo. Se è installato e attivato, puoi utilizzare Snowball Edge Device Management dopo aver ricevuto il dispositivo e averlo connesso alla rete locale. Puoi scegliere lo stato di gestione dei dispositivi Snowball Edge quando crei un lavoro per ordinare un dispositivo tramite il Console di gestione della famiglia di servizi AWS Snow client Snowball Edge o l'AWS CLI API di gestione dei lavori Snow.

Per scegliere lo stato di gestione dei dispositivi Snowball Edge tra i Console di gestione della famiglia di servizi AWS Snow

1. Per scegliere di installare e attivare Snowball Edge Device Management, scegli Gestisci il tuo dispositivo Snow da remoto con il nostro client AWS OpsHub Snowball.
2. Per scegliere che Snowball Edge Device Management sia installato ma non attivato, non selezionare Gestisci il tuo dispositivo Snow da remoto con un client AWS OpsHub Snowball.

Per ulteriori informazioni, consulta [Passaggio 3: scelta delle funzionalità e delle opzioni](#) in questa guida.

Per scegliere lo stato di gestione dei dispositivi Snowball Edge dal client AWS CLI Snowball Edge o dall'API Snow job management:

- Utilizzate il `remote-management` parametro per specificare lo stato di gestione dei dispositivi Snowball Edge. Il `INSTALLED_ONLY` valore del parametro indica che Snowball Edge Device Management è installato ma non attivato. Il `INSTALLED_AUTOSTART` valore del parametro indica che Snowball Edge Device Management è installato e attivato. Se non si specifica un valore per questo parametro, `INSTALLED_ONLY` è il valore predefinito.

Example della sintassi del **remote-management** parametro del comando **create-job**

```
aws snowball create-job \  
  --job-type IMPORT \  
  --remote-management INSTALLED_ONLY
```

```
--remote-management INSTALLED_AUTOSTART
--device-configuration '{"SnowconeDeviceConfiguration": {"WirelessConnection":
{"IsWifiEnabled": false} } }' \
--resources '{"S3Resources":[{"BucketArn":"arn:aws:s3:::bucket-name"}]}' \
--description "Description here" \
--address-id ADID000000000-0000-0000-0000-000000000000 \
--kms-key-arn arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--role-arn arn:aws:iam::000000000000:role/SnowconeImportGamma \
--snowball-capacity-preference T8 \
--shipping-option NEXT_DAY \
--snowball-type SNC1_HDD \
--region us-west-2 \
```

Per ulteriori informazioni, consulta [Job Management API Reference](#) nel AWS Snowball Edge API Reference.

Attivazione della gestione dei dispositivi Snowball Edge su Snowball Edge

Segui questa procedura per attivare Snowball Edge Device Management utilizzando il client Snowball Edge.

Prima di utilizzare questa procedura, effettuate le seguenti operazioni:

- Scarica e installa la versione più recente del client Snowball Edge. Per ulteriori informazioni, consulta [Scaricamento e installazione del client Snowball](#).
- Scarica il file manifest e ottieni il codice di sblocco per il dispositivo Snowball Edge. Per ulteriori informazioni, consulta [Ottenere le credenziali e gli strumenti](#).
- Connect il dispositivo Snowball Edge alla rete locale. Per ulteriori informazioni, consulta [Connessione alle di rete locale](#).
- Sblocca il dispositivo Snowball Edge. Per ulteriori informazioni, consulta [Sblocco di Snowball Edge Sblocco](#) di un dispositivo .

```
snowballEdge set-features /
--remote-management-state INSTALLED_AUTOSTART /
--manifest-file JID1717d8cc-2dc9-4e68-aa46-63a3ad7927d2_manifest.bin /
--unlock-code 7c0e1-bab84-f7675-0a2b6-f8k33 /
```

```
--endpoint https://192.0.2.0:9091
```

Il client Snowball Edge restituisce quanto segue quando il comando ha esito positivo.

```
{
  "RemoteManagementState" : "INSTALLED_AUTOSTART"
}
```

Aggiungere le autorizzazioni per Snowball Edge Device Management a un ruolo IAM su Snowball Edge

Sul dispositivo Account AWS da cui è stato ordinato il dispositivo, crea un ruolo AWS Identity and Access Management (IAM) e aggiungi la seguente policy al ruolo. Quindi, assegna il ruolo all'utente IAM che effettuerà l'accesso per gestire in remoto il tuo dispositivo con Snowball Edge Device Management. Per ulteriori informazioni, consulta [Creazione di ruoli IAM e Creazione di un utente IAM](#) nel tuo Account AWS

Policy

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "snow-device-management:ListDevices",
        "snow-device-management:DescribeDevice",
        "snow-device-management:DescribeDeviceEc2Instances",
        "snow-device-management:ListDeviceResources",
        "snow-device-management:CreateTask",
        "snow-device-management:ListTasks",
        "snow-device-management:DescribeTask",
        "snow-device-management:CancelTask",
        "snow-device-management:DescribeExecution",

```

```
        "snow-device-management:ListExecutions",
        "snow-device-management:ListTagsForResource",
        "snow-device-management:TagResource",
        "snow-device-management:UntagResource"
    ],
    "Resource": "*"
}
]
```

Comandi CLI di Snowball Edge Device Management

Questa sezione descrive i AWS CLI comandi che è possibile utilizzare per gestire Snowball Edge in remoto con Snowball Edge Device Management. È inoltre possibile eseguire alcune attività di gestione remota utilizzando AWS OpsHub. Per ulteriori informazioni, consulta [Gestione AWS dei servizi sul dispositivo](#).

Note

Prima di gestire il dispositivo, assicurati che sia acceso, connesso alla rete e che possa connettersi al Regione AWS punto in cui è stato fornito.

Argomenti

- [Creazione di un'attività per gestire uno Snowball Edge con Snowball Edge Device Management](#)
- [Verifica dello stato di un'attività per gestire uno Snowball Edge](#)
- [Verifica delle informazioni su Snowball Edge utilizzando Snowball Edge Device Management](#)
- [Verifica dello stato delle istanze EC2 compatibili con Amazon su Snowball Edge con Snowball Edge Device Management](#)
- [Visualizzazione dei metadati delle attività su Snowball Edge con Snowball Edge Device Management](#)
- [Annullamento di un'attività su Snowball Edge con Snowball Edge Device Management](#)
- [Elenco dei comandi e della sintassi di Snowball Edge Device Management](#)
- [Elenco Snowball Edge disponibile per la gestione remota](#)
- [Elenco dello stato delle attività di gestione dei dispositivi Snowball Edge su Snowball Edge](#)

- [Elenco delle risorse disponibili su Snowball Edge con Snowball Edge Device Management](#)
- [Elenco dei tag per i tag Snowball Edge o Snowball Edge Device Management](#)
- [Elenco delle attività di Snowball Edge Device Management per stato](#)
- [Applicazione di tag alle attività di gestione dei dispositivi di Snowball Edge o Snowball Edge](#)
- [Rimuovere i tag di Snowball Edge Device Management dalle attività o da Snowball Edge](#)

Creazione di un'attività per gestire uno Snowball Edge con Snowball Edge Device Management

Per indicare a uno o più dispositivi di destinazione di eseguire un'operazione, come lo sblocco o il riavvio, usa `create-task`. È possibile specificare i dispositivi di destinazione fornendo un elenco di dispositivi gestiti IDs con il `--targets` parametro e specificando le attività da eseguire con il parametro. `--command` È possibile eseguire un solo comando alla volta su un dispositivo.

Comandi supportati:

- `unlock`(senza argomenti)
- `reboot`(nessun argomento)

Per creare un'attività che deve essere eseguita dai dispositivi di destinazione, utilizzare il seguente comando. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management create-task
--targets smd-fictbgr3rbcjeqa5
--command reboot={}
```

Eccezioni

```
ValidationException
ResourceNotFoundException
InternalServerError
ThrottlingException
AccessDeniedException
```

```
ServiceQuotaExceededException
```

Output

```
{
  "taskId": "st-ficthmqoc2pht111",
  "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-
cjkwhmqoc2pht111"
}
```

Verifica dello stato di un'attività per gestire uno Snowball Edge

Per verificare lo stato di un'operazione remota in esecuzione su uno o più dispositivi di destinazione, usa il `describe-execution` comando.

Un'attività può avere uno dei seguenti stati:

- QUEUED
- IN_PROGRESS
- CANCELED
- FAILED
- COMPLETED
- REJECTED
- TIMED_OUT

Per verificare lo stato di un'attività, utilizzare il comando seguente. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management describe-execution \
--taskId st-ficthmqoc2pht1ef \
--managed-device-id smd-fictqic6gcldf111
```

Output

```
{
  "executionId": "1",
  "lastUpdatedAt": "2021-07-22T15:29:44.110000+00:00",
  "managedDeviceId": "smd-fictqic6gcldf111",
  "startedAt": "2021-07-22T15:28:53.947000+00:00",
  "state": "SUCCEEDED",
  "taskId": "st-ficthmqoc2pht111"
}
```

Verifica delle informazioni su Snowball Edge utilizzando Snowball Edge Device Management

Per controllare le informazioni specifiche del dispositivo, come il tipo di dispositivo, la versione del software, gli indirizzi IP e lo stato del blocco, usa il comando `describe-device`. L'output include anche quanto segue:

- `lastReachedOutAt`— L'ultima volta che il dispositivo ha contattato il Cloud AWS. Indica che il dispositivo è online.
- `lastUpdatedAt`— Quando i dati sono stati aggiornati l'ultima volta sul dispositivo. Indica quando la cache del dispositivo è stata aggiornata.

Per controllare le informazioni sul dispositivo, usa il seguente comando. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management describe-device \
--managed-device-id smd-fictqic6gcldf111
```

Eccezioni

```
ValidationException
ResourceNotFoundException
InternalServerError
```

```
ThrottlingException
AccessDeniedException
```

Verifica dello stato delle istanze EC2 compatibili con Amazon su Snowball Edge con Snowball Edge Device Management

Per verificare lo stato corrente dell' EC2istanza Amazon, usa il `describe-ec2-instances` comando. L'output è simile a quello del `describe-device` comando, ma i risultati provengono dalla cache del dispositivo Cloud AWS e includono un sottoinsieme dei campi disponibili.

Per verificare lo stato dell'istanza EC2 compatibile con Amazon, usa il seguente comando. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management describe-device-ec2-instances \
--managed-device-id smd-fictbgr3rbcje111 \
--instance-ids s.i-84fa8a27d3e15e111
```

Eccezioni

```
ValidationException
ResourceNotFoundException
InternalServerError
ThrottlingException
AccessDeniedException
```

Output

```
{
  "instances": [
    {
      "instance": {
        "amiLaunchIndex": 0,
        "blockDeviceMappings": [
```



```

        {
            "deviceName": "/dev/sda",
            "ebs": {
                "attachTime": "2021-07-23T15:25:38.719000-07:00",
                "deleteOnTermination": true,
                "status": "ATTACHED",
                "volumeId": "s.vol-84fa8a27d3e15e111"
            }
        },
        "cpuOptions": {
            "coreCount": 1,
            "threadsPerCore": 1
        },
        "createdAt": "2021-07-23T15:23:22.858000-07:00",
        "imageId": "s.ami-03f976c3cadaa6111",
        "instanceId": "s.i-84fa8a27d3e15e111",
        "state": {
            "name": "RUNNING"
        },
        "instanceType": "snc1.micro",
        "privateIpAddress": "34.223.14.193",
        "publicIpAddress": "10.111.60.160",
        "rootDeviceName": "/dev/sda",
        "securityGroups": [
            {
                "groupId": "s.sg-890b6b4008bdb3111",
                "groupName": "default"
            }
        ],
        "updatedAt": "2021-07-23T15:29:42.163000-07:00"
    },
    "lastUpdatedAt": "2021-07-23T15:29:58.
071000-07:00"
}
]
}

```

Visualizzazione dei metadati delle attività su Snowball Edge con Snowball Edge Device Management

Per controllare i metadati di una determinata attività su un dispositivo, usa il comando `describe-task`. I metadati di un'attività includono i seguenti elementi:

- I dispositivi di destinazione
- Lo stato dell'attività
- Quando è stata creata l'attività
- Quando i dati sono stati aggiornati l'ultima volta sul dispositivo
- Quando l'attività è stata completata
- L'eventuale descrizione fornita al momento della creazione dell'attività

Per controllare i metadati di un'attività, usa il comando seguente. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management describe-task \  
--task-id st-ficthmqoc2pht111
```

Eccezioni

```
ValidationException  
ResourceNotFoundException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Output

```
{  
  "completedAt": "2021-07-22T15:29:46.758000+00:00",
```

```
"createdAt": "2021-07-22T15:28:42.613000+00:00",
"lastUpdatedAt": "2021-07-22T15:29:46.758000+00:00",
"state": "COMPLETED",
"tags": {},
"targets": [
  "smd-fictbgr3rbcje111"
],
"taskId": "st-ficthmqoc2pht111",
"taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-
ficthmqoc2pht111"
}
```

Annullamento di un'attività su Snowball Edge con Snowball Edge Device Management

Per inviare una richiesta di annullamento per un'attività specifica, usa il `cancel-task` comando. È possibile annullare solo le attività nello QUEUED stato che non sono ancora state eseguite. Le attività già in esecuzione non possono essere annullate.

Note

Un'attività che si sta tentando di annullare potrebbe continuare a essere eseguita se viene elaborata dalla coda prima che il `cancel-task` comando modifichi lo stato dell'attività.

Per annullare un'operazione, utilizzare il comando seguente. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management cancel-task \
--task-id st-ficthmqoc2pht111
```

Eccezioni

```
ValidationException
ResourceNotFoundException
```

```
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Output

```
{  
  "taskId": "st-ficthmqoc2pht111"  
}
```

Elenco dei comandi e della sintassi di Snowball Edge Device Management

Per restituire un elenco di tutti i comandi supportati per l'API Snowball Edge Device Management, usa il `help` comando. È inoltre possibile utilizzare il `help` comando per restituire informazioni dettagliate e sulla sintassi di un determinato comando.

Per elencare tutti i comandi supportati, utilizzare il comando seguente.

Comando

```
aws snow-device-management help
```

Per restituire informazioni dettagliate e sintassi per un comando, utilizzare il comando seguente. Sostituiscilo *command* con il nome del comando che ti interessa.

Comando

```
aws snow-device-management command help
```

Elenco Snowball Edge disponibile per la gestione remota

Per restituire un elenco di tutti i dispositivi del tuo account su cui è abilitato Snowball Edge Device Management nel punto in Regione AWS cui viene eseguito il comando, usa il `list-devices` comando. `--max-resultse` `--next-token` sono opzionali. Per ulteriori informazioni, vedere [Uso delle opzioni di AWS CLI impaginazione](#) nella "Guida per l'utente dell'interfaccia a riga di AWS comando».

Per elencare i dispositivi gestibili in remoto, utilizzare il comando seguente. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management list-devices \  
--max-results 10
```

Eccezioni

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Output

```
{  
  "devices": [  
    {  
      "associatedWithJob": "ID2bf11d5a-ea1e-414a-b5b1-3bf7e6a6e111",  
      "managedDeviceId": "smd-fictbgr3rbcjeqa5",  
      "managedDeviceArn": "arn:aws:snow-device-management:us-west-2:000000000000:managed-device/smd-fictbgr3rbcje111",  
      "tags": {}  
    }  
  ]  
}
```

Elenco dello stato delle attività di gestione dei dispositivi Snowball Edge su Snowball Edge

Per restituire lo stato delle attività per uno o più dispositivi di destinazione, usa il `list-executions` comando. Per filtrare l'elenco restituito in modo da mostrare le attività che si trovano attualmente in un unico stato specifico, utilizzate il `--state` parametro. `--max-resultse` `--next-token` sono

opzionali. Per ulteriori informazioni, vedere [Uso delle opzioni di AWS CLI impaginazione](#) nella "Guida per l'utente dell'interfaccia a riga di AWS comando».

Un'attività può avere uno dei seguenti stati:

- QUEUED
- IN_PROGRESS
- CANCELED
- FAILED
- COMPLETED
- REJECTED
- TIMED_OUT

Per elencare lo stato delle attività su tutti i dispositivi, utilizzare il comando seguente. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management list-executions \  
--taskId st-ficthmqoc2phtlef \  
--state SUCCEEDED \  
--max-results 10
```

Eccezioni

```
ValidationException  
InternalServerError  
ThrottlingException  
AccessDeniedException
```

Output

```
{
```

```

    "executions": [
      {
        "executionId": "1",
        "managedDeviceId": "smd-fictbgr3rbcje111",
        "state": "SUCCEEDED",
        "taskId": "st-ficthmqoc2pht111"
      }
    ]
  }
}

```

Elenco delle risorse disponibili su Snowball Edge con Snowball Edge Device Management

Per restituire un elenco delle AWS risorse disponibili per un dispositivo, usa il `list-device-resources` comando. Per filtrare l'elenco in base a un tipo specifico di risorsa, utilizzate il `--type` parametro. Attualmente, le istanze EC2 compatibili con Amazon sono l'unico tipo di risorsa supportato. `--max-results` e `--next-token` sono opzionali. Per ulteriori informazioni, vedere [Uso delle opzioni di AWS CLI impaginazione](#) nella "Guida per l'utente dell'interfaccia a riga di AWS comando».

Per elencare le risorse disponibili per un dispositivo, utilizzare il comando seguente. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```

aws snow-device-management list-device-resources \
--managed-device-id smd-fictbgr3rbcje111 \
--type AWS::EC2::Instance
--next-
token YAQGPwAT9L3wVKaGYjt4yS34MiQLWvzcShe9oIeDJr05AT4rXSprqcqQhhBEYRfcerAp0YYbJmRT=
--max-results 10

```

Eccezioni

```

ValidationException
InternalServerError
ThrottlingException
AccessDeniedException

```

Output

```
{
  "resources": [
    {
      "id": "s.i-84fa8a27d3e15e111",
      "resourceType": "AWS::EC2::Instance"
    }
  ]
}
```

Elenco dei tag per i tag Snowball Edge o Snowball Edge Device Management

Per restituire un elenco di tag per un dispositivo o un'attività gestita, usa il `list-tags-for-resource` comando.

Per elencare i tag di un dispositivo, usa il comando seguente. Sostituisci l'esempio Amazon Resource Name (ARN) con l'ARN del tuo dispositivo.

Comando

```
aws snow-device-management list-tags-for-resource
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/
smd-fictbgr3rbcjeqa5
```

Eccezioni

```
AccessDeniedException
InternalServerError
ResourceNotFoundException
ThrottlingException
```

Output


```
{
  "tags": {
    "Project": "PrototypeA"
  }
}
```

Elenco delle attività di Snowball Edge Device Management per stato

Usa il `list-tasks` comando per restituire un elenco di attività dai dispositivi nella AWS regione in cui viene eseguito il comando. Per filtrare i risultati in base `IN_PROGRESS` `CANCELED` allo stato, utilizzate il `--state` parametro. `COMPLETED` `--max-resultse` `--next-token` sono opzionali. Per ulteriori informazioni, vedere [Uso delle opzioni di AWS CLI impaginazione](#) nella "Guida per l'utente dell'interfaccia a riga di AWS comando».

Per elencare le attività in base allo stato, utilizzare il comando seguente. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management list-tasks \
--state IN_PROGRESS \
--next-token K8VAMqKiP2Cf4xGkmH8GMyZrg0F8FUb+d10KTP9+P4pUb+8PhW+6MiXh4= \
--max-results 10
```

Eccezioni

```
ValidationException
InternalServerError
ThrottlingException
AccessDeniedException
```

Output

```
{
  "tasks": [
    {
      "state": "IN_PROGRESS",
      "tags": {},

```

```

        "taskId": "st-ficthmqoc2phtlef",
        "taskArn": "arn:aws:snow-device-management:us-west-2:000000000000:task/st-
ficthmqoc2phtlef"
    }
]
}

```

Applicazione di tag alle attività di gestione dei dispositivi di Snowball Edge o Snowball Edge

Per aggiungere o sostituire un tag per un dispositivo o per un'attività su un dispositivo, usa il `tag-resource` comando. Il `--tags` parametro accetta un elenco di coppie separate da virgole. `Key=Value`

Per applicare i tag a un dispositivo, utilizzate il seguente comando. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```

aws snow-device-management tag-resource \
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/
smd-fictbgr3rbcjeqa5 \
--tags Project=PrototypeA

```

Eccezioni

```

AccessDeniedException
InternalServerError
ResourceNotFoundException
ThrottlingException

```

Rimuovere i tag di Snowball Edge Device Management dalle attività o da Snowball Edge

Per rimuovere un tag da un dispositivo o da un'attività su un dispositivo, usa il `untag-resources` comando.

Per rimuovere i tag da un dispositivo, usa il seguente comando. Sostituisci ogni *user input placeholder* con le tue informazioni.

Comando

```
aws snow-device-management untag-resources \  
--resource-arn arn:aws:snow-device-management:us-west-2:123456789012:managed-device/  
smd-fictbgr3rbcjeqa5 \  
--tag-keys Project
```

Eccezioni

```
AccessDeniedException  
InternalServerError  
ResourceNotFoundException  
ThrottlingException
```

Aggiornamento del software sui dispositivi Snowball Edge

AWS ti avviserà quando sarà disponibile un nuovo software per Snowball Edge che possiedi. La notifica viene fornita tramite e-mail Health Dashboard e come CloudWatch evento. La notifica e-mail viene inviata da Amazon Web Services, Inc. all'indirizzo e-mail allegato all' AWS account utilizzato per ordinare il dispositivo Snowball Edge. Quando ricevi la notifica, segui le istruzioni riportate in questo argomento e scarica e installa l'aggiornamento il prima possibile per evitare l'interruzione dell'uso del dispositivo. Per ulteriori informazioni in merito Health Dashboard, consulta la [Guida AWS Health per l'utente](#). Per ulteriori informazioni sugli CloudWatch eventi, consulta la [Guida per l'utente di Amazon CloudWatch Events](#).

Puoi scaricare gli aggiornamenti software da AWS e installarli sui dispositivi Snowball Edge negli ambienti locali. Questi aggiornamenti avvengono in background. Puoi continuare a utilizzare i tuoi dispositivi normalmente mentre il software più recente viene scaricato in modo sicuro dal AWS dispositivo. Tuttavia, per applicare gli aggiornamenti scaricati, devi interrompere i carichi di lavoro sul dispositivo e riavviarlo.

Gli aggiornamenti software forniti da AWS per i dispositivi Snowball Edge/Snowball Edge (Appliance) sono software dell'appliance ai sensi della Sezione 9 dei Termini di servizio.

Gli aggiornamenti software vengono forniti esclusivamente allo scopo di installare gli aggiornamenti software sull'Appliance applicabile per conto di. AWS L'utente non potrà (o tenterà di) e non permetterà o autorizzerà terze parti a (o tenterà di) (i) effettuare copie degli aggiornamenti software diverse da quelle necessarie per installare gli aggiornamenti software sull'Apparecchio applicabile, o (ii) eludere o disabilitare qualsiasi funzionalità o misura degli aggiornamenti software, inclusa, a titolo esemplificativo, qualsiasi crittografia applicata all'aggiornamento del software. Una volta installati gli aggiornamenti software sull'Apparecchio applicabile, l'utente accetta di eliminare gli aggiornamenti software da tutti i supporti utilizzati per l'installazione degli aggiornamenti software sull'Apparecchio.

Warning

Si consiglia vivamente di sospendere tutte le attività sul dispositivo prima di installare l'aggiornamento. L'aggiornamento del dispositivo e il riavvio interromperanno l'esecuzione delle istanze e interromperanno le scritture sui bucket Amazon S3 locali.

Argomenti

- [Prerequisiti per l'aggiornamento del software sui dispositivi Snowball Edge](#)
- [Scaricamento degli aggiornamenti sui dispositivi Snowball Edge](#)
- [Installazione degli aggiornamenti sui dispositivi Snowball Edge](#)
- [Aggiornamento del certificato SSL sui dispositivi Snowball Edge](#)
- [Aggiornamento di Amazon Linux 2 AMIs su Snowball Edge](#)

Prerequisiti per l'aggiornamento del software sui dispositivi Snowball Edge

Prima di poter aggiornare il tuo dispositivo, è necessario soddisfare i seguenti prerequisiti:

- devi aver creato il tuo lavoro, devi avere il dispositivo locale e devi averlo sbloccato. Per ulteriori informazioni, consulta [Guida introduttiva a Snowball Edge](#).
- L'aggiornamento dei dispositivi Snowball Edge viene eseguito tramite il client Snowball Edge. La versione più recente del client Snowball Edge deve essere scaricata e installata su un computer dell'ambiente locale dotato di una connessione di rete al dispositivo che si desidera aggiornare. Per ulteriori informazioni, consulta [Utilizzo del client Snowball Edge](#).
- (Facoltativo) Ti consigliamo di configurare un profilo per il client Snowball Edge. Per ulteriori informazioni, vedere [Configurazione di un profilo per il client Snowball Edge](#).
- Per lo storage compatibile con Amazon S3 su Snowball Edge su dispositivi Snowball Edge in cluster, interrompi il servizio S3-Snow e disabilita l'avvio automatico. Per informazioni, consulta [Configurazione dello storage compatibile con Amazon S3 su Snowball Edge per l'avvio automatico tramite AWS OpsHub](#).

Note

Per i dispositivi in cluster, tutti i comandi devono essere eseguiti per ogni dispositivo.

Dopo aver completato queste attività, puoi scaricare e installare gli aggiornamenti per i dispositivi Snowball Edge.

Scaricamento degli aggiornamenti sui dispositivi Snowball Edge

Esistono due modi per scaricare un aggiornamento per Snowball Edge:

- È possibile attivare gli aggiornamenti manuali in qualsiasi momento utilizzando comandi specifici del client Snowball Edge.
- Puoi determinare in modo programmatico un momento per aggiornare automaticamente il dispositivo.

La procedura riportata di seguito illustra il processo di download manualmente degli aggiornamenti. Per informazioni sull'aggiornamento automatico del dispositivo Snowball Edge, consulta `configure-auto-update-strategy` [Aggiornamento di Snowball Edge](#).

Note

Se il dispositivo non ha accesso a Internet, puoi scaricare un file di aggiornamento utilizzando l'[GetSoftwareUpdates](#) API. Quindi, quando chiamate `download-updates` utilizzando il `uri` parametro, puntate a una posizione di file locale, come nell'esempio seguente.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Per i sistemi operativi Windows, formatta il valore del `uri` parametro come segue:

```
snowballEdge download-updates --uri file:/C:/path/to/local-update
```

Per verificare e scaricare gli aggiornamenti software Snowball Edge per dispositivi autonomi

1. Apri una finestra di terminale e assicurati che il dispositivo Snowball Edge sia sbloccato utilizzando il comando `describe-device`. Utilizza il comando `unlock-device` per sbloccarlo. Per ulteriori informazioni, consulta [Unlocking the Snowball Edge](#).
2. Quando il dispositivo è sbloccato, esegui il comando `snowballEdge check-for-updates`. Questo comando restituisce l'ultima versione disponibile del software Snowball Edge e anche la versione corrente installata sul dispositivo.
3. Se il software del dispositivo non è aggiornato, esegui il comando `snowballEdge download-updates`.

Note

Se il dispositivo non è connesso a Internet, scarica innanzitutto un file di aggiornamento utilizzando l'[GetSoftwareUpdates](#) API. Quindi esegui il `snowballEdge download-`

updates comando utilizzando il `uri` parametro con un percorso locale del file scaricato, come nell'esempio seguente.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

Per i sistemi operativi Windows, formatta il valore del `uri` parametro come segue:

```
snowballEdge download-updates --uri file:/C:/path/to/local-update
```

4. Puoi controllare lo stato del download con il comando `snowballEdge describe-device-software`. Durante il download di un aggiornamento, lo stato viene visualizzato utilizzando questo comando.

Example output del **describe-device-software** comando

```
Install State: Downloading
```

Per verificare e scaricare gli aggiornamenti software Snowball Edge per cluster di dispositivi

1. Apri una finestra di terminale e assicurati che tutti i dispositivi Snowball Edge del cluster siano sbloccati utilizzando il comando `snowballEdge describe-device`. Se i dispositivi sono bloccati, usa il `snowballEdge unlock-cluster` comando per sbloccarli. Per ulteriori informazioni, consulta [Unlocking the Snowball Edge](#).
2. Quando tutti i dispositivi del cluster sono sbloccati, esegui il comando per ogni dispositivo del cluster. `check-for-updates` Questo comando restituisce l'ultima versione disponibile del software Snowball Edge e anche la versione corrente installata sul dispositivo.

```
snowballEdge check-for-updates --unlock-code 29-character-unlock-code --manifest-file path/to/manifest/file.bin --endpoint https://ip-address-of-snow-device
```

 Note

Il codice di sblocco e il file manifest sono gli stessi per tutti i dispositivi del cluster.

Example del **check-for-updates** comando

```
{  
  "InstalledVersion" : "118",  
  "LatestVersion" : "119"  
}
```

Se il valore del LatestVersion nome è maggiore del valore del InstalledVersion nome, è disponibile un aggiornamento.

3. Per ogni dispositivo del cluster, usa il download-updates comando per scaricare l'aggiornamento.

```
snowballEdge download-updates --uri file:///tmp/local-update
```

 Note

Per i sistemi operativi Windows, formatta il valore del uri parametro come segue:

```
snowballEdge download-updates --uri file:/C:/path/to/local-update
```

4. Per verificare lo stato di questo download per ogni dispositivo del cluster, utilizzate il describe-device-software comando.

```
snowballEdge describe-device-software --unlock-code 29-character-unlock-code --  
manifest-file path/to/manifest/file.bin --endpoint https://ip-address-of-snow-  
device
```


Example dell'output del **describe-device-software** comando

```
{
  "InstalledVersion" : "118",
  "InstallingVersion" : "119",
  "InstallState" : "DOWNLOADED",
  "CertificateExpiry" : "Sat Mar 30 16:47:51 UTC 2024"
}
```

Se il valore del `InstallState` nome è `DOWNLOADED`, l'aggiornamento viene scaricato ed è disponibile per l'installazione.

Installazione degli aggiornamenti sui dispositivi Snowball Edge

Dopo aver scaricato gli aggiornamenti, è necessario installarli e riavviare il dispositivo affinché gli aggiornamenti abbiano effetto. La procedura seguente guida l'utente nell'installazione manuale degli aggiornamenti.

Per i cluster di dispositivi Snowball Edge, l'aggiornamento deve essere scaricato e installato per ogni dispositivo del cluster.

Note

Sospendi tutte le attività sul dispositivo prima di installare gli aggiornamenti software. L'installazione degli aggiornamenti interrompe l'esecuzione delle istanze e interrompe qualsiasi scrittura sui bucket Amazon S3 sul dispositivo. Ciò può causare la perdita di dati

Per installare gli aggiornamenti software già scaricati nella versione standalone Snowball Edge

1. Apri una finestra di terminale e assicurati che il dispositivo Snowball Edge sia sbloccato utilizzando il comando `describe-device`. Utilizza il comando `unlock-device` per sbloccarlo. Per ulteriori informazioni, consulta [Unlocking the Snowball Edge](#).
2. Esegui il `list-services` comando per visualizzare i servizi disponibili sul dispositivo. Il comando restituisce il servizio IDs di ogni servizio disponibile sul dispositivo.

```
snowballEdge list-services
```

Example dell'output del **list-services** comando

```
{
  "ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]
}
```

3. Per ogni ID di servizio identificato dal `list-services` comando, esegui il `describe-service` comando per visualizzarne lo stato. Utilizza queste informazioni per identificare i servizi da interrompere.

```
snowballEdge describe-service --service-id service-id
```

Example dell'output del **describe-service** comando

```
{
  "ServiceId" : "s3",
  "Status" : {
    "State" : "ACTIVE"
  },
  "Storage" : {
    "TotalSpaceBytes" : 99608745492480,
    "FreeSpaceBytes" : 99608744468480
  },
  "Endpoints" : [ {
    "Protocol" : "http",
    "Port" : 8080,
    "Host" : "192.0.2.0"
  }, {
    "Protocol" : "https",
    "Port" : 8443,
    "Host" : "192.0.2.0",
```

```
"CertificateAssociation" : {
  "CertificateArn" : "arn:aws:snowball-
device::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
}
} ]
}
```

Questo output mostra che il s3 servizio è attivo e deve essere interrotto utilizzando il `stop-service` comando.

- Utilizzate il `stop-service` comando per interrompere ogni servizio in cui il valore del State nome è ACTIVE nell'output del `list-services` comando. Se è in esecuzione più di un servizio, interrompi ciascuno prima di continuare.

Note

L'adattatore Amazon S3 EC2, AWS STS Amazon e i servizi IAM non possono essere interrotti. Se lo storage compatibile con Amazon S3 su Snowball Edge è in esecuzione, interrompilo prima di installare gli aggiornamenti. Lo storage compatibile con Amazon S3 su Snowball Edge ha come `s3-snow serviceId`

```
snowballEdge stop-service --service-id service-id --device-ip-addresses snow-
device-1-ip-address snow-device-device-2-ip-address snow-device-3-ip-address --
manifest-file path/to/manifest/file.bin --unlock-code 29-character-unlock-code --
endpoint https://snow-device-ip-address
```

Example dell'output del comando **stop-service**

Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS service using the `describe-service` command.

- Esegui il comando `snowballEdge install-updates`.

6. Puoi controllare lo stato dell'installazione con il comando `snowballEdge describe-device-software`. Durante l'installazione di un aggiornamento, lo stato viene visualizzato con questo comando.

Output di esempio

```
Install State: Installing //Possible values[NA, Installing, Requires Reboot]
```

Hai installato con successo un aggiornamento software per il tuo dispositivo Snowball Edge. L'installazione di un aggiornamento non applicherà automaticamente l'aggiornamento per il dispositivo. Per completare l'installazione dell'aggiornamento, il dispositivo deve essere riavviato.

 Warning

Il riavvio del dispositivo Snowball Edge senza interrompere tutte le attività in corso sul dispositivo può causare la perdita di dati.

7. Quando tutti i servizi sul dispositivo sono stati interrotti, riavvia il dispositivo, sblocca il dispositivo e riavvialo nuovamente. L'installazione degli aggiornamenti software scaricati viene completata. Per ulteriori informazioni sul riavvio del dispositivo, consulta [Riavvio di Snowball Edge](#) [Sblocco di Snowball Edge](#) [Sblocco di Snowball Edge](#) . Per ulteriori informazioni sullo sblocco del dispositivo, consulta [Sblocco di Snowball Edge](#) [Sblocco di Snowball Edge](#) .
8. Quando il dispositivo si accende dopo il secondo riavvio, sbloccalo.
9. Esegui il comando `check-for-updates`. Questo comando restituisce l'ultima versione disponibile del software Snowball Edge e anche la versione corrente installata sul dispositivo.

Per installare aggiornamenti software già scaricati su un cluster di dispositivi Snowball Edge

1. Per ogni dispositivo del cluster, esegui il `describe-device` comando per determinare se i dispositivi sono sbloccati. Se i dispositivi sono bloccati, usa il `unlock-cluster` comando per sbloccarli. Per ulteriori informazioni, consulta [Unlocking the Snowball Edge](#).
2. Per ogni dispositivo del cluster, esegui il `list-services` comando per visualizzare i servizi disponibili sul dispositivo. Il comando restituisce il servizio IDs di ogni servizio disponibile sul dispositivo.

```
snowballEdge list-services
```

Example dell'output del **list-services** comando

```
{
  "ServiceIds" : [ "greengrass", "fileinterface", "s3", "ec2", "s3-snow" ]
}
```

3. Per ogni ID di servizio identificato dal **list-services** comando, esegui il **describe-service** comando per visualizzarne lo stato. Utilizza queste informazioni per identificare i servizi da interrompere.

```
snowballEdge describe-service --service-id service-id
```

Example dell'output del **describe-service** comando

```
{
  "ServiceId" : "s3",
  "Status" : {
    "State" : "ACTIVE"
  },
  "Storage" : {
    "TotalSpaceBytes" : 99608745492480,
    "FreeSpaceBytes" : 99608744468480
  },
  "Endpoints" : [ {
    "Protocol" : "http",
    "Port" : 8080,
    "Host" : "192.0.2.0"
  }, {
    "Protocol" : "https",
    "Port" : 8443,
    "Host" : "192.0.2.0",
    "CertificateAssociation" : {
      "CertificateArn" : "arn:aws:snowball-
device:::certificate/6d955EXAMPLEdb71798146EXAMPLE3f0"
    }
  }
}
```

```
} ]
}
```

Questo output mostra che il s3 servizio è attivo e deve essere interrotto utilizzando il `stop-service` comando.

4. Per ogni dispositivo del cluster, utilizzate il `stop-service` comando per interrompere ogni servizio in cui il valore del State nome si trova ACTIVE nell'output del `list-services` comando. Se sono in esecuzione più servizi, interrompi ciascuno di essi prima di continuare.

Note

L'adattatore Amazon S3 EC2, AWS STS Amazon e i servizi IAM non possono essere interrotti. Se lo storage compatibile con Amazon S3 su Snowball Edge è in esecuzione, interrompilo prima di installare gli aggiornamenti. Lo storage compatibile con Amazon S3 su Snowball Edge ha come `s3-snow serviceId`

```
snowballEdge stop-service --service-id service-id --device-ip-addresses snow-device-1-ip-address snow-device-device-2-ip-address snow-device-3-ip-address --manifest-file path/to/manifest/file.bin --unlock-code 29-character-unlock-code --endpoint https://snow-device-ip-address
```

Example dell'output del comando **stop-service**

Stopping the AWS service on your Snowball Edge. You can determine the status of the AWS service using the `describe-service` command.

5. Per ogni dispositivo del cluster, esegui il `install-updates` comando.

```
snowballEdge install-updates
```

6. Puoi controllare lo stato dell'installazione con il comando `describe-device-software`.

```
snowballEdge describe-device-software
```

Example dell'output del **describe-device-service** comando

```
Install State: Installing //Possible values[NA, Installing, Requires Reboot]
```

In tal caso `Requires Reboot`, `Install State` l'aggiornamento software per il dispositivo Snowball Edge è stato installato correttamente. L'installazione di un aggiornamento non applicherà automaticamente l'aggiornamento per il dispositivo. Per completare l'installazione dell'aggiornamento, il dispositivo deve essere riavviato.

 Warning

Il riavvio del dispositivo Snowball Edge senza interrompere tutte le attività sul dispositivo può causare la perdita di dati.

7. Riavvia tutti i dispositivi del cluster, sblocca il cluster e riavvia nuovamente tutti i dispositivi del cluster. Questo completa l'installazione degli aggiornamenti software scaricati. Per ulteriori informazioni sul riavvio dei dispositivi, consulta [Riavvio](#) di Snowball Edge. Per ulteriori informazioni sullo sblocco del cluster di dispositivi, consulta [Sblocco di Snowball](#) Edge.
8. Dopo che ogni dispositivo del cluster è stato riavviato due volte, sblocca il cluster e usa il `check-for-updates` comando per verificare che il dispositivo sia stato aggiornato. Questo comando restituisce l'ultima versione disponibile del software Snowball Edge e anche la versione corrente installata sul dispositivo. Se la versione corrente e l'ultima versione disponibile coincidono, il dispositivo è stato aggiornato correttamente.

Ora hai aggiornato con successo Snowball Edge o il cluster di dispositivi e hai confermato l'aggiornamento alla versione più recente del software Snowball Edge.

Aggiornamento del certificato SSL sui dispositivi Snowball Edge

Se prevedi di conservare Snowball Edge per più di 360 giorni, dovrai aggiornare il certificato Secure Sockets Layer (SSL) sul dispositivo per evitare interruzioni nell'utilizzo del dispositivo. Se il certificato scade, non potrai più utilizzare il dispositivo e dovrai restituirlo. AWS

AWS riceverai una notifica 30 giorni prima della scadenza del certificato SSL per Snowball Edge in tuo possesso. La notifica viene fornita tramite e-mail e Health Dashboard come evento. AWS CloudTrail La notifica e-mail viene inviata da Amazon Web Services, Inc. all'indirizzo e-mail allegato all' AWS account utilizzato per ordinare il dispositivo Snowball Edge. Quando ricevi la notifica, segui le istruzioni riportate in questo argomento e richiedi un aggiornamento il prima possibile per evitare l'interruzione dell'uso del dispositivo. Per ulteriori informazioni in merito Health Dashboard, consulta la [Guida AWS Health per l'utente](#). Per ulteriori informazioni sugli CloudWatch eventi, consulta [Lavorare con la cronologia CloudTrail degli eventi](#).

L'aggiornamento del certificato SSL viene effettuato tramite il client Snowball Edge. La versione più recente del client Snowball Edge deve essere scaricata e installata su un computer dell'ambiente locale dotato di una connessione di rete al dispositivo che si desidera aggiornare. Per ulteriori informazioni, vedere [Utilizzo del client Snowball Edge con il client AWS](#) Edge.

Questo argomento spiega come determinare quando scadrà il certificato e come aggiornare il dispositivo.

1. Usa il `snowballEdge describe-device-software` comando per determinare quando scadrà il certificato. Nell'output del comando, il valore di `CertificateExpiry` include la data e l'ora di scadenza del certificato.

Example dell'**describe-device-software**output

```
Installed version: 101
Installing version: 102
Install State: Downloading
CertificateExpiry : Thur Jan 01 00:00:00 UTC 1970
```

2. Contatta Supporto e richiedi un aggiornamento del certificato SSL.
3. Supporto fornirà un file di aggiornamento. [Scarica](#) e [installa](#) il file di aggiornamento.
- 4.

Aggiornamento di Amazon Linux 2 AMIs su Snowball Edge

Come best practice per la sicurezza, mantieni Amazon Linux 2 AMIs up-to-date su Snowball Edge. Controlla regolarmente l'[AMI Amazon Linux 2 \(HVM\), tipo di volume SSD \(64 bit x86\)](#) nella sezione per gli Marketplace AWS aggiornamenti. Quando identifichi la necessità di aggiornare la tua AMI, importa l'immagine Amazon Linux 2 più recente sul dispositivo Snow. Vedi [Importazione di un'immagine nel tuo dispositivo come EC2 AMI compatibile con Amazon](#).

Puoi anche ottenere l'ID di immagine Amazon Linux 2 più recente usando il `ssm get-parameters` comando in AWS CLI.

```
aws ssm get-parameters --names /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 --query 'Parameters[0].[Value]' --region your-region
```

Il comando restituisce l'ID immagine più recente dell'AMI. Per esempio:

```
ami-0ccb473bada910e74
```

Informazioni sui job di Snowball Edge

Un job in AWS Snowball Edge è un'unità di lavoro discreta, definita al momento della creazione nella console o nell'API di gestione dei lavori. Il AWS Snowball Edge dispositivo offre tre diversi tipi di lavoro, tutti dotati di funzionalità di archiviazione e calcolo locali. Questa funzionalità utilizza l'interfaccia NFS o l'interfaccia Amazon S3 per leggere e scrivere dati. Attiva funzioni Lambda basate sulle azioni API degli oggetti PUT di Amazon S3 eseguite localmente sul dispositivo. AWS Snowball Edge

- [Lavori per importare dati in Amazon S3 utilizzando un dispositivo Snowball Edge](#)— Il trasferimento di 210 TB o meno di dati locali copiati su un singolo dispositivo e poi trasferiti in Amazon S3. Per i lavori di importazione, i dispositivi Snowball e i job hanno una one-to-one relazione. Ogni processo include un dispositivo associato. Se hai bisogno di importare altri dati, puoi creare nuovi processi di importazione o clonare quelli esistenti. Quando restituisce un dispositivo di questo tipo di lavoro, i dati in esso contenuti vengono importati in Amazon S3.
- [Lavori per esportare dati da Amazon S3 utilizzando un dispositivo Snowball Edge](#)— Il trasferimento di qualsiasi quantità di dati (che si trovano in Amazon S3), copiati su un numero qualsiasi di dispositivi Snowball Edge e quindi spostati su un AWS Snowball Edge dispositivo alla volta nella destinazione dati locale. Quando crei un processo di esportazione, viene suddiviso in diverse parti. Ogni parte del lavoro non ha una dimensione superiore a 210 TB e a ciascuna parte del lavoro è associato esattamente un AWS Snowball Edge dispositivo. Quando restituisce un dispositivo di questo tipo di processo, viene cancellato.
- [Informazioni sull'utilizzo dei dispositivi Snowball Edge per fornire funzionalità di elaborazione e archiviazione locali](#)— Questi lavori coinvolgono uno AWS Snowball Edge o più dispositivi utilizzati in un cluster. Questi processi non iniziano con i dati nei loro bucket, come nel caso di un processo di esportazione, e alla fine non possono importare i dati in Amazon S3 come se si trattasse di un processo di importazione. Quando restituisce un dispositivo di questo tipo di processo, viene cancellato. Con questo tipo di processo, puoi anche creare un cluster di dispositivi. Un cluster migliora la durabilità dello storage locale e puoi aumentare o diminuire le risorse con la capacità di storage locale.

Nelle regioni in cui Lambda non è disponibile, questo tipo di lavoro è denominato solo archiviazione locale.

Dettagli sulle offerte di lavoro Snowball Edge

Prima di creare un lavoro, assicurati che i [prerequisiti](#) siano soddisfatti. Ogni processo è definito dai dettagli specificati al momento della creazione. Nella seguente tabella sono descritti tutti i dettagli di un processo.

Identificatore della console	Identificatore API	Descrizione dettagliata
Nome processo	Description	Nome del processo, contenente caratteri alfanumerici, spazi e qualsiasi carattere speciale Unicode.
Tipo di processo	JobType	Tipo di processo, importazione, esportazione o storage ed elaborazione locale.
Job ID	JobId	Etichetta univoca composta da 39 caratteri che identifica il processo. L'ID processo viene visualizzato nella parte inferiore dell'etichetta di spedizione nella visualizzazione E Ink e nel nome del file manifest di un processo.
Indirizzo	AddressId	L'indirizzo di consegna del dispositivo. Nel caso dell'API, questo è l'ID per il tipo di dati dell'indirizzo.
Data di creazione	CreationDate	Data in cui è stato creato il processo.
Velocità di spedizione	ShippingOption	Opzioni di velocità basate sulla regione. Per ulteriori informazioni, consulta Velocità

Identificatore della console	Identificatore API	Descrizione dettagliata
		di spedizione per Snowball Edge.
IAM role ARN (ARN del ruolo IAM)	RoleARN	Questo Amazon Resource Name (ARN) è il ruolo AWS Identity and Access Management (IAM) creato durante la creazione di lavoro con autorizzazioni di scrittura per i tuoi bucket Amazon S3. Il processo di creazione è automatico e il ruolo IAM che autorizzi AWS Snowball Edge ad assumere viene utilizzato solo per copiare i dati tra i bucket S3 e lo Snowball. Per ulteriori informazioni, consulta Autorizzazioni necessarie per utilizzare la console AWS Snowball Edge.
AWS KMS chiave	KmsKeyARN	In AWS Snowball Edge, AWS Key Management Service (AWS KMS) crittografa le chiavi di ogni Snowball. Quando crei il tuo lavoro, scegli o crei anche un ARN per una chiave di AWS KMS crittografia di tua proprietà. Per ulteriori informazioni, consulta AWS Key Management Service nel AWS Snowball Edge.

Identificatore della console	Identificatore API	Descrizione dettagliata
Capacità di Snowball	<code>SnowballCapacityPreference</code>	La capacità di archiviazione del AWS Snowball Edge dispositivo ordinato in questo lavoro. La dimensione disponibile dipende dalla tua Regione AWS.
Servizio di storage	N/D	Il servizio AWS di storage associato a questo lavoro, in questo caso Amazon S3.
Risorse	<code>Resources</code>	Le risorse del servizio di AWS storage associate al tuo lavoro. In questo caso, si tratta dei bucket Amazon S3 verso i quali i dati vengono trasferiti o da cui vengono trasferiti.
Tipo di processo	<code>JobType</code>	Tipo di processo, importazione, esportazione o storage ed elaborazione locale.
Tipo di Snowball	<code>SnowballType</code>	Il tipo di dispositivo Snowball Edge ordinato in questo processo.
ID cluster	<code>ClusterId</code>	Etichetta univoca composta da 39 caratteri che identifica il cluster.

Stati delle offerte di lavoro Snowball Edge

Ogni processo AWS Snowball Edge del dispositivo ha uno stato, che cambia per indicare lo stato corrente del lavoro. Queste informazioni sullo stato del processo non riflettono l'integrità, lo stato di elaborazione corrente o lo storage utilizzato per i dispositivi associati.

Per visualizzare lo stato di un lavoro

1. Accedere a [Console di gestione della famiglia di servizi AWS Snow](#).
2. Nella dashboard Job, scegli il lavoro.
3. Fai clic sul nome del lavoro all'interno della console.
4. Il riquadro Job Status si trova nella parte superiore e riflette lo stato del lavoro.

AWS Snowball Edge stati dei processi del dispositivo

Identificatore della console	Identificatore API	Descrizione dello stato
Job created (Processo creato)	New	Il processo è appena stato creato. Questo stato è l'unico durante il quale è possibile annullare un processo o parti di esso, se si tratta di un processo di esportazione.
Preparazione dell'apparecchiatura	PreparingAppliance	AWS sta preparand o un dispositivo per il tuo lavoro.
Exporting (Esportazione)	InProgress	AWS sta esportando i tuoi dati da Amazon S3 su un dispositivo.
Preparing shipment (Preparazione spedizione)	PreparingShipment	AWS si sta preparand o a spedirti un dispositivo. Le informazioni di tracciabilità della spedizione previste vengono fornite ai clienti nello stato.

Identificatore della console	Identificatore API	Descrizione dello stato
In transit to you (In transito verso l'utente)	InTransitToCustomer	Il dispositivo è stato spedito all'indirizzo fornito durante la creazione del processo.
Delivered to you (Consegnato all'utente)	WithCustomer	Il dispositivo è arrivato all'indirizzo fornito durante la creazione del processo.
In transit verso AWS	InTransitToAWS	Hai rispedito il dispositivo a AWS.
Al centro di smistamento	WithAWSSortingFacility	Il dispositivo per questo processo si trova presso il nostro centro di smistamento. Qualsiasi elaborazione aggiuntiva per i lavori di importazione in Amazon S3 inizierà presto, in genere entro 2 giorni.
In AWS	WithAWS	La tua spedizione è arrivata a AWS. Se stai importando i dati, l'importazione in genere inizia nell'arco di un giorno dall'arrivo.

Identificatore della console	Identificatore API	Descrizione dello stato
Importing (Importazione)	InProgress	AWS sta importando i tuoi dati in Amazon Simple Storage Service (Amazon S3).
Completato	Complete	Il processo o una parte del processo è stato completato.
Annullato	Cancelled	Il processo è stato annullato.

Stati dei job del cluster Snowball Edge

Ogni cluster ha uno stato che cambia per indicare lo stato di avanzamento generale corrente del cluster. Ogni singolo nodo del cluster ha un proprio status di processo.

Queste informazioni sullo stato del cluster non riflettono l'integrità, lo stato di elaborazione corrente o lo storage utilizzato per il cluster o i nodi.

Identificatore della console	Identificatore API	Descrizione dello stato
Awaiting Quorum (In attesa del quorum)	AwaitingQuorum	Il cluster non è stato ancora creato, perché non ci sono abbastanza nodi per iniziare a elaborare la richiesta del cluster. Affinché un cluster possa essere creato, deve avere almeno cinque nodi.

Identificatore della console	Identificatore API	Descrizione dello stato
In attesa	Pending	Il cluster è stato creato e stiamo preparando i nodi per la spedizione. È possibile tenere traccia dello stato di ciascun nodo con lo stato del processo di quel nodo.
Delivered to you (Consegnato all'utente)	InUse	Almeno un nodo del cluster si trova all'indirizzo fornito durante la creazione del processo.
Completato	Complete	Tutti i nodi del cluster sono stati restituiti AWS.
Annullato	Cancelled	La richiesta di creare un cluster è stata annullata. Le richieste del cluster possono essere annullate solamente prima di entrare nello stato In sospeso.

Lavori per importare dati in Amazon S3 utilizzando un dispositivo Snowball Edge

Con un processo di importazione, i dati vengono copiati AWS Snowball Edge sul dispositivo con l'adattatore Amazon S3 integrato o il punto di montaggio NFS. L'origine dati per un processo di importazione deve essere locale. In altre parole, i dispositivi di storage che contengono i dati da trasferire devono essere fisicamente situati presso l'indirizzo fornito al momento della creazione del processo.

Quando importi file, ogni file diventa un oggetto in Amazon S3 e ogni directory diventa un prefisso. Se importi i dati in un bucket esistente, tutti gli oggetti esistenti con lo stesso nome degli oggetti appena importate sono sovrascritti. Il tipo di processo importazione offre anche la funzionalità di storage ed elaborazione locale. Questa funzionalità utilizza l'interfaccia NFS o l'adattatore Amazon S3 per leggere e scrivere dati e attiva le funzioni Lambda basate sulle azioni API degli oggetti Amazon S3 PUT eseguite localmente sul dispositivo. AWS Snowball Edge

Quando tutti i dati sono stati importati nei bucket Amazon S3 specificati nel Cloud AWS, AWS esegue una cancellazione completa del dispositivo. Questa cancellazione segue gli standard NIST 800-88.

Una volta completata l'importazione, è possibile scaricare il rapporto del processo. Questo rapporto indica tutti gli oggetti che non sono stati importati. Ulteriori informazioni sono disponibili nei log delle operazioni riuscite e non riuscite.

Important

Non eliminare le copie locali dei dati trasferiti finché non hai verificato i risultati nel rapporto di completamento del processo ed esaminato i log di importazione.

Lavori per esportare dati da Amazon S3 utilizzando un dispositivo Snowball Edge

Note

I tag e i metadati NON sono attualmente supportati, in altre parole, tutti i tag e i metadati verrebbero rimossi durante l'esportazione di oggetti dai bucket S3.

La tua fonte di dati per un processo di esportazione è uno o più bucket Amazon S3. Dopo aver trasferito i dati per una parte del lavoro da Amazon S3 a un AWS Snowball Edge dispositivo, puoi scaricare un rapporto sul lavoro. In questo rapporto vengono indicati gli oggetti che non sono stati trasferiti nel dispositivo. Ulteriori informazioni sono disponibili nei log delle operazioni riuscite e non riuscite del processo.

Puoi esportare un numero qualsiasi di oggetti per ogni processo di esportazione, utilizzando tutti i dispositivi necessari per completare il trasferimento. Ogni AWS Snowball Edge dispositivo per le parti del lavoro di un processo di esportazione viene consegnato uno dopo l'altro, mentre i dispositivi successivi vengono spediti all'utente dopo che la parte del lavoro precedente è passata AWS allo stato In transit verso.

Quando copi oggetti nella destinazione dei dati locale da un dispositivo utilizzando l'adattatore Amazon S3 o il punto di montaggio NFS, tali oggetti vengono salvati come file. Se copi gli oggetti in un percorso che contiene già dei file, i file esistenti con lo stesso nome vengono sovrascritti. Il tipo di processo esportazione offre anche la funzionalità di storage ed elaborazione locale. Questa funzionalità utilizza l'interfaccia NFS o l'adattatore Amazon S3 per leggere e scrivere dati e attiva le funzioni Lambda basate sulle azioni API degli oggetti Amazon S3 PUT eseguite localmente sul dispositivo. AWS Snowball Edge

Quando AWS riceviamo un dispositivo restituito, lo cancelliamo completamente, seguendo gli standard NIST 800-88.

Important

I dati che desideri esportare su un dispositivo Snow devono trovarsi in Amazon S3. Tutti i dati Amazon Glacier che intendi esportare sul dispositivo Snow dovranno essere scongelati o spostati nella classe di storage S3 prima di poter essere esportati. Eseguite questa operazione prima di creare il processo di esportazione di Snow.

Non modificare, aggiornare o eliminare gli oggetti Amazon S3 esportati finché non avrai verificato che tutti i contenuti dell'intero processo siano stati copiati nella destinazione dei dati locale.

Quando crei un processo di esportazione, puoi esportare un intero bucket Amazon S3 o una gamma specifica di chiavi di oggetti.

Utilizzo delle chiavi oggetto Amazon S3 per l'esportazione di dati su un dispositivo Snowball Edge

Quando crei un processo di esportazione nella [Console di gestione della famiglia di servizi AWS Snowo](#) con l'API di gestione dei lavori, puoi esportare un intero bucket Amazon S3 o una gamma specifica di chiavi di oggetti. I nomi delle chiavi degli oggetti identificano in modo univoco gli oggetti in un bucket. Se esporti un'intervallo, definisci la lunghezza dell'intervallo fornendo un intervallo inclusivo iniziale, un intervallo inclusivo finale o entrambi.

Gli intervalli sono binari UTF-8 ordinati. I dati binari UTF-8 sono ordinati nel modo seguente:

- I numeri da 0 a 9 precedono i caratteri inglesi maiuscoli e minuscoli.
- I caratteri inglesi maiuscoli vengono prima di tutti i caratteri inglesi minuscoli.
- I caratteri inglesi minuscoli vengono per ultimi quando ordinati rispetto ai caratteri inglesi maiuscoli e i numeri.
- I caratteri speciali vengono ordinati tra gli altri set di caratteri.

[Per ulteriori informazioni sulle specifiche di UTF-8, vedi UTF-8 su Wikipedia.](#)

Esempi di utilizzo delle chiavi oggetto Amazon S3 durante l'esportazione di dati su un dispositivo Snowball Edge

Supponiamo di avere un bucket contenente i seguenti oggetti e prefissi, ordinati in ordine binario UTF-8:

- 01
- Aardvark
- Aardwolf
- Aasvogel/apple
- Aasvogel/arrow/object1
- Aasvogel/arrow/object2
- Aasvogel/banana
- Aasvogel/banker/object1
- Aasvogel/banker/object2
- Aasvogel/cherry

- Banana
- Car

Inizio dell'intervallo specificato	Fine dell'intervallo specificato	Oggetti dell'intervallo che verranno esportati
(nessuno)	(nessuno)	Tutti gli oggetti nel bucket
(nessuno)	Aasvogel	01 Aardvark Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry
(nessuno)	Aasvogel/banana	01 Aardvark

Inizio dell'intervallo specificato	Fine dell'intervallo specificato	Oggetti dell'intervallo che verranno esportati
		Aardwolf
		Aasvogel/apple
		Aasvogel/arrow/object1
		Aasvogel/arrow/object2
		Aasvogel/banana
Aasvogel	(nessuno)	Aasvogel/apple
		Aasvogel/arrow/object1
		Aasvogel/arrow/object2
		Aasvogel/banana
		Aasvogel/banker/object1
		Aasvogel/banker/object2
		Aasvogel/cherry
		Banana
		Car

Inizio dell'intervallo specificato	Fine dell'intervallo specificato	Oggetti dell'intervallo che verranno esportati
Aardwolf	(nessuno)	Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry Banana Car

Inizio dell'intervallo specificato	Fine dell'intervallo specificato	Oggetti dell'intervallo che verranno esportati
Aar	(nessuno)	Aardvark Aardwolf Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry Banana Car

Inizio dell'intervallo specificato	Fine dell'intervallo specificato	Oggetti dell'intervallo che verranno esportati
car	(nessuno)	Nessun oggetto viene esportato e viene visualizzato un messaggio di errore quando cerchi creare il processo. Nota che l'auto è ordinata sotto Auto in base ai valori binari UTF-8.
Aar	Aarr	Aardvark Aardwolf
AASVogel/Arrow	AASVogel/Arrox	Aasvogel/arrow/object1 Aasvogel/arrow/object2

Inizio dell'intervallo specificato	Fine dell'intervallo specificato	Oggetti dell'intervallo che verranno esportati
Aasvogel/apple	Aasvogel/banana	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana
Aasvogel/apple	Aasvogel/Banchiere	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2

Inizio dell'intervallo specificato	Fine dell'intervallo specificato	Oggetti dell'intervallo che verranno esportati
Aasvogel/apple	Aasvogel/cherry	Aasvogel/apple Aasvogel/arrow/object1 Aasvogel/arrow/object2 Aasvogel/banana Aasvogel/banker/object1 Aasvogel/banker/object2 Aasvogel/cherry

Supponiamo di avere questi tre bucket e di voler copiare tutti gli oggetti dalla cartella 2.

- s3://bucket/folder1/
- s3://bucket/folder2/
- s3://bucket/folder3/

Inizio dell'intervallo specificato	Fine dell'intervallo specificato	Oggetti dell'intervallo che verranno esportati
cartella2/	cartella 2/	Tutti gli oggetti in bucket folder2.

Procedure consigliate per lavori di esportazione di dati da Amazon S3 a un dispositivo Snowball Edge

- Assicurati che i dati siano in Amazon S3, esegui il batch di file di piccole dimensioni prima di ordinare il lavoro
- Assicurati che gli intervalli chiave siano specificati nella definizione del processo di esportazione se hai milioni di oggetti nel tuo bucket
- Aggiorna le chiavi oggetto per rimuovere la barra nel nome poiché gli oggetti con barre finali nei nomi (/o\) non vengono trasferiti su Snowball Edge
- Per i bucket S3, la lunghezza massima degli oggetti è di 255 caratteri.
- Per i bucket S3 abilitati alla versione, viene esportata solo la versione corrente degli oggetti.
- I marker di eliminazione non vengono esportati.

Informazioni sull'utilizzo dei dispositivi Snowball Edge per fornire funzionalità di elaborazione e archiviazione locali

I processi di elaborazione e archiviazione locali consentono di utilizzare lo storage compatibile con Amazon S3 su Snowball Edge localmente, senza una connessione Internet. Non puoi esportare dati da Amazon S3 al dispositivo o importare dati in Amazon S3 quando il dispositivo viene restituito.

Argomenti

- [Informazioni sui lavori di archiviazione locale dei dati sui dispositivi Snowball Edge](#)
- [Informazioni sui lavori che forniscono archiviazione locale su un cluster di dispositivi Snowball Edge](#)

Informazioni sui lavori di archiviazione locale dei dati sui dispositivi Snowball Edge

Puoi leggere e scrivere oggetti su un AWS Snowball Edge dispositivo utilizzando lo storage compatibile con Amazon S3 su Snowball Edge o sull'adattatore S3. Quando ordini un dispositivo, se scegli di utilizzare l'adattatore S3, scegli anche quali bucket Amazon S3 saranno inclusi nel dispositivo al momento della ricezione. Se scegli di utilizzare lo storage compatibile con Amazon S3 su Snowball Edge, al momento della ricezione il dispositivo non include bucket Amazon S3.

Puoi creare bucket Amazon S3 sui dispositivi Snowball Edge per archiviare e recuperare oggetti in locale per applicazioni che richiedono l'accesso locale ai dati, l'elaborazione locale dei dati e la residenza dei dati. Lo storage compatibile con Amazon S3 su Snowball Edge offre una nuova classe di storage che utilizza Amazon S3 ed è progettata per archiviare i dati in modo duraturo e ridondante su più dispositivi APIs Snowball Edge. Sui bucket Snowball Edge puoi utilizzare le stesse APIs funzionalità che usi su Amazon S3, tra cui le policy del ciclo di vita dei bucket, la crittografia e l'etichettatura. Quando il dispositivo o i dispositivi vengono restituiti AWS, tutti i dati creati o archiviati nello storage compatibile con Amazon S3 su Snowball Edge vengono cancellati. Per ulteriori informazioni, consulta [Local Compute and Storage Only Jobs](#).

Per ulteriori informazioni, consulta lo [storage compatibile con Amazon S3 su Snowball Edge](#) in questa guida.

Quando hai finito di utilizzare il dispositivo, ripristinalo e il dispositivo verrà cancellato. AWS Questa cancellazione rispetta gli standard 800-88 della National Institute of Standards and Technology (NIST).

Informazioni sui lavori che forniscono archiviazione locale su un cluster di dispositivi Snowball Edge

Un cluster è un raggruppamento logico di dispositivi Snowball Edge, in gruppi da 3 a 16 dispositivi. Un cluster viene creato come un singolo processo, il che offre maggiore durata e dimensioni di archiviazione rispetto ad altre offerte di AWS Snowball Edge lavoro. Per ulteriori informazioni sui job del cluster, consulta la [panoramica sul clustering](#) in questa guida.

Procedure consigliate per l'utilizzo di un dispositivo Snowball Edge

Per ottenere il massimo vantaggio e soddisfazione dal tuo AWS Snowball Edge dispositivo, ti consigliamo di seguire queste best practice.

Consigli di sicurezza per Snowball Edge

Di seguito sono riportati consigli e best practice per mantenere la sicurezza durante l'utilizzo di un AWS Snowball Edge dispositivo.

Sicurezza generale

- Se noti qualcosa che sembra sospetto nel AWS Snowball Edge dispositivo, non collegarlo alla rete interna. Contattaci [Supporto AWS](#) invece e ti verrà spedito un nuovo AWS Snowball Edge dispositivo.
- Ti consigliamo di non salvare una copia del codice di sblocco nella stessa posizione sulla workstation in cui è stato inserito il manifesto del lavoro. Il salvataggio di questi dati in luoghi diversi aiuta a impedire l'accesso al dispositivo da parte di persone non autorizzate. AWS Snowball Edge Ad esempio, puoi salvare una copia del manifest nel server locale e mandare a un utente per e-mail il codice che sblocca il dispositivo. Questo approccio limita l'accesso al AWS Snowball Edge dispositivo alle persone che hanno accesso ai file salvati sul server e all'indirizzo e-mail dell'utente.
- Le credenziali visualizzate, quando si eseguono i list-access-keys comandi get-secret-access-key del client Snowball Edge, sono un paio di chiavi di accesso utilizzate per accedere al dispositivo.

Queste chiavi sono associate solo al processo e alle risorse locali del dispositivo. Non vengono mappate al tuo Account AWS o a nessun altro. Account AWS Se provi a utilizzare queste chiavi per accedere ai servizi e alle risorse di Cloud AWS, falliranno perché funzionano solo per le risorse locali associate al tuo lavoro.

- Se ritieni che le tue credenziali siano andate perdute o siano state compromesse, richiedi un nuovo file manifest e sblocca il codice seguendo la procedura per aggiornare il certificato SSL del dispositivo. Consultare [Aggiornamento del certificato SSL sui dispositivi Snowball Edge](#).

Per informazioni su come utilizzare le policy AWS Identity and Access Management (IAM) per controllare l'accesso, consulta. [AWS-Policy gestite \(predefinite\) per AWS Snowball Edge](#)

Sicurezza di rete

- Ti consigliamo di utilizzare un solo metodo alla volta per leggere e scrivere dati in un bucket locale su un AWS Snowball Edge dispositivo.
- Per evitare di danneggiare i dati, non scollegare il AWS Snowball Edge dispositivo o modificarne le impostazioni di rete durante il trasferimento dei dati.
- I file su cui si sta scrivendo sul dispositivo devono trovarsi in uno stato statico. I file modificati durante la scrittura possono causare conflitti di lettura/scrittura.
- Per ulteriori informazioni sul miglioramento delle prestazioni del AWS Snowball Edge dispositivo, consulta [Consigli per ottimizzare le prestazioni di trasferimento dei dati da o verso uno Snowball Edge](#)

Procedure consigliate per la gestione delle risorse di Snowball Edge

Prendi in considerazione le seguenti best practice per la gestione di lavori e risorse sul tuo AWS Snowball Edge dispositivo.

- I 15 giorni gratuiti per eseguire il trasferimento dei dati in locale iniziano il giorno successivo all'arrivo del AWS Snowball Edge dispositivo al data center. Questo vale solo per i tipi di dispositivi Snowball Edge.
- Lo stato Job created (Processo creato) è l'unico in cui è possibile annullare un processo. Quando un lavoro passa a uno stato diverso, non è possibile annullarlo. Questo vale per i cluster.
- Per i lavori di importazione, non eliminare le copie locali dei dati trasferiti fino a quando l'importazione in Amazon S3 non è stata completata. Come parte del processo, accertarsi di verificare i risultati del trasferimento dati.

Consigli per ottimizzare le prestazioni di trasferimento dei dati da o verso uno Snowball Edge

Note

Le prestazioni di trasferimento dei dati sperimentate variano in base all'ambiente di rete, ai sistemi operativi, al metodo di copia, al protocollo, alle prestazioni di lettura dei dati di

origine e alle caratteristiche del set di dati, come la dimensione del file. Per determinare con precisione le velocità e i tempi di trasferimento dei dati, ti consigliamo di misurare le prestazioni mediante proof-of-concept test nel tuo ambiente.

Di seguito, puoi trovare consigli e informazioni sulle prestazioni AWS Snowball Edge del dispositivo. Questa sezione descrive le prestazioni in termini generali, poiché gli ambienti locali hanno un modo diverso di fare le cose: diverse tecnologie di rete, hardware diversi, sistemi operativi diversi, procedure diverse e così via.

La tabella seguente illustra in che modo la velocità di trasferimento della rete influisce sul tempo necessario per riempire di dati un dispositivo Snowball Edge. Il trasferimento di file più piccoli riduce la velocità di trasferimento a causa dell'aumento del sovraccarico. Se hai molti file di piccole dimensioni, ti consigliamo di comprimerli in archivi più grandi prima di trasferirli su un dispositivo Snowball Edge.

Velocità (MB/s)	Tempo di trasferimento di 82 TB
800	1.22 giorni
450	2.11 giorni
400	2.37 giorni
300	3.16 giorni
277	3.42 giorni
200	4.75 giorni
100	9.49 giorni
60	15.53 giorni
30	31.06 giorni
10	85.42 giorni

Per fornire indicazioni significative sulle prestazioni, le sezioni seguenti descrivono come determinare quando utilizzare il AWS Snowball Edge dispositivo e come ottenere il massimo dal servizio.

Le seguenti pratiche sono altamente consigliate, poiché hanno il maggiore impatto sul miglioramento delle prestazioni del trasferimento dei dati:

- Ti consigliamo un massimo di 500.000 file o directory all'interno di ogni directory.
- Si consiglia che tutti i file trasferiti su un dispositivo Snowball Edge abbiano una dimensione non inferiore a 1 MB.
- Se hai molti file di dimensioni inferiori a 1 MB, ti consigliamo di comprimerli in archivi più grandi prima di trasferirli su un dispositivo Snowball Edge.

Miglioramento della velocità di trasferimento dei dati da e verso uno Snowball Edge

Uno dei modi migliori per migliorare le prestazioni di un AWS Snowball Edge dispositivo consiste nell'accelerare il trasferimento dei dati da e verso un dispositivo. In generale, è possibile migliorare la velocità di trasferimento dalla fonte di dati al dispositivo nei seguenti modi. L'elenco seguente è ordinato dal maggiore al più piccolo impatto positivo sulle prestazioni:

1. Esegui più operazioni di scrittura contemporaneamente: a tale scopo, esegui ogni comando da più finestre di terminale su un computer con una connessione di rete a un singolo AWS Snowball Edge dispositivo.
2. Trasferimento di file di piccole dimensioni in batch: ogni operazione di copia comporta un sovraccarico dovuto alla crittografia. Per velocizzare il processo, raggruppa i file in un unico archivio. Quando i file vengono raggruppati in batch, possono essere estratti automaticamente quando vengono importati in Amazon S3. Per ulteriori informazioni, consulta [Suddivisione in batch di file di piccole dimensioni per migliorare le prestazioni di trasferimento dei dati su Snowball Edge](#).
3. Non eseguire altre operazioni sui file durante il trasferimento: la ridenominazione dei file durante il trasferimento, la modifica dei relativi metadati o la scrittura di dati sui file durante un'operazione di copia hanno un impatto negativo sulle prestazioni di trasferimento. Consigliamo di lasciare i file in uno stato statico durante il trasferimento.
4. Riduci l'uso della rete locale: il AWS Snowball Edge dispositivo comunica attraverso la rete locale. In questo modo puoi migliorare la velocità di trasferimento dei dati riducendo il traffico di altra rete locale tra il AWS Snowball Edge dispositivo, lo switch a cui è collegato e il computer che ospita la fonte di dati.

5. Elimina gli hop non necessari: ti consigliamo di configurare il AWS Snowball Edge dispositivo, la fonte dati e il computer su cui è in esecuzione la connessione terminale tra di essi in modo che siano le uniche macchine che comunicano attraverso un singolo switch. In questo modo è possibile migliorare la velocità di trasferimento dei dati.

Sicurezza per AWS Snowball Edge

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 come sicurezza del cloud e sicurezza nel cloud:

- **Sicurezza del cloud:** AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei [programmi di conformitàAWS](#). Per ulteriori informazioni sui programmi di conformità applicabili AWS Snowball Edge, consulta [AWS Services in Scope by Compliance Program](#).
- **Sicurezza nel cloud:** la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Snowball Edge. Negli argomenti seguenti viene illustrato come eseguire la configurazione AWS Snowball Edge per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS Snowball Edge le tue risorse.

Argomenti

- [Protezione dei dati in AWS Snowball Edge](#)
- [Identity and Access Management in AWS Snowball Edge](#)
- [Logging e monitoraggio in AWS Snowball Edge](#)
- [Convalida della conformità per AWS Snowball Edge](#)
- [Resilienza](#)
- [Sicurezza dell'infrastruttura in AWS Snowball Edge](#)

Protezione dei dati in AWS Snowball Edge

AWS Snowball Edge è conforme al [modello di responsabilità AWS condivisa](#), che include regolamenti e linee guida per la protezione dei dati. AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i AWS servizi. AWS mantiene il controllo sui dati ospitati su questa infrastruttura, compresi i controlli di configurazione di sicurezza per la gestione dei contenuti e dei dati personali dei clienti. AWS i clienti e i partner APN, che agiscono in qualità di titolari o incaricati del trattamento dei dati, sono responsabili di tutti i dati personali che inseriscono nel Cloud AWS.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS Identity and Access Management (IAM), in modo che a ciascun utente vengano concesse solo le autorizzazioni necessarie per svolgere le proprie mansioni lavorative. Ti 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 consigliabile TLS 1.2 o versioni successive.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati personali archiviati in Amazon S3.
- 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 FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Consigliamo di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero come un campo Nome. Ciò include quando si lavora con AWS Snowball Edge o con altri AWS servizi che utilizzano la console, l'API o AWS CLI AWS SDKs. Gli eventuali dati immessi in AWS Snowball Edge o altri servizi potrebbero essere prelevati per l'inserimento nei log di diagnostica. Quando fornisci un URL a un server esterno, non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta a tale server.

Per ulteriori informazioni sulla protezione dei dati, consulta il post del blog [AWS Modello di responsabilità condivisa e GDPR](#) su AWS Security Blog.

Argomenti

- [Protezione dei dati nel cloud](#)
- [Protezione dei dati sul tuo dispositivo](#)

Protezione dei dati nel cloud

AWS Snowball Edge protegge i tuoi dati quando importi o esporti dati in Amazon S3, quando crei un lavoro per ordinare un dispositivo Snowball Edge e quando il dispositivo viene aggiornato. Le sezioni seguenti descrivono come proteggere i dati quando si utilizza Snowball Edge e si è online o si interagisce AWS nel cloud.

Argomenti

- [Crittografia per AWS Snowball Edge](#)
- [AWS Key Management Service nel AWS Snowball Edge](#)

Crittografia per AWS Snowball Edge

Quando usi Snowball Edge per importare dati in S3, tutti i dati trasferiti su un dispositivo sono protetti dalla crittografia SSL sulla rete. Per proteggere i dati inattivi, AWS Snowball Edge usa SSE (crittografia lato server).

Crittografia lato server in AWS Snowball Edge

AWS Snowball Edge supporta la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3). La crittografia lato server serve a proteggere i dati inattivi e SSE-S3 dispone di una crittografia avanzata a più fattori per proteggere i dati archiviati in Amazon S3. Per ulteriori informazioni su SSE-S3, consulta [Protezione dei dati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 \(SSE-S3\) nella Guida per l'utente di Amazon Simple Storage Service](#).

Attualmente AWS Snowball Edge non offre la crittografia lato server con chiavi fornite dal cliente (SSE-C). Lo storage compatibile con Amazon S3 su Snowball Edge offre SSE-C per processi di elaborazione e storage locali. Tuttavia, è possibile usare questo tipo di SSE per proteggere i dati importati o potrebbe essere già utilizzato sui dati che si desidera esportare. In questi casi tieni a mente le seguenti considerazioni:

- Importa —

Se desideri utilizzare SSE-C per crittografare gli oggetti che hai importato in Amazon S3, dovresti prendere in considerazione l'utilizzo della crittografia SSE-KMS o SSE-S3, stabilita come parte della policy sui bucket di quel bucket. Tuttavia, se devi utilizzare SSE-C per crittografare gli oggetti che hai importato in Amazon S3, dovrai copiare l'oggetto all'interno del tuo bucket per crittografarlo con SSE-C. Di seguito è riportato un esempio di comando CLI per ottenere ciò:

```
aws s3 cp s3://amzn-s3-demo-bucket/object.txt s3://amzn-s3-demo-bucket/object.txt --sse-c --sse-c-key 1234567891SAMPLEKEY
```

oppure

```
aws s3 cp s3://amzn-s3-demo-bucket s3://amzn-s3-demo-bucket --sse-c --sse-c-key 1234567891SAMPLEKEY --recursive
```

- **Esporta:** se desideri esportare oggetti crittografati con SSE-C, copia innanzitutto tali oggetti in un altro bucket che non dispone di crittografia lato server o che ha SSE-KMS o SSE-S3 specificato nella politica del bucket di quel bucket.

Abilitazione di SSE-S3 per i dati importati in Amazon S3 da Snowball Edge

Utilizza la seguente procedura nella console di gestione Amazon S3 per abilitare SSE-S3 per l'importazione di dati in Amazon S3. Non è necessaria alcuna configurazione nel Console di gestione della famiglia di servizi AWS Snow o sul dispositivo Snowball stesso.

Per abilitare la crittografia SSE-S3 per i dati che stai importando in Amazon S3, è sufficiente impostare le policy dei bucket per tutti i bucket in cui stai importando i dati. Puoi aggiornare la policy per rifiutare l'autorizzazione (`s3:PutObject`) dell'oggetto da caricare, se la richiesta di caricamento non include l'intestazione `x-amz-server-side-encryption`.

Per abilitare SSE-S3 per i dati importati in Amazon S3

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegliere il bucket in cui stai importando i dati dall'elenco dei bucket.
3. Seleziona Autorizzazioni.
4. Scegli Bucket Policy (Policy del bucket).

5. In Editor policy bucket (Editor della policy del bucket), immettere le seguenti policy. Sostituire tutte le istanze di *YourBucket* in questa policy con il nome effettivo del bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::YourBucket/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      }
    }
  ]
}
```

6. Scegli Save (Salva).

Hai finito di configurare il tuo bucket Amazon S3. Quando i dati vengono importati in questo bucket, sono protetti da SSE-S3. Ripeti questa procedura per qualsiasi altro bucket, se necessario.

AWS Key Management Service nel AWS Snowball Edge

AWS Key Management Service (AWS KMS) è un servizio gestito che semplifica la creazione e il controllo delle chiavi di crittografia utilizzate per crittografare i dati. AWS KMS utilizza moduli di sicurezza hardware (HSMs) per proteggere la sicurezza delle chiavi. In particolare, l'Amazon Resource Name (ARN) per la AWS KMS chiave scelta per un job in AWS Snowball Edge è associato a una chiave KMS. Questa chiave KMS viene utilizzata per crittografare il codice di sblocco del processo. Il codice di sblocco viene utilizzato per decrittografare il primo livello della crittografia del file manifest. Le chiavi di crittografia archiviate all'interno del file manifest vengono utilizzate per crittografare e decrittografare i dati sul dispositivo.

In AWS Snowball Edge, AWS KMS protegge le chiavi di crittografia utilizzate per proteggere i dati su ciascun AWS Snowball Edge dispositivo. Quando crei il tuo lavoro, puoi anche scegliere una chiave KMS esistente. La specificazione dell'ARN per AWS KMS una chiave AWS Snowball Edge indica AWS KMS keys quale utilizzare per crittografare le chiavi univoche sul dispositivo. AWS Snowball Edge Per ulteriori informazioni sulle server-side-encryption opzioni Amazon S3 AWS Snowball Edge supportate, consulta. [Crittografia lato server in AWS Snowball Edge](#)

Utilizzo del Managed Customer AWS KMS keys per Snowball Edge

Se desideri utilizzare il cliente gestito AWS KMS keys per Snowball Edge creato per il tuo account, segui questi passaggi.

Per selezionarlo AWS KMS keys per il tuo lavoro

1. In Console di gestione della famiglia di servizi AWS Snow, scegli Crea lavoro.
2. Scegliere il tipo di processo, quindi selezionare Next (Avanti).
3. Fornire i dettagli di spedizione, quindi selezionare Next (Avanti).
4. Specificare i dettagli del processo, quindi selezionare Next (Avanti).
5. Impostare le opzioni di sicurezza. In Crittografia, per la chiave KMS scegli la chiave Chiave gestita da AWS o una chiave personalizzata precedentemente creata in AWS KMS oppure scegli Inserisci una chiave ARN se devi inserire una chiave di proprietà di un account separato.

Note

L' AWS KMS key ARN è un identificatore univoco globale per le chiavi gestite dai clienti.

6. Scegli Avanti per completare la selezione del tuo. AWS KMS key

7. Concedi all'utente IAM del dispositivo Snow l'accesso alla chiave KMS.
 - a. Nella console IAM (<https://console.aws.amazon.com/iam/>), vai su Encryption Keys e apri la chiave KMS che hai scelto di utilizzare per crittografare i dati sul dispositivo.
 - b. In Utenti chiave, seleziona Aggiungi, cerca l'utente IAM del dispositivo Snow e seleziona Attach.

Creazione di una chiave di crittografia envelope KMS personalizzata

Hai la possibilità di utilizzare la tua chiave di crittografia personalizzata per AWS KMS buste con AWS Snowball Edge. Se scegli di creare una tua propria chiave, questa deve essere creata nella stessa regione in cui è stato creato il processo.

Per creare una AWS KMS chiave personalizzata per un lavoro, consulta [Creating Keys](#) nella AWS Key Management Service Developer Guide.

Protezione dei dati sul tuo dispositivo

Proteggere il tuo AWS Snowball Edge

Di seguito sono riportati alcuni punti di sicurezza che consigliamo di prendere in considerazione durante l'utilizzo AWS Snowball Edge e anche alcune informazioni di alto livello su altre precauzioni di sicurezza che adottiamo quando un dispositivo arriva AWS per l'elaborazione.

Consigliamo i seguenti approcci di sicurezza:

- La prima volta che ricevi il dispositivo, controlla se risulta danneggiato o manomesso in modo evidente. Se noti qualcosa di sospetto sul dispositivo, non connetterlo alla rete interna. Contattaci [Supporto AWS](#) invece e ti verrà spedito un nuovo dispositivo.
- Ti invitiamo a impegnarti per proteggere le credenziali del processo dalla divulgazione. Chiunque abbia accesso al manifest e al codice di sblocco di un processo può accedere al contenuto del dispositivo inviato per tale processo.
- Non lasciare il dispositivo incustodito in un'area di carico. Se lasciato su un'area di carico può essere esposto agli elementi. Sebbene ogni AWS Snowball Edge dispositivo sia robusto, gli agenti atmosferici possono danneggiare l'hardware più robusto. Segnala i dispositivi rubati, mancanti o rotti il prima possibile. Prima segnali il problema, prima sarà possibile inviarne un'altra per completare il processo.

 Note

I AWS Snowball Edge dispositivi sono di proprietà di AWS. La manomissione di un dispositivo è una violazione della Politica di utilizzo AWS accettabile. Per ulteriori informazioni, consulta <http://aws.amazon.com/aup/>.

Viene eseguita la seguente procedura di sicurezza:

- Quando si trasferiscono dati con l'adattatore Amazon S3, i metadati degli oggetti non vengono mantenuti. Gli unici metadati che rimangono inalterati sono `filename` e `filesize`. Tutti gli altri metadati sono impostati come nel seguente esempio: `-rw-rw-r-- 1 root root [filesize]
Dec 31 1969 [path/filename]`
- Quando si trasferiscono dati con l'interfaccia NFS, i metadati degli oggetti vengono mantenuti.
- Quando un dispositivo arriva AWS, lo ispezioniamo per individuare eventuali segni di manomissione e per verificare che non siano state rilevate modifiche dal Trusted Platform Module (TPM). AWS Snowball Edge utilizza più livelli di sicurezza progettati per proteggere i dati, tra cui custodie resistenti alle manomissioni, crittografia a 256 bit e un TPM standard del settore progettato per fornire sicurezza e catena di custodia completa dei dati.
- Una volta elaborato e verificato il processo di trasferimento dei dati, AWS esegue una cancellazione software del dispositivo Snowball seguendo le linee guida del National Institute of Standards and Technology (NIST) per la sanificazione dei supporti.

Convalida dei tag NFC

I dispositivi Snowball Edge Compute Optimized e Snowball Edge Storage Optimized (per il trasferimento dati) dispongono di tag NFC incorporati. Puoi scansionare questi tag con l'app di AWS Snowball Edge verifica, disponibile su Android. La scansione e la convalida di questi tag NFC può aiutarti a verificare che il dispositivo non è stato manomesso prima dell'uso.

La convalida dei tag NFC include l'utilizzo del client Snowball Edge per generare un codice QR specifico del dispositivo per verificare che i tag da scansionare siano per il dispositivo giusto.

La procedura seguente descrive come convalidare i tag NFC su un dispositivo Snowball Edge. Prima di iniziare, assicurati di aver eseguito le seguenti cinque operazioni dell'esercizio delle nozioni di base:

1. Crea il tuo lavoro in Snowball Edge. Per ulteriori informazioni, consulta [Creazione di un lavoro per ordinare un dispositivo Snowball Edge](#)
2. Ricevere il dispositivo. Per ulteriori informazioni, consulta [Ricevere lo Snowball Edge](#).
3. Connessione alla rete locale. Per ulteriori informazioni, consulta [Connessione di uno Snowball Edge alla rete locale](#).
4. Ottenere credenziali e strumenti. Per ulteriori informazioni, consulta [Ottenere le credenziali per accedere a Snowball Edge](#).
5. Scarica e installa il client Snowball Edge. Per ulteriori informazioni, consulta [Scaricamento e installazione del client Snowball Edge](#).

Per convalidare i tag NFC

1. Esegui il comando `client snowballEdge get-app-qr-code` Snowball Edge. Se si esegue il comando per un nodo in un cluster, specificare il numero di serie (`--device-sn`) per ottenere un codice QR per un singolo nodo. Ripetere questo passaggio per ogni nodo nel cluster. Per ulteriori informazioni sull'utilizzo di questo comando, consulta [Ottenere un codice QR per convalidare i tag NFC di Snowball Edge](#).

Il codice QR viene salvato in un percorso scelto come file `.png`.

2. Passare al file `.png` salvato e aprirlo in modo che sia possibile scansionare il codice QR con l'app.
3. Puoi scansionare questi tag utilizzando l'app AWS Snowball Edge di verifica su Android.

 Note

L'app di AWS Snowball Edge verifica non è disponibile per il download, ma se hai un dispositivo con l'app già installata, puoi utilizzare l'app.

4. Avvia l'app e segui le istruzioni a video.

Hai ora correttamente scansionato e convalidato i tag NFC per il tuo dispositivo.

In caso di problemi durante la scansione, provare quanto segue:

- Verifica che il tuo dispositivo disponga delle opzioni Snowball Edge Compute Optimized.
- Se hai l'app su un altro dispositivo, prova a utilizzarlo.

- Spostare il dispositivo a un'area isolata del locale, lontano da interferenze con altri tag NFC e riprovare.
- Se i problemi persistono, contatta [Supporto AWS](#).

Identity and Access Management in AWS Snowball Edge

Ogni AWS Snowball Edge lavoro deve essere autenticato. Puoi farlo creando e gestendo gli utenti IAM nel tuo account. Utilizzando IAM, puoi creare e gestire utenti e autorizzazioni in AWS.

AWS Snowball Edge gli utenti devono disporre di determinate autorizzazioni relative all'IAM per accedere a per creare lavori. AWS Snowball Edge Console di gestione AWS Un utente IAM che crea un processo di importazione o esportazione deve inoltre avere accesso alle risorse Amazon Simple Storage Service (Amazon S3) corrette, come i bucket Amazon S3 da utilizzare per il lavoro, le risorse AWS KMS , l'argomento Amazon SNS e EC2 l'AMI compatibile con Amazon per i lavori di edge computing.

Important

Per informazioni sull'utilizzo di IAM localmente sul tuo dispositivo, consulta. [Utilizzo di IAM localmente su Snowball Edge](#)

Argomenti

- [Controllo degli accessi per la console Snowball Edge e creazione di lavori](#)

Controllo degli accessi per la console Snowball Edge e creazione di lavori

Come per tutti i AWS servizi, l'accesso a AWS Snowball Edge richiede credenziali che AWS possono essere utilizzate per autenticare le richieste. Tali credenziali devono disporre delle autorizzazioni per accedere alle AWS risorse, come un bucket Amazon S3 o una funzione. AWS Lambda AWS Snowball Edge differisce in due modi:

1. I job in AWS Snowball Edge non dispongono di Amazon Resource Names (ARNs).
2. Il controllo dell'accesso fisico e di rete per un dispositivo locale è una tua responsabilità.

Scopri [Identity and Access Management per AWS Snowball Edge](#) i dettagli su come utilizzare [AWS Identity and Access Management \(IAM\)](#) AWS Snowball Edge e su come proteggere le tue risorse controllando chi può accedervi nei consigli Cloud AWS sul controllo degli accessi locali.

Identity and Access Management per AWS Snowball Edge

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. AWS Snow Family IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come AWS Snow Family funziona con IAM](#)
- [Esempi di policy basate sull'identità per AWS Snowball Edge](#)
- [Risoluzione dei problemi AWS Snowball Edge di identità e accesso](#)

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS Snow Family svolgi.

Utente del servizio: se utilizzi il AWS Snow Family servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS Snow Family funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS Snow Family, consulta [Risoluzione dei problemi AWS Snowball Edge di identità e accesso](#).

Amministratore del servizio: se sei responsabile delle AWS Snow Family risorse della tua azienda, probabilmente hai pieno accesso a AWS Snow Family. È tuo compito determinare a quali AWS Snow Family funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste

all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS Snow Family, consulta [Come AWS Snow Family funziona con IAM](#).

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS Snow Family. Per visualizzare esempi di policy AWS Snow Family basate sull'identità che puoi utilizzare in IAM, consulta. [Esempi di policy basate sull'identità per AWS Snowball Edge](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al Console di gestione AWS o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta [Signature Version 4 AWS per le richieste API](#) nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'utente di AWS IAM Identity Center e [Utilizzo dell'autenticazione a più fattori \(MFA\)AWS in IAM](#) nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, un provider di identità Web Directory Service, la directory Identity Center o qualsiasi utente che accede Servizi AWS utilizzando credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta [Cos'è IAM Identity Center?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti

alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in Console di gestione AWS, puoi [passare da un ruolo utente a un ruolo IAM \(console\)](#). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta [Create a role for a third-party identity provider \(federation\)](#) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center.
- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze 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 IAM.

- **Accesso a più servizi:** alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- **Sessioni di accesso inoltrato (FAS):** quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).
- **Ruolo di servizio:** 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 la sezione [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.
- **Ruolo collegato al servizio:** 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'azione 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 ai servizi, ma non modificarle.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. È preferibile archiviare le chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon](#) nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua

una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' Console di gestione AWS AWS CLI, dall' o dall' AWS API.

Policy basate sull'identità

Le policy basate su 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 IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente IAM.

Policy basate sulle risorse

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 dei 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.

È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

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.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica della lista di controllo degli accessi \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare

le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere [Resource control policies \(RCPs\)](#) nella Guida per l'AWS Organizations utente.

- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta la [logica di valutazione delle policy](#) nella IAM User Guide.

Come AWS Snow Family funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Snow Family, scopri con quali funzionalità IAM è disponibile l'uso AWS Snow Family.

Funzionalità IAM che puoi utilizzare con AWS Snow Family

Funzionalità IAM	AWS Snow Family supporto
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì

Funzionalità IAM	AWS Snow Family supporto
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	No

Per avere una panoramica di alto livello su come AWS Snow Family 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 AWS Snow Family

Supporta le policy basate su identità: sì

Le policy basate su 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 IAM.

Con le policy basate su 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. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. 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 di IAM.

Esempi di politiche basate sull'identità per AWS Snow Family

Per visualizzare esempi di politiche basate sull' AWS Snow Family identità, vedere. [Esempi di policy basate sull'identità per AWS Snowball Edge](#)

Politiche basate sulle risorse all'interno AWS Snow Family

Supporta le policy basate sulle risorse: sì

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 dei 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. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Azioni politiche per AWS Snow Family

Supporta le operazioni di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale 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 a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS Snow Family azioni, vedere [Azioni definite da AWS Snow Family](#) nel Service Authorization Reference.

Le azioni politiche in AWS Snow Family uso utilizzano il seguente prefisso prima dell'azione:

```
snowball
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
    "snowball:action1",  
    "snowball:action2"  
]
```

Per visualizzare esempi di politiche AWS Snow Family basate sull'identità, vedere. [Esempi di policy basate sull'identità per AWS Snowball Edge](#)

Risorse politiche per AWS Snow Family

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale 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. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di AWS Snow Family risorse e relativi ARNs, vedere [Resources defined by AWS Snow Family](#) nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione [Operazioni definite da AWS Snow Family](#).

Per visualizzare esempi di politiche AWS Snow Family basate sull'identità, vedere. [Esempi di policy basate sull'identità per AWS Snowball Edge](#)

Chiavi relative alle condizioni delle politiche per AWS Snow Family

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 principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. 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.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. OR Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta [Elementi delle policy IAM: variabili e tag](#) nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. 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 di chiavi di AWS Snow Family condizione, consulta [Condition keys for AWS Snow Family](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi [Azioni definite da AWS Snow Family](#).

Per visualizzare esempi di politiche AWS Snow Family basate sull'identità, vedere. [Esempi di policy basate sull'identità per AWS Snowball Edge](#)

ACLs in AWS Snow Family

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 AWS Snow Family

Supporta ABAC (tag nelle policy): parzialmente

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci 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 Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente 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 AWS Snow Family

Supporta le credenziali temporanee: sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla [Servizi AWS compatibilità con IAM nella IAM](#) User Guide.

Stai utilizzando credenziali temporanee se accedi Console di gestione AWS utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Passaggio da un ruolo utente a un ruolo IAM \(console\)](#) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API o l'AWS CLI. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

Sessioni di accesso diretto per AWS Snow Family

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli di servizio per AWS Snow Family

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 la sezione [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 compromettere la funzionalità. AWS Snow Family Modifica i ruoli di servizio solo quando viene AWS Snow Family fornita una guida in tal senso.

Ruoli collegati ai servizi per AWS Snow Family

Supporta i ruoli collegati ai servizi: no

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'azione 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 ai servizi, 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 sull'identità per AWS Snowball Edge

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS Snow Family. Inoltre, non possono eseguire attività utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) o l'API. AWS Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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 IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Snow Family, incluso il formato di ARNs per ogni tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione AWS Snow Family](#) nel Service Authorization Reference.

Argomenti

- [Best practice per le policy](#)
- [Utilizzo della console di AWS Snow Family](#)
- [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 Snow Family risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui 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 ulteriori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi 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 privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue 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 ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente 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, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Protezione dell'accesso API con MFA](#) nella Guida per l'utente 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 di AWS Snow Family

Per accedere alla AWS Snow Family console, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS Snow Family risorse del tuo 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 agli utenti che effettuano chiamate solo verso AWS CLI o l'AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la AWS Snow Family console, allega anche la policy AWS Snow Family *ConsoleAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente 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 AWS Snowball Edge di identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un AWS Snow Family IAM.

Argomenti

- [Non sono autorizzato a eseguire alcuna azione in AWS Snow Family](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Snow Family risorse](#)

Non sono autorizzato a eseguire alcuna azione in AWS Snow Family

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 `snowball:GetWidget` fittizie.

```

User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
snowball: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 `snowball: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 errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS Snow Family.

Alcuni Servizi AWS consentono di passare 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 Snow Family. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare 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.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Snow Family risorse

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 ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Snow Family supporta queste funzionalità, consulta [Come AWS Snow Family funziona con IAM](#)
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, 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 IAM.

Controllo degli accessi in Cloud AWS

Puoi avere credenziali valide per autenticare le tue richieste. AWS Tuttavia, a meno che non si disponga delle autorizzazioni necessarie, non è possibile creare o accedere alle risorse. AWS Ad esempio, è necessario disporre delle autorizzazioni per creare un lavoro per ordinare un dispositivo Snowball Edge.

Nelle sezioni seguenti viene descritto come gestire le autorizzazioni basate su cloud per AWS Snowball Edge. Consigliamo di leggere prima la panoramica.

- [Panoramica della gestione delle autorizzazioni di accesso alle risorse in Cloud AWS](#)
- [Utilizzo di politiche basate sull'identità \(politiche IAM\) per AWS Snowball Edge](#)

Panoramica della gestione delle autorizzazioni di accesso alle risorse in Cloud AWS

Ogni AWS risorsa è di proprietà di un Account AWS, e le autorizzazioni per creare o accedere a una risorsa sono regolate da politiche di autorizzazione. Un amministratore di account può associare politiche di autorizzazione alle identità IAM (ovvero utenti, gruppi e ruoli) e alcuni servizi (come AWS Lambda) supportano anche l'associazione di politiche di autorizzazione alle risorse.

Note

Un amministratore account (o un utente amministratore) è un utente con privilegi di amministratore. Per ulteriori informazioni, consulta [Best practice IAM](#) nella Guida per l'utente di IAM.

Argomenti

- [Risorse e operazioni](#)
- [Informazioni sulla proprietà delle risorse](#)
- [Gestione dell'accesso alle risorse in Cloud AWS](#)
- [Specifica degli elementi delle policy: operazioni, effetti e principali](#)
- [Specifica delle condizioni in una policy](#)

Risorse e operazioni

Nel AWS Snowball Edge, la risorsa principale è un lavoro. AWS Snowball Edge dispone anche di dispositivi come Snowball e il AWS Snowball Edge dispositivo, tuttavia è possibile utilizzare tali dispositivi solo nel contesto di un lavoro esistente. I bucket Amazon S3 e le funzioni Lambda sono risorse rispettivamente di Amazon S3 e Lambda.

Come accennato in precedenza, ai job non è associato Amazon Resource Names (ARNs). Tuttavia, alle risorse di altri servizi, come i bucket Amazon S3, è associata una funzione unique ARNs (), come illustrato nella tabella seguente.

AWS Snowball Edge fornisce una serie di operazioni per creare e gestire i lavori. Per un elenco delle operazioni disponibili, consulta l'[AWS Snowball Edge API Reference](#).

Informazioni sulla proprietà delle risorse

È Account AWS proprietario delle risorse create nell'account, indipendentemente da chi le ha create. In particolare, il proprietario Account AWS della risorsa è l'[entità principale](#) (ovvero l'account root, un utente IAM o un ruolo IAM) che autentica la richiesta di creazione delle risorse. Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi le credenziali dell'account root del tuo account Account AWS per creare un bucket S3, sei il proprietario della risorsa (in pratica AWS Snowball Edge, la risorsa Account AWS è il lavoro).
- Se crei un utente IAM nel tuo Account AWS e concedi le autorizzazioni per creare un lavoro per ordinare un dispositivo Snowball Edge a quell'utente, l'utente può creare un lavoro per ordinare un dispositivo Snowball Edge. Tuttavia Account AWS, la risorsa di lavoro è di proprietà dell'utente a cui appartiene.
- Se crei un ruolo IAM Account AWS con le autorizzazioni necessarie per creare un lavoro, chiunque possa assumere il ruolo può creare un lavoro per ordinare un dispositivo Snowball Edge. Il tuo Account AWS, a cui appartiene il ruolo, è il proprietario della risorsa di lavoro.

Gestione dell'accesso alle risorse in Cloud AWS

La policy delle autorizzazioni descrive chi ha accesso a cosa. Nella sezione seguente vengono descritte le opzioni disponibili per la creazione di policy relative alle autorizzazioni.

 Note

Questa sezione illustra l'utilizzo di IAM nel contesto di AWS Snowball Edge. Non vengono fornite informazioni dettagliate sul servizio IAM. Per la documentazione di IAM completa, consulta [Che cos'è IAM?](#) nella Guida per l'utente di IAM. Per informazioni sulla sintassi delle policy IAM e le rispettive descrizioni, consulta [Riferimento alle policy IAM di AWS](#) nella Guida per l'utente di IAM.

Le politiche collegate a un'identità IAM sono denominate politiche basate sull'identità (politiche IAM) e le politiche allegate a una risorsa sono denominate politiche basate sulle risorse. AWS Snowball Edge supporta solo politiche basate sull'identità (politiche IAM).

Argomenti

- [Policy basate su risorse](#)

Policy basate su risorse

Anche altri servizi, ad esempio Amazon S3, supportano policy di autorizzazioni basate su risorse. Ad esempio, puoi allegare una policy a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket. AWS Snowball Edge non supporta politiche basate sulle risorse.

Specifica degli elementi delle policy: operazioni, effetti e principali

Per ogni lavoro (vedi [Risorse e operazioni](#)), il servizio definisce una serie di operazioni API (vedi [AWS Snowball Edge API Reference](#)) per creare e gestire tale lavoro. Per concedere le autorizzazioni per queste operazioni API, AWS Snowball Edge definisce una serie di azioni che puoi specificare in una politica. Ad esempio, per un processo, vengono definite le seguenti operazioni: `CreateJob`, `CancelJob` e `DescribeJob`. Si noti che l'esecuzione di un'operazione API può richiedere le autorizzazioni per più di un'azione.

Di seguito sono elencati gli elementi di base di una policy:

- **Risorsa:** in una policy si utilizza il nome della risorsa Amazon (ARN) per identificare la risorsa a cui si applica la policy stessa. Per ulteriori informazioni, consulta [Risorse e operazioni](#).

 Note

Questa funzionalità è supportata per Amazon S3, Amazon AWS KMS, EC2 AWS Lambda e molti altri servizi.

Snowball non supporta la specificazione di un ARN di risorsa nell'elemento `Resource` di una dichiarazione di policy IAM. Per consentire l'accesso a Snowball, specificalo `"Resource": "*" nella tua politica.`

- Operazione: utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Ad esempio, a seconda del `Effect`, `snowball:*` specificato, autorizzi o rifiuti all'utente le autorizzazioni per eseguire tutte le operazioni.

 Note

Questa funzionalità è supportata per Amazon EC2, Amazon S3 e IAM.

- Effetto: l'effetto prodotto quando l'utente richiede l'operazione specifica, ovvero un'autorizzazione o un rifiuto. Se non concedi esplicitamente (consenti) l'accesso a una risorsa, l'accesso viene implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per garantire che un utente non possa accedervi, anche se l'accesso viene concesso da un'altra policy.

 Note

Questa funzionalità è supportata per Amazon EC2, Amazon S3 e IAM.

- Principale: nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per le politiche basate sulle risorse, specifichi l'utente, l'account, il servizio o l'altra entità a cui desideri ricevere le autorizzazioni (si applica solo alle politiche basate sulle risorse). AWS Snowball Edge non supporta politiche basate sulle risorse.

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consulta [AWS Riferimento alle policy IAM](#) nella Guida per l'utente di IAM.

Per una tabella che mostra tutte le azioni dell' AWS Snowball Edge API, vedi. [AWS Snowball Edge Autorizzazioni API: riferimento ad azioni, risorse e condizioni](#)

Specifica delle condizioni in una policy

Quando si concedono le autorizzazioni, è possibile utilizzare il linguaggio della policy IAM per specificare le condizioni in base a cui la policy deve essere applicata. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni su come specificare le condizioni in un linguaggio di policy, consulta la sezione [Condizione](#) nella Guida per l'utente di IAM.

Per esprimere le condizioni è necessario utilizzare chiavi di condizione predefinite. Non esistono chiavi di condizione specifiche per AWS Snowball Edge. Tuttavia, ci sono chiavi AWS-wide condition che puoi usare a seconda delle esigenze. Per un elenco completo delle chiavi AWS-wide, consulta [Available Keys for Conditions](#) nella IAM User Guide.

Utilizzo di politiche basate sull'identità (politiche IAM) per AWS Snowball Edge

Questo argomento fornisce esempi di politiche basate sull'identità che dimostrano come un amministratore di account può collegare politiche di autorizzazione alle identità IAM (ovvero utenti, gruppi e ruoli). Queste politiche concedono quindi le autorizzazioni per eseguire operazioni sulle risorse di AWS Snowball Edge Cloud AWS

Important

In primo luogo, è consigliabile esaminare gli argomenti introduttivi in cui vengono spiegati i concetti di base e le opzioni disponibili per gestire l'accesso alle risorse AWS Snowball Edge. Per ulteriori informazioni, consulta [Panoramica della gestione delle autorizzazioni di accesso alle risorse in Cloud AWS](#).

In questa sezione vengono trattati gli argomenti seguenti:

- [Autorizzazioni necessarie per utilizzare la console AWS Snowball Edge](#)
- [AWS-Policy gestite \(predefinite\) per AWS Snowball Edge](#)
- [Esempi di policy gestite dal cliente](#)

Di seguito viene illustrato un esempio di policy di autorizzazione.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "snowball:*",
        "importexport:*"
      ],
      "Resource": "*"
    }
  ]
}
```

La policy include due dichiarazioni:

- La prima istruzione concede le autorizzazioni per tre azioni Amazon S3 `s3:GetBucketLocation` (`s3:GetObject`, `s3:ListBucket` e) su tutti i bucket Amazon S3 utilizzando l'Amazon Resource Name (ARN) di `arn:aws:s3:::*`. L'ARN specifica un carattere jolly (*) in modo che l'utente possa scegliere uno o tutti i bucket Amazon S3 da cui esportare i dati.
- La seconda dichiarazione concede le autorizzazioni per tutte le azioni. AWS Snowball Edge Poiché tali operazioni non supportano le autorizzazioni a livello di risorsa, la policy specifica il carattere jolly (*) e anche il valore `Resource` specifica un carattere jolly.

La policy non specifica l'elemento `Principal` poiché in una policy basata su identità l'entità che ottiene l'autorizzazione non viene specificata. Quando alleggi una policy a un utente, l'utente è il principale implicito. Quando colleghi una policy di autorizzazioni a un ruolo IAM, il principale identificato nella policy di attendibilità del ruolo ottiene le autorizzazioni.

Per una tabella che mostra tutte le azioni dell'API di gestione dei AWS Snowball Edge lavori e le risorse a cui si applicano, consulta. [AWS Snowball Edge Autorizzazioni API: riferimento ad azioni, risorse e condizioni](#)

Autorizzazioni necessarie per utilizzare la console AWS Snowball Edge

La tabella di riferimento delle autorizzazioni elenca le operazioni dell'API di gestione dei AWS Snowball Edge lavori e mostra le autorizzazioni richieste per ciascuna operazione. Per ulteriori informazioni sulle operazioni API di gestione dei processi, consulta [AWS Snowball Edge Autorizzazioni API: riferimento ad azioni, risorse e condizioni](#).

Per utilizzare Console di gestione della famiglia di servizi AWS Snow, è necessario concedere le autorizzazioni per azioni aggiuntive, come illustrato nella seguente politica di autorizzazione:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

```
    "Effect": "Allow",
    "Action": [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
    ],
    "Resource": "arn:aws:lambda:*::function:*"
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:ListFunctions"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:RetireGrant",
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:CreateRole",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:PutRolePolicy"
    ],
    "Resource": [
        "*"
    ]
},
```

```
{
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/snowball*",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": "importexport.amazonaws.com"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeImages",
    "ec2:ModifyImageAttribute"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "sns:CreateTopic",
    "sns:ListTopics",
    "sns:GetTopicAttributes",
    "sns:SetTopicAttributes",
    "sns:ListSubscriptionsByTopic",
    "sns:Subscribe"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "greengrass:getServiceRoleForAccount"
  ],
  "Resource": [
    "*"
  ]
},
{
```



```

        "Effect": "Allow",
        "Action": [
            "snowball:*"
        ],
        "Resource": [
            "*"
        ]
    }
]
}

```

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "lambda:GetFunction",

```

```

        "lambda:GetFunctionConfiguration"
    ],
    "Resource": "arn:aws:lambda::function:*"
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:ListFunctions"
    ],
    "Resource": "arn:aws:lambda:::*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:CreateRole",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:PutRolePolicy"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/snowball*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "importexport.amazonaws.com"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute"
    ],
    "Resource": [
        "*"
    ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:CreateTopic",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "greengrass:getServiceRoleForAccount"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "snowball:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

La AWS Snowball Edge console necessita di queste autorizzazioni aggiuntive per i seguenti motivi:

- **ec2:** — Consentono all'utente di descrivere le istanze EC2 compatibili con Amazon e di modificarne gli attributi per scopi di elaborazione locale. Per ulteriori informazioni, consulta [Utilizzo di istanze EC2 di calcolo compatibili con Amazon su Snowball Edge](#).

- **kms** :— Consentono all'utente di creare o scegliere la chiave KMS che crittograferà i dati. Per ulteriori informazioni, consulta [AWS Key Management Service nel AWS Snowball Edge](#).
- **iam** :— Consentono all'utente di creare o scegliere un ruolo IAM ARN che AWS Snowball Edge assumerà per accedere alle AWS risorse associate alla creazione e all'elaborazione dei lavori.
- **sns** :— Consentono all'utente di creare o scegliere le notifiche Amazon SNS per i lavori che crea. Per ulteriori informazioni, consulta [Notifiche per Snowball Edge](#).

AWS-Policy gestite (predefinite) per AWS Snowball Edge

AWS affronta molti casi d'uso comuni fornendo policy IAM autonome create e amministrate da AWS. Le policy gestite concedono le autorizzazioni necessarie per i casi di utilizzo comune in modo da non dover cercare quali sono le autorizzazioni richieste. Per ulteriori informazioni, consulta [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

È possibile utilizzare le seguenti politiche AWS gestite con AWS Snowball Edge.

Creazione di una policy sui ruoli IAM per Snowball Edge

È necessario creare una policy di ruolo IAM con autorizzazioni di lettura e scrittura per i bucket Amazon S3. Il ruolo IAM deve inoltre avere un rapporto di fiducia con Snowball Edge. Avere una relazione di fiducia significa AWS poter scrivere i dati nello Snowball e nei bucket Amazon S3, a seconda che si stiano importando o esportando dati.

Quando si crea un lavoro per ordinare un dispositivo Snowball Edge in Console di gestione della famiglia di servizi AWS Snow, la creazione del ruolo IAM necessario avviene nel passaggio 4 della sezione Autorizzazione. Questo processo è automatico. Il ruolo IAM che consenti a Snowball Edge di assumere viene utilizzato solo per scrivere i dati nel bucket quando arriva lo Snowball con i dati trasferiti. AWS La procedura seguente illustra tale processo.

Per creare il ruolo IAM per il tuo i

1. Accedi a Console di gestione AWS e apri la AWS Snowball Edge console all'indirizzo <https://console.aws.amazon.com/importexport/>.
2. Scegli Crea processo.
3. Nel primo passaggio, inserisci i dettagli per il processo di importazione in Amazon S3, quindi scegli Avanti.
4. Nella seconda fase, in Permission (Autorizzazione), scegliere Create/Select IAM Role (Crea/Seleziona ruolo IAM).

Si apre la console di gestione IAM, che mostra il ruolo IAM AWS utilizzato per copiare gli oggetti nei bucket Amazon S3 specificati.

5. Esaminare i dettagli in questa pagina, quindi scegliere Allow (Consenti).

Ritorni al Console di gestione della famiglia di servizi AWS Snow, dove l'ARN del ruolo IAM selezionato contiene l'Amazon Resource Name (ARN) per il ruolo IAM che hai appena creato.

6. Scegli Avanti per completare la creazione del tuo ruolo IAM.

La procedura precedente crea un ruolo IAM con autorizzazioni di scrittura per i bucket Amazon S3 in cui intendi importare i dati. Il ruolo IAM che viene creato ha una delle seguenti strutture, a seconda del fatto che sia per un processo di importazione o di esportazione.

del ruolo IAM per un processo di importazione

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:PutObjectAcl",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

```
]
}
```

Se utilizzi la crittografia lato server con chiavi AWS KMS gestite (SSE-KMS) per crittografare i bucket Amazon S3 associati al tuo processo di importazione, devi anche aggiungere la seguente dichiarazione al tuo ruolo IAM.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Se le dimensioni degli oggetti sono maggiori, il client Amazon S3 utilizzato per il processo di importazione utilizza il caricamento in più parti. Se avvii un caricamento in più parti utilizzando SSE-KMS, tutte le parti caricate vengono crittografate utilizzando la chiave specificata. AWS KMS Poiché le parti sono crittografate, devono essere decrittografate prima di poter essere assemblate per completare il caricamento multipart. Pertanto, è necessario disporre dell'autorizzazione per decrittografare la AWS KMS chiave (`kms:Decrypt`) quando si esegue un caricamento multipart su Amazon S3 con SSE-KMS.

Di seguito è riportato un esempio di ruolo IAM necessario per un processo di importazione che richiede l'autorizzazione `kms:Decrypt`.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey", "kms:Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Di seguito è riportato un esempio di ruolo IAM necessario per un processo di esportazione.

JSON

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

Se utilizzi la crittografia lato server con chiavi AWS KMS gestite per crittografare i bucket Amazon S3 associati al tuo processo di esportazione, devi anche aggiungere la seguente dichiarazione al tuo ruolo IAM.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/abc123a1-abcd-1234-efgh-111111111111"
}
```

Puoi creare politiche IAM personalizzate per consentire le autorizzazioni per le operazioni API per la gestione dei lavori. AWS Snowball Edge Puoi collegare queste policy personalizzate agli utenti o ai gruppi IAM che richiedono le autorizzazioni.

Esempi di policy gestite dal cliente

In questa sezione, puoi trovare esempi di politiche utente che concedono autorizzazioni per varie azioni di gestione dei AWS Snowball Edge lavori. Queste politiche funzionano quando si utilizza

AWS SDKs o il AWS CLI. Se utilizzi la console, sarà necessario concedere autorizzazioni aggiuntive specifiche per quest'ultima, come illustrato in [Autorizzazioni necessarie per utilizzare la console AWS Snowball Edge](#).

Note

Tutti gli esempi utilizzano la regione us-west-2 e contengono account fittizi. IDs

Esempi

- [Esempio 1: politica relativa al ruolo che consente a un utente di creare un Job per ordinare un dispositivo Snowball Edge con l'API](#)
- [Esempio 2: policy del ruolo per la creazione di processi di importazione](#)
- [Esempio 3: policy del ruolo per la creazione di processi di esportazione](#)
- [Esempio 4: autorizzazioni di ruolo previste e politica di attendibilità](#)
- [AWS Snowball Edge Autorizzazioni API: riferimento ad azioni, risorse e condizioni](#)

Esempio 1: politica relativa al ruolo che consente a un utente di creare un Job per ordinare un dispositivo Snowball Edge con l'API

La seguente policy di autorizzazioni è un componente necessario di qualsiasi policy utilizzata per concedere l'autorizzazione per la creazione di un processo o un cluster utilizzando l'API di gestione dei processi. La dichiarazione è necessaria come dichiarazione politica sulle relazioni di fiducia per il ruolo IAM di Snowball.

JSON

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



```
    ]
  }
}
```

Esempio 2: policy del ruolo per la creazione di processi di importazione

La seguente politica di fiducia dei ruoli viene utilizzata per creare processi di importazione per Snowball Edge che utilizzano le funzioni AWS Lambda powered by AWS IoT Greengrass .

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
        "s3:GetBucketLocation",
        "s3:ListBucketMultipartUploads",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:PutObjectAcl",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "snowball:*"
      ]
    }
  ]
}
```

```

    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:DescribeEndpoint",
        "iot:GetPolicy"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:GetFunction"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateDeployment",
        "greengrass:CreateDeviceDefinition",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:GetDeploymentStatus",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:GetGroupCertificateAuthority",

```

```

        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListDeployments",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

Esempio 3: policy del ruolo per la creazione di processi di esportazione

La seguente politica di fiducia dei ruoli viene utilizzata per creare lavori di esportazione per Snowball Edge che utilizzano le funzioni AWS Lambda powered by AWS IoT Greengrass .

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "snowball:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

```

    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "iot:AttachPrincipalPolicy",
      "iot:AttachThingPrincipal",
      "iot:CreateKeysAndCertificate",
      "iot:CreatePolicy",
      "iot:CreateThing",
      "iot:DescribeEndpoint",
      "iot:GetPolicy"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "lambda:GetFunction"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "greengrass:CreateCoreDefinition",
      "greengrass:CreateDeployment",
      "greengrass:CreateDeviceDefinition",
      "greengrass:CreateFunctionDefinition",
      "greengrass:CreateGroup",
      "greengrass:CreateGroupVersion",
      "greengrass:CreateLoggerDefinition",
      "greengrass:CreateSubscriptionDefinition",
      "greengrass:GetDeploymentStatus",
      "greengrass:UpdateGroupCertificateConfiguration",
      "greengrass:CreateGroupCertificateAuthority",
      "greengrass:GetGroupCertificateAuthority",
      "greengrass:ListGroupCertificateAuthorities",
      "greengrass:ListDeployments",
      "greengrass:GetGroup",

```

```

        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

Esempio 4: autorizzazioni di ruolo previste e politica di attendibilità

La seguente politica di autorizzazione prevista per i ruoli è necessaria per l'utilizzo di un ruolo di servizio esistente. È una configurazione unica.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sns:Publish",
      "Resource": ["[[snsArn]]"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/SnowFamily"
        }
      }
    }
  ]
}

```

```

    }
  }
]
}

```

La seguente politica di attendibilità dei ruoli prevista è necessaria per l'utilizzo di un ruolo di servizio esistente. È una configurazione unica.

JSON

```

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

```

AWS Snowball Edge Autorizzazioni API: riferimento ad azioni, risorse e condizioni

Quando configuri il [Controllo degli accessi in Cloud AWS](#) e scrivi una policy di autorizzazione che puoi collegare a un'identità IAM (policy basate su identità), puoi utilizzare l' nella tabella seguente come riferimento. La include ogni operazione dell'API di gestione dei lavori AWS Snowball Edge e le azioni corrispondenti per le quali è possibile concedere le autorizzazioni per eseguire l'azione. Include inoltre, per ogni operazione API, la AWS risorsa per la quale è possibile concedere le autorizzazioni. Puoi specificare le azioni nel campo `Action` della policy e il valore della risorsa nel campo `Resource`.

Puoi utilizzare i tasti AWS-wide condition nelle tue AWS Snowball Edge politiche per esprimere condizioni. Per un elenco completo delle chiavi AWS-wide, consulta [Available Keys](#) nella IAM User Guide.

 Note

Per specificare un'operazione, utilizza il prefisso `snowball:` seguito dal nome dell'operazione API (ad esempio, `snowball:CreateJob`).

Logging e monitoraggio in AWS Snowball Edge

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle soluzioni AWS Snowball Edge esistenti. AWS È necessario raccogliere i dati di monitoraggio in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWS fornisce diversi strumenti per monitorare le AWS Snowball Edge risorse e rispondere a potenziali incidenti:

AWS CloudTrail registri

CloudTrail fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio nell'API AWS Snowball Edge Job Management o durante l'utilizzo della AWS Console. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta API che è stata effettuata al AWS Snowball Edge servizio, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta [Registrazione delle chiamate AWS Snowball Edge API con AWS CloudTrail](#).

Convalida della conformità per AWS Snowball Edge

Per sapere se un Servizio AWS programma rientra nell'ambito di applicazione di specifici programmi di conformità, consulta [Servizi AWS Ambito per programma di conformità](#)[Servizi AWS](#) di conformità e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta [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 vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Governance e conformità per la sicurezza](#): queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- [Riferimenti sui servizi conformi ai requisiti HIPAA](#): elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- [AWS Risorse per la conformità](#): questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- [Valutazione delle risorse con regole](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- [AWS Security Hub CSPM](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

[Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS](#)

Sicurezza dell'infrastruttura in AWS Snowball Edge

In quanto servizio gestito, AWS Snow Family è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS Snow Family attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), 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. O puoi utilizzare [AWS Security Token Service](#) (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Convalida dei dati trasferiti con dispositivi Snowball Edge

Di seguito, troverai informazioni su come AWS Snowball Edge convalida i trasferimenti di dati e sui passaggi manuali che puoi adottare per garantire l'integrità dei dati durante e dopo un lavoro.

Quando copi un file da un'origine dati locale utilizzando l'interfaccia Amazon S3 a Snowball Edge, vengono creati diversi checksum. Questi checksum vengono utilizzati per convalidare automaticamente i dati quando vengono trasferiti.

Ad alto livello, questi checksum vengono creati per ogni file (o per parti di file di grandi dimensioni). Per Snowball Edge, questi checksum sono visibili quando si esegue il AWS CLI comando seguente su un bucket del dispositivo. I checksum vengono utilizzati per convalidare l'integrità dei dati durante i trasferimenti e assicurano che i dati vengano copiati correttamente.

```
aws s3api list-objects --bucket bucket-name --endpoint http://ip:8080 --profile edge-profile
```

Quando questi checksum non corrispondono, i dati associati non vengono importati in Amazon S3.

Inventario locale dei file e trasferimento dei dati con Snowball Edge

Crea un inventario locale dei file copiati su Snowball Edge utilizzando l'adattatore Amazon S3 o la CLI. Il contenuto dell'inventario locale può essere utilizzato per confrontare il contenuto dello storage o del server locale.

Ad esempio,

```
aws s3 cp folder/ s3://bucket --recursive > inventory.txt
```

Cause comuni degli errori di convalida dei dati con Snowball Edge

Quando si verifica un errore di convalida, i dati corrispondenti (un file o parte di un file di grandi dimensioni) non vengono scritti nella destinazione. Le cause più comuni degli errori di convalida sono le seguenti:

- Tentativo di copiare collegamenti simbolici.
- Tentativo di copiare file che vengono modificati attivamente. Il tentativo non supera la convalida del checksum ed è contrassegnato come trasferimento non riuscito.

- Sto cercando di copiare file di dimensioni superiori a 5 TB.
- Tentativo di copiare parti di dimensioni superiori a 2 GiB.
- Tentativo di copiare file su un dispositivo Snowball Edge che ha già raggiunto la piena capacità di archiviazione dei dati.
- Tentativo di copiare file su un dispositivo Snowball Edge che non segue le [linee guida per la denominazione delle chiavi degli oggetti per Amazon S3](#).

Quando si verifica uno di questi errori di convalida, viene registrato. È possibile adottare misure per identificare manualmente quali file non sono stati convalidati e perché. Per informazioni, consultare [Convalida manuale dei dati da un dispositivo Snowball Edge dopo l'importazione in Amazon S3](#).

Convalida manuale dei dati da un dispositivo Snowball Edge dopo l'importazione in Amazon S3

Una volta completato un processo di importazione, sono disponibili diverse opzioni per convalidare manualmente i dati in Amazon S3, come descritto di seguito.

Controllo del rapporto di completamento del processo e dei log associati

Ogni volta che i dati vengono importati o esportati da Amazon S3, ricevi un report di lavoro in PDF scaricabile. Per processi di importazione, questo rapporto diventa disponibile alla fine del processo di importazione. Per ulteriori informazioni, consulta [Ottenimento del report e dei log di completamento del processo di trasferimento dei dati](#).

Inventario S3

Se hai trasferito un'enorme quantità di dati in Amazon S3 in più lavori, l'analisi di ogni report di completamento del lavoro potrebbe non essere un uso efficiente del tempo. Puoi invece creare un inventario di tutti gli oggetti in uno o più bucket Amazon S3. L'inventario di Amazon S3 fornisce un file con valori separati da virgole (CSV) che mostra gli oggetti e i metadati corrispondenti su base giornaliera o settimanale. Questo file copre gli oggetti per un bucket Amazon S3 o un prefisso condiviso (ovvero oggetti i cui nomi iniziano con una stringa comune).

Una volta che hai l'inventario dei bucket Amazon S3 in cui hai importato i dati, puoi facilmente confrontarli con i file che hai trasferito nella posizione dei dati di origine. In questo modo, puoi identificare rapidamente quali file non sono stati trasferiti.

Usa il comando di sincronizzazione di Amazon S3

Se la tua workstation è in grado di connettersi a Internet, puoi eseguire una convalida finale di tutti i file trasferiti eseguendo il comando. AWS CLI `aws s3 sync` Questo comando consente di sincronizzare le directory e i S3 prefissi e di copiare in maniera ricorsiva file nuovi e aggiornati dalla directory di origine nella destinazione. Per ulteriori informazioni, consulta [sync](#) nel AWS CLI Command Reference.

 Important

Se specificate la memoria locale come destinazione per questo comando, assicuratevi di disporre di un backup dei file con cui effettuare la sincronizzazione. Questi file vengono sovrascritti dai contenuti nella fonte Amazon S3 specificata.

Notifiche per Snowball Edge

In che modo Snow utilizza Amazon SNS

Il servizio Snow è progettato per sfruttare le solide notifiche fornite da Amazon Simple Notification Service (Amazon SNS). Durante la creazione di un lavoro per ordinare un dispositivo Snow, puoi fornire indirizzi e-mail per ricevere notifiche relative alle modifiche allo stato del lavoro. Quando lo fai, scegli un argomento SNS esistente o ne crei uno nuovo. Se l'argomento SNS è crittografato, è necessario abilitare la crittografia KMS gestita dal cliente per l'argomento e impostare la politica delle chiavi KMS gestita dal cliente. Per informazioni, consulta [Scegli le preferenze per le notifiche relative al job Snowball Edge](#).

Dopo aver creato il lavoro, ogni indirizzo e-mail che hai specificato per ricevere le notifiche di Amazon SNS riceve un messaggio e-mail dalle AWS notifiche che richiedono la conferma dell'abbonamento all'argomento. Un utente dell'account e-mail deve confermare l'iscrizione selezionando Conferma abbonamento. Le e-mail di notifica di Amazon SNS sono personalizzate per ogni stato del lavoro e includono un collegamento a [Console di gestione della famiglia di servizi AWS Snow](#)

Puoi anche configurare Amazon SNS per inviare messaggi di testo per notifiche di modifica dello stato dalla console Amazon SNS. Per ulteriori informazioni, consulta [Messaggistica SMS](#) nella Guida per sviluppatori di Amazon Simple Notification Service.

Argomenti sulla crittografia di SNS per AWS le modifiche allo stato di Snow Job

Abilita la crittografia KMS gestita dal cliente per l'argomento SNS per le notifiche di modifica dello stato dei lavori Snow. Gli argomenti SNS crittografati con AWS-managed encryption non possono ricevere modifiche allo stato di Snow job perché il ruolo IAM di importazione di Snow non ha accesso alla chiave KMS AWS gestita da Snow per eseguire e eseguire azioni. Decrypt GenerateDataKey Inoltre, le politiche delle chiavi KMS AWS gestite non possono essere modificate.

Per abilitare la crittografia lato server per un argomento SNS utilizzando la console di gestione Amazon SNS

1. [Accedi a Console di gestione AWS e apri la console Amazon SNS nella versione v3/home.
https://console.aws.amazon.com/sns/](#)
2. Nel pannello di navigazione, scegli Topics (Argomenti).

3. Nella pagina Argomenti, scegli l'argomento utilizzato per le notifiche di modifica dello stato del lavoro, quindi scegli Modifica.
4. Espandere la sezione Encryption (Crittografia) e procedere come segue:
 - a. Scegliere Enable encryption (Abilita crittografia).
 - b. Specificate la chiave AWS KMS. See
 - c. Per ogni tipo di KMS, vengono visualizzati la descrizione, l'account e l'ARN KMS.
5. Per utilizzare una chiave personalizzata del tuo AWS account, scegli il campo Chiave AWS KMS, quindi scegli il KMS personalizzato dall'elenco. Per istruzioni sulla creazione di KMS personalizzati, consulta [Creazione di chiavi](#) nella Guida per gli sviluppatori. AWS Key Management Service

Per utilizzare un ARN KMS personalizzato dal tuo account AWS o da un altro account AWS, inserisci l'ARN AWS della chiave KMS nel campo Chiave KMS.

6. Scegli Save changes (Salva modifiche). La crittografia lato server è abilitata per l'argomento e viene visualizzata la pagina dell'argomento.

Impostazione di una politica di chiavi KMS gestita dal cliente per Snow AWS

Dopo aver abilitato la crittografia per gli argomenti SNS che riceveranno notifiche per le modifiche allo stato dei job Snow, aggiorna la politica KMS per la crittografia degli argomenti SNS e consenti al responsabile del servizio Snow le azioni e le azioni. "importexport.amazonaws.com" "kms:Decrypt" "kms:GenerateDataKey*"

Per consentire il ruolo del servizio di importazione ed esportazione nella politica chiave di KMS

1. Accedi Console di gestione AWS e apri la console AWS Key Management Service (AWS KMS) in <https://console.aws.amazon.com/kms>.
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Nell'angolo in alto a destra della console, imposta la Regione AWS stessa area da cui è stato ordinato il dispositivo Snow.
4. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
5. Nell'elenco delle chiavi KMS, scegli l'alias o l'ID della chiave KMS da aggiornare.

6. Scegli la scheda **Politica chiave**, nelle dichiarazioni politiche chiave, puoi vedere i responsabili a cui è stato concesso l'accesso alla chiave KMS dalla politica chiave e puoi vedere le azioni che possono eseguire.
7. Per il responsabile del servizio Snow "importexport.amazonaws.com", aggiungi la seguente dichiarazione politica "kms:Decrypt" e "kms:GenerateDataKey*" le azioni seguenti:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "service.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:service:region:customer-account-id:resource-type/customer-resource-id"
    }
  },
  "StringEquals": {
    "kms:EncryptionContext:aws:sns:topicArn": "arn:aws:sns:your_region:customer-account-id:your_sns_topic_name"
  }
}
```

8. Scegli **Salva modifiche** per applicare le modifiche e uscire dall'editor delle politiche.

Esempi di notifiche Amazon SNS per Snow AWS

Le notifiche di Amazon SNS producono i seguenti messaggi e-mail quando lo stato del lavoro cambia. Questi messaggi sono esempi del protocollo tematico Email-JSON SNS.

Stato di un processo	Notifica SNS (JSON)
Job created (Processo creato)	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) has been created. More info - https://console.aws.amazon. com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAIkP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtN5IbZew3foxgx8GT +1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
Preparazione dell'apparecchiatura	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) is being prepared. More info - https://console.aw s.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAIkP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
Exporting (Esportazione)	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) is being Exported. More info - https://console.aw s.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAIkP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
In transit to you (In transito verso l'utente)	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) is in transit to you. More info - https://console.aw s.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAikP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
Delivered to you (Consegnato all'utente)	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) was delivered to you. More info - https://console.aw s.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAIkP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtN5IbZew3foxgx8GT +1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
In transito verso AWS	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) is in transit to AWS. More info - https://console.aw s.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAikP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
Al centro di smistamento	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) is at AWS sorting facility. More info - https:// console.aws.amazon.com/impor texport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAikP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd507lX1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD0lzmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
In AWS	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) is at AWS. More info - https://console.aws.amazon.com/ importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAikP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
Importing (Importazione)	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) is being imported. More info - https://console.aw s.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAIkP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJ1IyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)
Completato	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) complete.\nThanks for using AWS Snowball Edge.\nCan you take a quick survey on your experienc e? Survey here: http://bit.ly/1pLQ JMY. More info - https://console.aw s.amazon.com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAIkP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNklVypfy+7 Ta1MD01zmJu0rExtSnSIbZew3foxgx8GT +1bZkLd0ZdtdRJLIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Stato di un processo	Notifica SNS (JSON)

Stato di un processo	Notifica SNS (JSON)
Annullato	<pre> { "Type" : "Notification", "MessageId" : "dc1e94d9-56c5-5e9 6-808d-cc7f68faa162", "TopicArn" : "arn:aws:sns:us-ea st-2:111122223333:ExampleTopic1", "Message" : "Your job Job-name (JID8bca334a-6c2f-4cd0-97e2 -3f5a4dc9bd6d) was canceled. More info - https://console.aws.amazon. com/importexport", "Timestamp" : "2023-02-23T00:27: 58.831Z", "SignatureVersion" : "1", "Signature" : "FMG5t1ZhJNHLHUXvZ gtZz1k24FzVa7oX0T4P03neeXw8 ZEXZx6z35j2F0TuNYShn2h0bKNC/ zLTnMyIxEzmi2X1sh0BWsJHkrW2xkR58ABZ F+4uWHEE73yDVR4SyYAikP9jstZzDRm +bcVs8+T0yaLiEGLrIIIL4esi11lhIkG ErCuy5btPcWXBdio2fpCRD5x9oR 6gmE/rd5071X1c1uvnv4r1Lkk4pqP2/ iUfxFZva1xLSRvgyfm6D9hNk1VyPfy+7 Ta1MD01zmJu0rExtnSIbZew3foxgx8GT +1bZkLd0ZdtdRJlIyPRP44eyq78sU0Eo/ LsDr0Iak4ZDpg8dXg==", "SigningCertURL" : "https:// sns.us-east-1.amazonaws.com/ SimpleNotificationService-010a507c1 833636cd94bdb98bd93083a.pem", "UnsubscribeURL" : "https:// sns.us-east-2.amazonaws.com/? Action=Unsubscribe&SubscriptionArn =arn:aws:sns:us-east-2:1111 22223333:ExampleTopic1:e103 9402-24e7-40a3-a0d4-797da162b297" } </pre>

Registrazione delle chiamate AWS Snowball Edge API con AWS CloudTrail

Il servizio AWS Snowball o Snowball Edge si integra con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o servizio. CloudTrail acquisisce tutte le chiamate API per il servizio AWS Snowball Edge. Le chiamate acquisite includono chiamate dalla console AWS Snowball Edge Family e chiamate in codice all'API AWS Snowball Edge Family Job Management. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per le chiamate AWS Snowball Edge Family API. 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, puoi determinare la richiesta effettuata con AWS Snowball Edge Family API, l'indirizzo IP della richiesta effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

AWS Snowball Edge informazioni in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in AWS Snowball Edge, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con cronologia degli CloudTrail eventi](#) nella Guida AWS CloudTrail per l'utente.

Per una registrazione continua degli eventi del tuo sito Account AWS, inclusi gli eventi di AWS Snowball Edge, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni AWS. Il trail registra gli eventi da tutti gli Regioni AWS elementi della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di AWS CloudTrail :

- [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 azioni di gestione dei lavori sono documentate nell'[AWS Snowball Edge API Reference](#) e vengono registrate CloudTrail con le seguenti eccezioni:

- L'[CreateAddress](#) operazione non viene registrata per proteggere le informazioni sensibili dei clienti.
- Tutte le chiamate API di sola lettura (per le operazioni API che iniziano con il prefisso Get, Describe o List) non registrano elementi di risposta.

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 root o AWS Identity and Access Management (utente 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, vedete l'[elemento CloudTrail UserIdentity nella Guida](#) per l'AWS CloudTrail utente.

Informazioni sulle voci dei file di registro per AWS Snowball Edge

Un trail è una configurazione che consente la distribuzione 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 dimostra l'[DescribeJob](#) operazione.

```
{
  "Records": [
    {
      "eventVersion": "1.05",
```

```
"userIdentity": {
  "type": "Root",
  "principalId": "111122223333",
  "arn": "arn:aws:iam::111122223333:root",
  "accountId": "111122223333",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {"attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2019-01-22T21:58:38Z"
  }},
  "invokedBy": "signin.amazonaws.com"
},
"eventTime": "2019-01-22T22:02:21Z",
"eventSource": "snowball.amazonaws.com",
"eventName": "DescribeJob",
"awsRegion": "eu-west-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "signin.amazonaws.com",
"requestParameters": {"jobId": "JIDa1b2c3d4-0123-abcd-1234-0123456789ab"},
"responseElements": null,
"requestID": "12345678-abcd-1234-abcd-ab0123456789",
"eventID": "33c7ff7c-3efa-4d81-801e-7489fe6ffff62",
"eventType": "AwsApiCall",
"recipientAccountId": "444455556666"
}
}}
```

AWS Snowball Edge quote

Di seguito, puoi trovare informazioni sulle limitazioni all'uso del AWS Snowball Edge dispositivo.

Important

Quando trasferisci dati in Amazon Simple Storage Service (Amazon S3) utilizzando Snowball Edge, tieni presente che le dimensioni dei singoli oggetti Amazon S3 possono variare da un minimo di 0 byte a un massimo di 5 terabyte (TB).

Disponibilità regionale per AWS Snowball Edge

La tabella seguente evidenzia le regioni in cui AWS Snowball Edge è disponibile.

Regione	Disponibilità di Snowball Edge
Stati Uniti orientali (Ohio)	✓
Stati Uniti orientali (Virginia settentrionale)	✓
Stati Uniti occidentali (California settentrionale)	✓
US West (Oregon)	✓
AWS GovCloud (Stati Uniti orientali)	✓
AWS GovCloud (Stati Uniti occidentali)	✓
Canada (Centrale)	✓
Asia Pacifico (Giacarta)	✓
Asia Pacifico (Mumbai)	✓
Asia Pacific (Osaka)	✓
Asia Pacific (Seul)	✓
Asia Pacifico (Singapore)	✓

Regione	Disponibilità di Snowball Edge
Asia Pacifico (Sydney)	✓
Asia Pacifico (Tokyo)	✓
Europa (Francoforte)	✓
Europa (Irlanda)	✓
Europa (Londra)	✓
Europa (Milano)	✓
Europa (Parigi)	✓
Europa (Stoccolma)	✓
Medio Oriente (Emirati Arabi Uniti)	✓
Sud America (San Paolo)	✓

Per informazioni sulle AWS regioni e gli endpoint supportati, consulta [Endpoint e quote AWS Snowball Edge](#) nel Riferimenti generali di AWS

Limitazioni per i lavori AWS Snowball Edge

Esistono le seguenti limitazioni per la creazione di lavori AWS Snowball Edge relativi ai dispositivi:

- Per motivi di sicurezza, i lavori che utilizzano un AWS Snowball Edge dispositivo devono essere completati entro 360 giorni dalla preparazione. Se devi conservare uno o più dispositivi per più di 360 giorni, consulta [Aggiornamento del certificato SSL sui dispositivi Snowball Edge](#). Altrimenti, dopo 360 giorni, il dispositivo si blocca, non è più accessibile e deve essere restituito. Se il AWS Snowball Edge dispositivo si blocca durante un processo di importazione, possiamo comunque trasferire i dati esistenti sul dispositivo in Amazon S3.
- AWS Snowball Edge supporta la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3) e la crittografia lato server con chiavi gestite (SSE-KMS). AWS Key Management Service Lo storage compatibile con Amazon S3 su Snowball Edge supporta SSE-C per processi

di elaborazione e storage locali. Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia lato server](#) nella Guida per l'utente di Amazon Simple Storage Service.

- Se utilizzi un AWS Snowball Edge dispositivo per importare dati e devi trasferire più dati di quanti ne possa contenere un singolo dispositivo Snowball Edge, crea ulteriori job. Ogni processo di esportazione può utilizzare più dispositivi Snowball Edge.
- Il limite di servizio predefinito per il numero di dispositivi Snowball Edge che puoi avere contemporaneamente è 1 per account, per. Regione AWS Se desideri aumentare il limite del servizio o creare un job in cluster, contatta [Supporto AWS](#).
- I metadati per gli oggetti trasferiti su un dispositivo non vengono mantenuti. Gli unici metadati che rimangono inalterati sono filename e filesize. Tutti gli altri metadati sono impostati come nell'esempio seguente:

```
-rw-rw-r-- 1 root root [filesize] Dec 31 1969 [path/filename]
```

Limiti di velocità su AWS Snowball Edge

Il Rate Limiter viene utilizzato per controllare la frequenza delle richieste in un ambiente di cluster di server.

Limite di connessione dell'adattatore Amazon Snow S3

Il limite massimo di connessioni è 1000 per Snowball Edge su Amazon S3. Tutte le connessioni oltre 1000 vengono interrotte.

Limitazioni al trasferimento di dati locali con un dispositivo Snowball Edge

Esistono le seguenti limitazioni per il trasferimento di dati da o verso un AWS Snowball Edge dispositivo locale:

- Durante la scrittura lo stato dei file deve essere statico. I file modificati durante il trasferimento non vengono importati in Amazon S3.
- I frame jumbo non sono supportati, ovvero i frame Ethernet con più di 1500 byte di payload.
- Quando selezioni i dati da esportare, tieni presente che gli oggetti con barre finali nel nome (/o\) non vengono trasferiti. Prima di esportare eventuali oggetti con barre finali, aggiorna i relativi nomi per rimuovere la barra.

- Quando si utilizza il trasferimento dati multiparte, la dimensione massima della parte è di 2 GiB.

Quote per le istanze di calcolo su un dispositivo Snowball Edge

Di seguito sono riportate le quote di archiviazione e le limitazioni delle risorse condivise per le risorse di elaborazione su un dispositivo. AWS Snowball Edge

Calcolo delle quote di storage delle risorse su Snowball Edge

Lo storage disponibile per le risorse di elaborazione è una risorsa separata dallo storage Amazon S3 dedicato su un dispositivo Snowball Edge. Le quote per lo storage sono le seguenti:

Un dispositivo ottimizzato per il calcolo Snowball Edge può eseguire fino a 20 AMIs e 10 volumi per istanza.

Tipo di istanza	Core vCPU	Memoria (GiB)	Opzione del dispositivo supportata
sbe1.small	1	1	ottimizzato per lo storage
sbe1.medium	1	2	ottimizzato per lo storage
sbe1.large	2	4	ottimizzato per lo storage

Tipo di istanza	Core vCPU	Memoria (GiB)	Opzione del dispositivo supportata	
sbe1.xlarge	4	8	ottimizzato per lo storage	
sbe1.2xlarge	8	16	ottimizzato per lo storage	
sbe1.4xlarge	16	32	ottimizzato per lo storage	
sbe1.6xlarge	24	32	ottimizzato per lo storage	
sbe-c.small	1	2	ottimizzato per il calcolo	
sbe-c.medium	1	4	ottimizzato per il calcolo	

Tipo di istanza	Core vCPU	Memoria (GiB)	Opzione del dispositivo supportata	
sbe-c.large	2	8	ottimizzato per il calcolo	
sbe-c.xlarge	4	16	ottimizzato per il calcolo	
sbe-c.2xlarge	8	32	ottimizzato per il calcolo	
sbe-c.4xlarge	16	64	ottimizzato per il calcolo	
sbe-c.8xlarge	32	128	ottimizzato per il calcolo	
sbe-c.12xlarge	48	192	ottimizzato per il calcolo	

Tipo di istanza	Core vCPU	Memoria (GiB)	Opzione del dispositivo supportata
sbe-c.16xlarge	64	256	ottimizzato per il calcolo
sbe-c.24xlarge	96	384	ottimizzato per il calcolo

Limitazioni delle risorse di elaborazione condivise su Snowball Edge

Tutti i servizi su un dispositivo Snowball Edge utilizzano alcune delle risorse limitate del dispositivo. Un dispositivo Snowball Edge con le risorse di elaborazione disponibili massimizzate non può lanciare nuove risorse di elaborazione. Ad esempio, se si tenta di avviare l'interfaccia NFS mentre si esegue anche un'istanza di sbe1.4xlarge calcolo su un dispositivo ottimizzato per lo storage, il servizio di interfaccia NFS non si avvia. Quanto segue illustra le risorse disponibili sulle diverse opzioni del dispositivo, nonché i requisiti delle risorse per ciascun servizio.

- Se non vi sono servizi di elaborazione impostati su ACTIVE:
 - Con un'opzione ottimizzata per lo storage, hai a disposizione 24 v CPUs e 32 GiB di memoria per le tue istanze di calcolo.
 - Con un'opzione ottimizzata per l'elaborazione, hai a disposizione 104 v CPUs e 208 GiB di memoria per le tue istanze di calcolo.
- Benché AWS IoT Greengrass e AWS Lambda alimentato da: AWS IoT Greengrass ACTIVE
 - Su un'opzione ottimizzata per lo storage, questi servizi utilizzano 4 core vCPU e 8 GiB di memoria.

- Su un'opzione ottimizzata per il calcolo, questi servizi utilizzano 1 core vCPU e 1 GiB di memoria.
- Sebbene l'interfaccia NFS sia disponibile ACTIVE, utilizza 8 core vCPU e 16 GiB di memoria su un dispositivo Snowball Edge.
- Sebbene lo storage compatibile con Amazon S3 su Snowball Edge sia ATTIVO su Snowball Edge Compute Optimized con AMD EPYC Gen2 e NVME, per un singolo nodo con la configurazione minima di 3 TB di storage compatibile con Amazon S3 su Snowball Edge, utilizza 8 core vCPU e 16 GB di memoria. Per un singolo nodo con più di 3 TB di storage compatibile con Amazon S3 su Snowball Edge, utilizza 20 core vCPU e 40 GB di memoria. Per un cluster, utilizza 20 core vCPU e 40 GB di memoria.

È possibile determinare se un servizio si trova ACTIVE su uno Snowball Edge utilizzando il comando `snowballEdge describe-service` sul client Snowball Edge. Per ulteriori informazioni, consulta [Visualizzazione dello stato dei servizi in esecuzione su Snowball Edge](#).

Limitazioni alla spedizione di un dispositivo Snowball Edge Edge

Esistono le seguenti limitazioni per la spedizione di un AWS Snowball Edge dispositivo:

- AWS non spedisce un dispositivo Snowball Edge Edge a una casella postale.
- AWS non spedisce un dispositivo Snowball Edge tra regioni diverse dagli Stati Uniti, ad esempio dall'UE (Irlanda) all'UE (Francoforte) o all'Asia Pacifico (Sydney).
- Lo spostamento di un dispositivo Snowball Edge a un indirizzo diverso dal Paese specificato al momento della creazione del lavoro non è consentito e costituisce una violazione dei termini del AWS servizio.

Per ulteriori informazioni sulla spedizione, consulta [Considerazioni sulla spedizione per Snowball Edge](#).

Limitazioni all'elaborazione di uno Snowball Edge Edge restituito per l'importazione

Per importare i dati AWS, il dispositivo deve soddisfare i seguenti requisiti:

- Il AWS Snowball Edge dispositivo non deve essere compromesso. Fatta eccezione per l'apertura delle tre porte sulla parte anteriore, posteriore e superiore o per aggiungere e sostituire il filtro dell'aria opzionale, non aprire il AWS Snowball Edge dispositivo per nessun motivo.
- Il dispositivo non deve essere fisicamente danneggiato. Puoi prevenire i danni chiudendo le tre porte del dispositivo Snowball Edge Edge fino a quando le chiusure non emettono un suono udibile.
- Il display E Ink sul dispositivo Snowball Edge Edge deve essere visibile. Deve inoltre mostrare l'etichetta di reso che è stata generata automaticamente al termine del trasferimento dei dati sul AWS Snowball Edge dispositivo.

 Note

Tutti i dispositivi Snowball Edge Edge restituiti che non soddisfano questi requisiti vengono cancellati senza che sia stato eseguito alcun intervento.

Risoluzione dei problemi AWS Snowball Edge

Tieni a mente le seguenti linee guida generali durante la risoluzione dei problemi.

- Gli oggetti in Amazon S3 hanno una dimensione massima del file di 5 TB.
- Gli oggetti trasferiti su un AWS Snowball Edge dispositivo hanno una lunghezza massima della chiave di 933 byte. I nomi chiave che includono caratteri che richiedono più di 1 byte ciascuno comunque hanno una lunghezza chiave massima di 933 byte. Durante la determinazione della lunghezza della chiave, includi il nome del file o dell'oggetto, nonché il relativo percorso o i prefissi. In questo modo, i file con nomi brevi all'interno di un percorso fortemente nidificato possono avere chiavi lunghe più di 933 byte. Il nome del bucket non viene conteggiato nel percorso durante la determinazione della lunghezza della chiave. Di seguito sono riportati alcuni esempi.

Nome dell'oggetto	Nome bucket	Percorso più nome del bucket	Lunghezza chiave
sunflower-1.jpg	pictures	sunflower-1.jpg	15 caratteri
receipts.csv	MyTaxInfo	/Users/Eric/Documents/2016/January/	47 caratteri
bhv.1	\$7\$zWwwXKQj\$gLA0oZCj\$r8p	/.VfV/FqGC3QN\$7BXys3KHYePfuIOMNjY83dVxugPY1xVg/evpcQEJLT/rSwZc\$M1VVf/\$hwefVISRqwepB\$/BiiD/PP	135 caratteri

Nome dell'oggetto	Nome bucket	Percorso più nome del bucket	Lunghezza chiave

F\$tWRAjxD
/fIMp/0NY

- Per motivi di sicurezza, i lavori che utilizzano un AWS Snowball Edge dispositivo devono essere completati entro 360 giorni dalla preparazione. Se devi conservare uno o più dispositivi per più di 360 giorni, consulta [Aggiornamento del certificato SSL sui dispositivi Snowball Edge](#). Altrimenti, dopo 360 giorni, il dispositivo si blocca, non è più accessibile e deve essere restituito. Se il AWS Snowball Edge dispositivo si blocca durante un processo di importazione, possiamo comunque trasferire i dati esistenti sul dispositivo in Amazon S3.
- Se riscontri errori imprevisti durante l'utilizzo di un AWS Snowball Edge dispositivo, desideriamo saperne di più. Copia i registri pertinenti e includili insieme a una breve descrizione dei problemi riscontrati in un messaggio a Supporto AWS. Per ulteriori informazioni sui log, consulta [Configurazione e utilizzo del client Snowball Edge](#).

Argomenti

- [Come identificare uno Snowball Edge](#)
- [Risoluzione dei problemi di avvio con Snowball Edge](#)
- [Risoluzione dei problemi di connessione con Snowball Edge](#)
- [Risoluzione dei problemi relativi ai unlock-device comandi con Snowball Edge](#)
- [Risoluzione dei problemi relativi alle credenziali con Snowball Edge](#)
- [Risoluzione dei problemi di trasferimento dei dati con Snowball Edge](#)
- [Risoluzione dei AWS CLI problemi con Snowball Edge](#)
- [Risoluzione dei problemi delle istanze di calcolo su Snowball Edge](#)

Come identificare uno Snowball Edge

Usa il `describe-device` comando per trovare il tipo di dispositivo, quindi cerca il valore restituito `DeviceType` nella tabella seguente per determinare la configurazione.


```
snowballEdge describe-device
```

Example di **describe-device** output

```
{
  "DeviceId" : "JID-206843500001-35-92-20-211-23-06-02-18-24",
  "UnlockStatus" : {
    "State" : "UNLOCKED"
  },
  ...
  "DeviceType" : "V3_5C"
}
```

DeviceType configurazioni dei dispositivi Snowball Edge

DeviceType value	Configurazione del dispositivo
V3_5C	Snowball Edge ottimizzato per il calcolo con AMD EPYC Gen2 e NVME
V3_5S	210 TB ottimizzati per lo storage con Snowball Edge

Per ulteriori informazioni sulle configurazioni dei dispositivi Snowball Edge, vedere. [AWS Snowball Edge informazioni sull'hardware del dispositivo](#)

Risoluzione dei problemi di avvio con Snowball Edge

Le seguenti informazioni possono aiutarti a risolvere alcuni problemi che potresti riscontrare durante l'avvio di Snowball Edge.

- Attendi 10 minuti per l'avvio di un dispositivo. Evita di spostare o utilizzare il dispositivo durante questo periodo.
- Assicurarsi che entrambe le estremità del cavo di alimentazione siano collegate saldamente.
- Sostituisci il cavo di alimentazione con un altro cavo che ritieni sia in buone condizioni.
- Collega il cavo di alimentazione a un'altra fonte di alimentazione che ritieni sia buona.

Risoluzione dei problemi relativi al display LCD di un dispositivo Snowball Edge durante l'avvio

A volte, dopo l'accensione di un dispositivo Snowball Edge, il display LCD può presentare un problema.

- Lo schermo LCD è nero e non visualizza alcuna immagine dopo aver collegato il dispositivo Snowball Edge all'alimentazione e aver premuto il pulsante di accensione sopra lo schermo LCD.
- Lo schermo LCD non supera le impostazioni impostate per Snowball Edge, l'operazione potrebbe richiedere alcuni minuti. messaggio e la schermata di configurazione della rete non viene visualizzata.

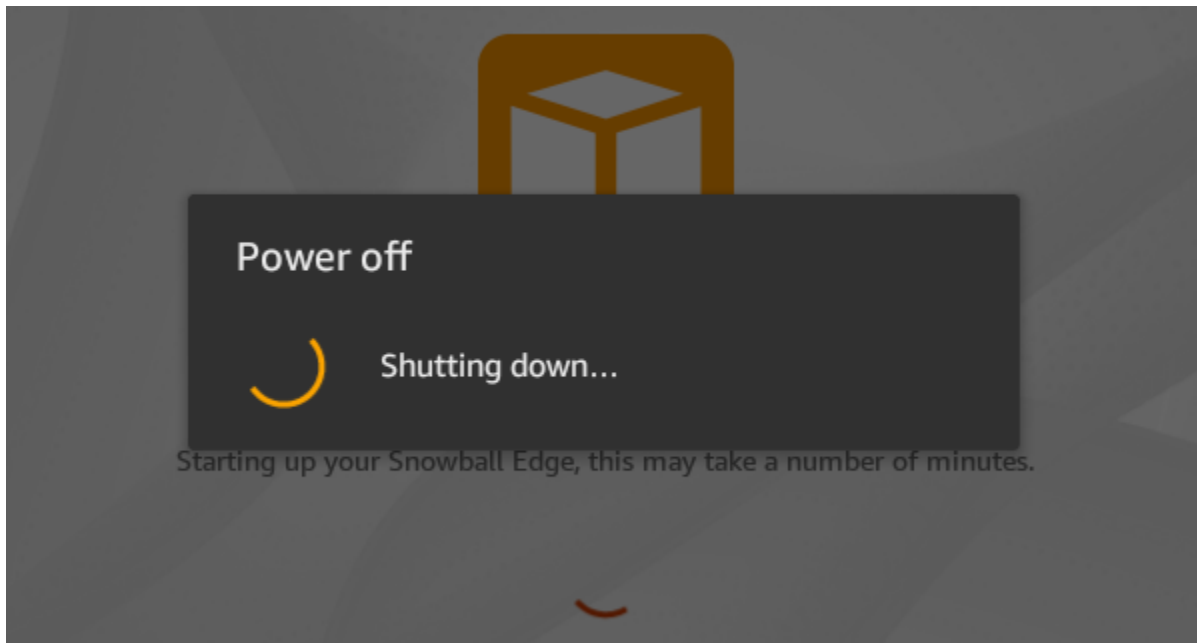


Azione da eseguire quando lo schermo LCD è nero dopo aver premuto il pulsante di accensione

1. Assicurati che il dispositivo Snowball Edge sia collegato a una fonte di alimentazione e che la fonte di alimentazione fornisca energia.
2. Lascia il dispositivo collegato alla fonte di alimentazione per 1 o 2 ore. Assicurati che le porte anteriori e posteriori del dispositivo siano aperte.
3. Ritorna al dispositivo e lo schermo LCD sarà pronto per l'uso.

Azione da intraprendere quando Snowball Edge non passa alla schermata di configurazione della rete

1. Lascia che lo schermo rimanga sulle impostazioni di Snowball Edge, l'operazione potrebbe richiedere alcuni minuti. messaggio per 10 minuti.
2. Sullo schermo, scegli il pulsante Riavvia lo schermo. Verrà visualizzato il messaggio Spegnimento..., quindi l'impostazione di Snowball Edge. L'operazione potrebbe richiedere alcuni minuti. verrà visualizzato un messaggio e il dispositivo si avvierà normalmente.



Se lo schermo LCD non supera le impostazioni di Snowball Edge, l'operazione potrebbe richiedere alcuni minuti. messaggio dopo aver usato il pulsante Riavvia lo schermo, utilizzare la seguente procedura.

Operazione da eseguire

1. Sopra lo schermo LCD, premere il pulsante di accensione per spegnere il dispositivo.
2. Scollegare tutti i cavi dal dispositivo.
3. Lascia il dispositivo spento e scollegato per 20 minuti.
4. Connect i cavi di alimentazione e di rete.
5. Sopra lo schermo LCD, premi il pulsante di accensione per accendere il dispositivo.

Se il problema persiste, contattateci Supporto AWS per restituire il dispositivo e ricevere un nuovo dispositivo Snowball Edge.

Risoluzione dei problemi relativi al display E Ink durante l'avvio

A volte, dopo aver acceso un dispositivo Snowball Edge, il display E Ink sulla parte superiore del dispositivo può visualizzare il seguente messaggio:

The appliance has timed out

Questo messaggio non indica un problema con il dispositivo. Usalo normalmente e quando lo spegni per restituirlo AWS, le informazioni sulla spedizione del reso appariranno come previsto.

Risoluzione dei problemi di connessione con Snowball Edge

Le seguenti informazioni possono aiutarti a risolvere alcuni problemi che potresti riscontrare con la connessione a Snowball Edge:

- I router e gli switch che funzionano a una velocità di 100 megabyte al secondo non funzionano con Snowball Edge. Ti consigliamo di utilizzare uno switch che funziona a una velocità di 1 GB al secondo (o superiore).
- Se riscontri strani errori di connessione con il dispositivo, spegni Snowball Edge, scollega tutti i cavi e lascialo agire per 10 minuti. Trascorsi 10 minuti, riavvia il dispositivo e riprova.
- Assicurati che nessun software antivirus o firewall blocchi la connessione di rete del dispositivo Snowball Edge.
- Tieni presente che l'interfaccia NFS e l'interfaccia Amazon S3 hanno indirizzi IP diversi.

Per la risoluzione di problemi di connessione più avanzati, puoi procedere come segue:

- Se non riesci a comunicare con Snowball Edge, esegui il ping dell'indirizzo IP del dispositivo. Se il ping restituisce no connect, conferma l'indirizzo IP del dispositivo e conferma la configurazione di rete locale.
- Se l'indirizzo IP è corretto e le spie sul retro del dispositivo lampeggiano, usa telnet per testare il dispositivo sulle porte 22, 9091 e 8080. La porta di test 22 determina se Snowball Edge funziona correttamente. La porta di test 9091 determina se AWS CLI è possibile utilizzarla per inviare comandi al dispositivo. La porta di test 8080 aiuta a garantire che il dispositivo possa scrivere nei bucket Amazon S3 su di esso solo con l'adattatore S3. Se riesci a connetterti alla porta 22 ma non

alla porta 8080, spegni innanzitutto il dispositivo Snowball Edge e quindi scollega tutti i cavi. Lascia riposare il dispositivo per 10 minuti, quindi ricollegalo e ricomincia.

Risoluzione dei problemi relativi ai **unlock-device** comandi con Snowball Edge

Se il `unlock-device` comando viene restituito `connection refused`, è possibile che tu abbia digitato male la sintassi del comando o che la configurazione del computer o della rete impedisca al comando di raggiungere il dispositivo Snow. Esegui queste azioni per risolvere la situazione:

1. Assicurati che il comando sia stato inserito correttamente.
 - a. Utilizzate lo schermo LCD del dispositivo per verificare che l'indirizzo IP utilizzato nel comando sia corretto.
 - b. Assicuratevi che il percorso del file manifesto utilizzato nel comando sia corretto, incluso il nome del file.
 - c. Usa la [console di gestione AWS Snowball Edge](#) per verificare che il codice di sblocco utilizzato nel comando sia corretto.
2. Assicurati che il computer che stai utilizzando sia sulla stessa rete e sottorete del dispositivo Snow.
3. Assicurati che il computer che stai utilizzando e la rete siano configurati per consentire l'accesso al dispositivo Snow. Usa il `ping` comando del tuo sistema operativo per determinare se il computer è in grado di raggiungere il dispositivo Snow tramite la rete. Controlla le configurazioni del software antivirus, della configurazione del firewall, della rete privata virtuale (VPN) o altre configurazioni del computer e della rete.

Risoluzione dei problemi relativi ai file manifest con Snowball Edge

Ogni processo è associato a un determinato file manifest. Se crei più processi, è consigliabile tenere traccia dei manifest e del relativo processo.

Se perdi un file manifesto o se un file manifesto è danneggiato, potete scaricare nuovamente il file manifesto per un lavoro specifico. Puoi farlo utilizzando la AWS CLI console o uno dei AWS APIs.

Se si esegue un aggiornamento su Snowball Edge, è necessario scaricare e utilizzare un nuovo file manifesto per il job. Per informazioni sul download di un file manifesto, consulta [Ottenere le credenziali per accedere a Snowball Edge](#).

Risoluzione dei problemi relativi alle credenziali con Snowball Edge

Utilizza i seguenti argomenti per risolvere i problemi relativi alle credenziali con il dispositivo Snowball Edge.

Impossibile individuare le AWS CLI credenziali per Snowball Edge

Se comunichi con il AWS Snowball Edge dispositivo tramite l'interfaccia Amazon S3 utilizzando AWS CLI il, potresti ricevere un messaggio di errore che dice «Impossibile individuare le credenziali». Puoi configurare le credenziali eseguendo «aws configure».

Operazione da eseguire

Configura AWS le credenziali che AWS CLI utilizza per eseguire i comandi al posto tuo. Per ulteriori informazioni, consulta [Configurazione della AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface .

Risoluzione dei problemi relativi al messaggio di errore di Snowball Edge: verifica della chiave di accesso segreta e della firma

Quando si utilizza l'interfaccia Amazon S3 per trasferire dati su Snowball Edge, è possibile che venga visualizzato il seguente messaggio di errore.

```
An error occurred (SignatureDoesNotMatch) when calling the CreateMultipartUpload
operation: The request signature we calculated does not match the signature you
provided.
Check your AWS secret access key and signing method. For more details go to:
http://docs.aws.amazon.com/AmazonS3/latest/dev/
RESTAuthentication.html#ConstructingTheAuthenticationHeader
```

Operazione da eseguire

Ottieni le tue credenziali dal client Snowball Edge. Per ulteriori informazioni, consulta [Ottenere le credenziali per uno Snowball Edge](#).

Risoluzione dei problemi di trasferimento dei dati con Snowball Edge

Se riscontri problemi di prestazioni durante il trasferimento dei dati da o verso Snowball Edge, consulta [Consigli per ottimizzare le prestazioni di trasferimento dei dati da o verso uno Snowball Edge](#) per i suggerimenti e le indicazioni su come migliorare le prestazioni di trasferimento. Le seguenti indicazioni ti consentono di risolvere i problemi che possono verificarsi con il trasferimento dei dati da o verso un dispositivo Snowball Edge:

- Non è possibile trasferire dati nella directory principale di Snowball Edge. In caso di problemi durante il trasferimento di dati nel dispositivo, assicurati che il trasferimento sia diretto a una sottodirectory. Le sottodirectory di primo livello hanno i nomi dei bucket Amazon S3 che hai incluso nel job. Inserisci i dati in quelle sottodirectory.
- Se usi Linux e non riesci a caricare file con caratteri UTF-8 su un AWS Snowball Edge dispositivo, è possibile che il tuo server Linux non riconosca la codifica dei caratteri UTF-8. Puoi risolvere questo problema installando il pacchetto `locales` sul server Linux e configurarlo per l'utilizzo di una delle impostazioni locali UTF-8, ad esempio `en_US.UTF-8`. Puoi configurare il pacchetto `locales` esportando la variabile di ambiente `LC_ALL`, ad esempio: `export LC_ALL=en_US.UTF-8`
- Quando usi l'interfaccia Amazon S3 con AWS CLI, puoi lavorare con file o cartelle con spazi nel nome, ad esempio `my photo.jpg` o `My Documents`. Tuttavia, accertati di gestire gli spazi correttamente. Per ulteriori informazioni, consulta [Specificare i valori dei parametri per la AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Risoluzione dei problemi relativi ai processi di importazione con Snowball Edge

A volte i file non vengono importati in Amazon S3. Se si verifica il problema seguente, prova a eseguire le operazioni specificate per risolverlo. Se non è possibile importare un file, potrebbe essere necessario ripetere l'operazione. Per importarlo nuovamente potrebbe essere necessario un nuovo processo per Snowball Edge.

Impossibile importare i file in Amazon S3 a causa di caratteri non validi nei nomi degli oggetti

Questo problema si verifica se il nome di un file o di una cartella contiene caratteri non supportati da Amazon S3. Amazon S3 prevede regole su quali caratteri possono essere presenti nei nomi degli oggetti. Per ulteriori informazioni, consulta [Creating object key names](#) in Amazon S3 User Guide.

Operazione da eseguire

Se si verifica questo problema, nel rapporto di completamento del processo viene visualizzato un elenco di file e cartelle che non è stato possibile importare.

In alcuni casi, l'elenco è eccessivamente grande o i file nell'elenco sono troppo grandi per essere trasferiti su Internet. In questi casi, è necessario creare un nuovo processo di importazione Snowball, modificare i nomi di file e cartelle per conformarli alle regole di Amazon S3 e trasferire nuovamente i file.

Se i file sono piccoli e non ce n'è un gran numero, puoi copiarli su Amazon S3 tramite AWS CLI o il Console di gestione AWS. Per ulteriori informazioni, vedi [Come si caricano file e cartelle in un bucket S3?](#) nella Guida per l'utente di Amazon Simple Storage Service.

Risoluzione dei problemi relativi ai processi di esportazione con Snowball Edge

A volte non è possibile esportare i file nella workstation. Se si verifica il problema seguente, prova a eseguire le operazioni specificate per risolverlo. Se non è possibile esportare un file, potrebbe essere necessario ripetere l'operazione. Per esportarlo nuovamente potrebbe essere necessario un nuovo processo per Snowball Edge.

Impossibile esportare i file in un Microsoft Windows Server

Potrebbe non essere possibile esportare un file in un Microsoft Windows Server se il formato del file o di una cartella correlata non è supportato da Windows. Ad esempio, se il nome del file o della cartella contiene i due punti (:), l'esportazione non riesce perché Windows non accetta quel carattere nei nomi di file o cartelle.

Operazione da eseguire

1. Creare un elenco dei nomi che causano l'errore. I nomi dei file e delle cartelle che non è possibile esportare sono disponibili nei log. Per ulteriori informazioni, consulta [Visualizzazione e download dei log da Snowball Edge](#).
2. Modifica i nomi degli oggetti in Amazon S3 che causano il problema per rimuovere o sostituire i caratteri non supportati.

3. Se l'elenco dei nomi è eccessivamente grande o i file nell'elenco sono troppo grandi per essere trasferiti su Internet, creare un nuovo processo di esportazione appositamente per tali oggetti.

Se i file sono piccoli e non ce ne sono molti, copia gli oggetti rinominati da Amazon S3 tramite o AWS CLI il. Console di gestione AWS Per ulteriori informazioni, consulta [Come faccio a scaricare un oggetto da un bucket S3?](#) nella Guida per l'utente di Amazon Simple Storage Service.

Risoluzione dei problemi dell'interfaccia NFS con Snowball Edge

Snowball Edge può indicare che lo stato dell'interfaccia NFS è. DEACTIVATED Ciò potrebbe verificarsi se Snowball Edge è stato spento senza prima arrestare l'interfaccia NFS.

Operazione da eseguire

Per risolvere il problema, arrestate e riavviate il servizio NFS utilizzando la procedura seguente.

1. Utilizzate il `describe-service` comando per determinare lo stato del servizio:

```
snowballEdge describe-service --service-id nfs
```

Il comando restituisce quanto segue.

```
{
  "ServiceId" : "nfs",
  "Status" : {
    "State" : "DEACTIVATED"
  }
}
```

2. Utilizzare il `stop-service` comando per interrompere il servizio NFS.

```
snowballEdge stop-service --service-id nfs
```

3. Utilizzare il `start-service` comando per avviare il servizio NFS. Per ulteriori informazioni, vedere [Gestione dell'interfaccia NFS](#).

```
snowballEdge start-service --virtual-network-interface-arns vni-arn --service-id  
nfs --service-configuration AllowedHosts=0.0.0.0/0
```

4. Utilizzate il `describe-service` comando per assicurarvi che il servizio sia in esecuzione.

```
snowballEdge describe-service --service-id nfs
```

Se il valore del State nome è `ACTIVE`, il servizio di interfaccia NFS è attivo.

```
{  
  "ServiceId" : "nfs",  
  "Status" : {  
    "State" : "ACTIVE"  
  },  
  "Endpoints" : [ {  
    "Protocol" : "nfs",  
    "Port" : 2049,  
    "Host" : "192.0.2.0"  
  } ],  
  "ServiceConfiguration" : {  
    "AllowedHosts" : [ "10.24.34.0/23", "198.51.100.0/24" ]  
  }  
}
```

Risoluzione di un errore di accesso negato durante il trasferimento di dati tramite l'interfaccia S3

Quando si utilizza l'interfaccia S3 per trasferire dati da o verso un dispositivo Snowball Edge, è possibile che si verifichi un errore di accesso negato. Questo errore può essere il risultato di policy relative agli utenti o ai bucket di IAM.

Operazione da eseguire

1. Controlla la policy del bucket S3 che stai utilizzando per i seguenti problemi di sintassi.

- a. Se la policy consente il caricamento dei dati solo se vengono passate le intestazioni KMS, assicurati che la policy specifichi un ARN principale anziché un ID utente. L'esempio seguente mostra la sintassi corretta.

```
{
  "Sid": "Statement3",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "StringNotLike": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/JohnDoe"
    },
    "StringNotEquals": {
      "s3:x-amz-server-side-encryption": [
        "aws:kms",
        "AES256"
      ]
    }
  }
},
{
  "Sid": "Statement4",
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "StringNotLike": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/JohnDoe"
    },
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
}
```

- b. Se la policy del bucket consente il caricamento nel bucket solo se vengono passate le intestazioni corrette, i caricamenti dai dispositivi Snowball Edge non passano alcuna

installazione per impostazione predefinita. Modifica la policy per consentire un'eccezione per l'utente IAM utilizzato per caricare i dati. Di seguito è riportato un esempio della sintassi corretta a tale scopo.

```
{
  "Sid": "Statement3",
  "Effect": "Deny",
  "Principal": "",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/",
  "Condition": {
    "StringNotEquals": {
      "s3:x-amz-server-side-encryption": "AES256"
    },
    "StringNotLike": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/JohnDoe"
    }
  }
},
{
  "Sid": "Statement4",
  "Effect": "Deny",
  "Principal": "",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/JohnDoe"
    }
  }
}
}
```

2. Controlla la politica della chiave KMS che stai utilizzando per la sintassi corretta nell'elemento Principal. L'esempio seguente mostra la sintassi corretta.

```
{
  "Sid": "Statement2",
```

```

    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:role/service-role/JohnDoe"
      ]
    },
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }

```

Risoluzione di un errore 403 proibito durante il trasferimento di dati utilizzando l'interfaccia S3

Quando si utilizza l'interfaccia S3 per trasferire dati da o verso un dispositivo Snowball Edge, è possibile che si verifichi un errore 403 proibito. Questo errore può essere il risultato di policy relative agli utenti o ai bucket di IAM. Controlla la policy del bucket S3 che stai utilizzando per i seguenti problemi di sintassi.

Operazione da eseguire

1. La politica non fornisce il PrincipalArn Utilizza la seguente policy come esempio per utilizzare l'PrincipalArn intestazione aws: e fornire il ruolo IAM : * ARN senza.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyIncorrectEncryptionHeader",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",

```

```

    "Resource": "arn:aws:s3:::BucketName/*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
      },
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": [
          "aws:kms",
          "AES256"
        ]
      }
    }
  },
  {
    "Sid": "DenyUnEncryptedObjectUploads",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
      },
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Sid": "DenyInsecureTransport",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": [
      "arn:aws:s3:::BucketName/*",
      "arn:aws:s3:::BucketName"
    ],
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    }
  }
}

```

```

    },
    {
      "Sid": "AllowSnowballPutObjectAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::1234567890:role/RoleName"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::BucketName/*"
    }
  ]
}s

```

2. Se la policy KMS utilizza il formato IAM Role errato, potrebbe verificarsi un errore 403. Modifica la policy per consentire un'eccezione per l'utente IAM utilizzato per caricare i dati. Di seguito è riportato un esempio della sintassi corretta a tale scopo.

```

{{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::1234567890:role/service-role/RoleName"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}

```

3. Potrebbe essere necessario che il ruolo IAM aggiri la condizione dell'intestazione di crittografia. Per impostazione predefinita, tutti gli oggetti archiviati su un dispositivo Snowball Edge sono crittografati con la crittografia SSE-S3. Utilizza la policy riportata di seguito per fornire un'eccezione al ruolo IAM per il caricamento di oggetti senza intestazioni di crittografia.

JSON

```

{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [{
    "Sid": "DenyIncorrectEncryptionHeader",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::BucketName/",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      },
      "StringNotLike": {
        "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
      }
    }
  },
  {
    "Sid": "DenyUnEncryptedObjectUploads",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::BucketName/*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      },
      "StringNotLike": {
        "aws:PrincipalArn": "arn:aws:iam::1234567890:role/
RoleName"
      }
    }
  }
]
}

```

4. Il messaggio di errore indica che l'accesso è negato all' PutObject uso NotPrincipal con condizione IP. Aggiungi un'eccezione come illustrato di seguito per il ruolo IAM di Snowball Edge.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": [
          "IAMRole"
        ]
      },
      "Action": [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::BucketName/*",
        "arn:aws:s3:::BucketName"
      ],
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "IPAddress"
          ]
        },
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::1234567890:role/"
RoleName"
        }
      }
    }
  ]
}
```

Risoluzione dei AWS CLI problemi con Snowball Edge

Utilizza i seguenti argomenti per aiutarti a risolvere i problemi relativi all'utilizzo di un AWS Snowball Edge dispositivo e di AWS CLI.

Risoluzione dei problemi relativi al messaggio di AWS CLI errore: «Profile Cannot Be Null» con Snowball Edge

Quando si lavora con AWS CLI, è possibile che venga visualizzato un messaggio di errore che indica che il profilo non può essere nullo. Puoi riscontrare questo errore se AWS CLI non è stato installato o se un AWS CLI profilo non è stato configurato.

Operazione da eseguire

Assicurati di averlo scaricato e configurato AWS CLI sulla tua workstation. Per ulteriori informazioni, consulta [Installare o aggiornare alla versione più recente di AWS CLI nella Guida per l'AWS Command Line Interface utente](#).

Risoluzione dei problemi relativi all'errore null pointer durante il trasferimento di dati con AWS CLI Snowball Edge

Quando si utilizza il comando AWS CLI per trasferire dati, è possibile che si verifichi un errore null pointer. Questo può accadere nelle condizioni seguenti:

- Il nome file specificato contiene errori, ad esempio `flower.png` o `flower.npg` anziché `flower.png`
- Il percorso specificato è errato, ad esempio `C:\Documents\flower.png` anziché `C:\Documents\flower.png`
- Il file è danneggiato

Operazione da eseguire

Assicurati che il nome file e il percorso siano corretti e riprova. Se il problema persiste, assicurati che il file non sia danneggiato, annulla il trasferimento o tenta di riparare il file.

Risoluzione dei problemi delle istanze di calcolo su Snowball Edge

Di seguito sono riportati suggerimenti per la risoluzione dei problemi relativi alle istanze di computer sui dispositivi Snowball Edge.

Argomenti

- [Interfaccia di rete virtuale con indirizzo IP 0.0.0.0](#)
- [Il dispositivo Snowball Edge smette di rispondere all'avvio di un'istanza di calcolo di grandi dimensioni](#)
- [La mia istanza su Snowball Edge ha un volume root](#)
- [Errore nel file con chiave privata non protetto](#)

Interfaccia di rete virtuale con indirizzo IP 0.0.0.0

Questo problema può verificarsi se l'interfaccia di rete fisica (NIC) è associata all'interfaccia di rete virtuale (VNIC) e dispone di un indirizzo IP di 0.0.0.0. Questo effetto può verificarsi se la NIC non è stata configurata con un indirizzo IP (ad esempio, se hai appena acceso il dispositivo). Può anche verificarsi se stai utilizzando l'interfaccia sbagliata. Ad esempio, è possibile che stiate cercando di ottenere l'indirizzo IP dell'interfaccia SFP+, ma è l' RJ45 interfaccia connessa alla rete.

Operazione da eseguire

In questo caso, puoi eseguire le seguenti operazioni:

- Crea un nuovo VNI associato a una NIC con un indirizzo IP. Per ulteriori informazioni, consulta [Configurazioni di rete per istanze di calcolo su Snowball Edge](#).
- Aggiornare un VNI esistente. Per ulteriori informazioni, consulta [Aggiornamento di un'interfaccia di rete virtuale su Snowball Edge](#).

Il dispositivo Snowball Edge smette di rispondere all'avvio di un'istanza di calcolo di grandi dimensioni

Può sembrare che Snowball Edge abbia smesso di avviare un'istanza. ma normalmente non è così. Tuttavia, per l'avvio delle istanze di calcolo più grandi può essere necessaria più di un'ora.

Per verificare lo stato delle istanze, usa il AWS CLI comando `aws ec2 describe-instances` run sull'endpoint HTTP o HTTPS EC2 compatibile con Amazon su Snowball Edge.

La mia istanza su Snowball Edge ha un volume root

Per impostazione predefinita, le istanze dispongono di un volume root. Tutte le sbe istanze hanno un unico volume root, ma su un dispositivo Snowball Edge puoi aggiungere o rimuovere lo storage a blocchi in base alle esigenze delle tue applicazioni. Per ulteriori informazioni, consulta [Utilizzo dello storage a blocchi con istanze EC2 compatibili con Amazon su Snowball Edge](#).

Errore nel file con chiave privata non protetto

Questo errore può verificarsi se il `.h` file sull'istanza di calcolo non dispone di autorizzazioni sufficienti read/write .

Operazione da eseguire

Per risolvere il problema, puoi modificare le autorizzazioni per il file con la procedura seguente:

1. Apri un terminale e vai alla posizione in cui hai salvato il `.pem` file.
2. Inserire il seguente comando.

```
chmod 400 filename.pem
```

Cronologia dei documenti

- Versione API: 1.0
- Ultimo aggiornamento della documentazione: 14 marzo 2024

La tabella seguente descrive le modifiche importanti alla AWS Snowball Edge Developer Guide dopo luglio 2018. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Tape Gateway sui dispositivi Snowball Edge è obsoleto	La funzionalità Tape Gateway non è più disponibile sui dispositivi Snowball Edge.	14 marzo 2024
Interfaccia di file obsoleta	L'interfaccia di file non è più disponibile per il trasferimento dei dati.	1 marzo 2024
Storage compatibile con Amazon S3 su Snowball Edge disponibile su dispositivi da 210 TB ottimizzati per lo storage Snowball Edge	Lo storage compatibile con Amazon S3 su Snowball Edge è disponibile per lo storage S3 su dispositivi da 210 TB ottimizzati per lo storage Snowball Edge. Per ulteriori informazioni, consulta Utilizzo dello storage compatibile con Amazon S3 su Snowball Edge .	26 febbraio 2024
Includi dispositivi personalizzati AMLs nell'ordine	Le immagini personalizzate di Amazon Machine ora possono essere precariate durante l'ordine dei job Snowball Edge. Per ulteriori informazioni, consulta Aggiungere un AML da Marketplace AWS .	15 novembre 2023

[Lo storage compatibile con Amazon S3 su Snowball Edge è generalmente disponibile](#)

Lo storage compatibile con Amazon S3 su Snowball Edge è supportato sui dispositivi ottimizzati per il computer Snowball Edge. Per ulteriori informazioni, consulta [Storage compatibile con Amazon S3 su Snowball Edge](#).

20 aprile 2023

[Nuovo supportato Regione AWS](#)

AWS Snowball Edge è ora supportato nella regione del Medio Oriente (Emirati Arabi Uniti). Per informazioni sugli endpoint di questa regione, consulta [Snowball Edge Endpoints and Quotas](#) in. Riferimenti generali di AWS Per informazioni sulla spedizione, consulta [Considerazioni sulla spedizione e per Snowball Edge](#).

6 marzo 2023

[Nuovo supportato Regione AWS](#)

AWS Snowball Edge è ora supportato nella regione Asia Pacifico (Giacarta). Per informazioni sugli endpoint di questa regione, consulta [Snowball Edge Endpoints and Quotas](#) in. Riferimenti generali di AWS Per informazioni sulla spedizione, consulta [Considerazioni sulla spedizione e per Snowball Edge](#).

7 settembre 2022

[Migrazione di grandi quantità di dati per Snowball Edge](#)

Snowball Edge ora supporta l'automazione di un piano di migrazione dei dati di grandi dimensioni. Per ulteriori informazioni, consulta [Large Data Migration](#) (procedura manuale) e [Creazione di un piano di migrazione di grandi dimensioni](#) per avviare l'automazione, se lo si desidera.

27 aprile 2022

[Presentazione AWS Snowball Edge Device Management](#)

Snowball Edge Device Management consente di gestire il dispositivo Snowball Edge e i servizi locali da remoto. AWS Tutti i dispositivi Snowball Edge supportano Snowball Edge Device Management ed è preinstallato sui nuovi dispositivi nella maggior parte dei paesi in cui è disponibile Regioni AWS Snowball Edge. [Per ulteriori informazioni, consulta Utilizzo per gestire i dispositivi vi AWS Snowball Edge Device Management](#)

27 aprile 2022

[Configurazione NFS per Snowball Edge](#)

È stata aggiunta la [configurazione NFS per Snowball Edge per dispositivi ottimizzati](#) per lo storage.

21 aprile 2022

Limiti di velocità per Load Balancer	Snowball Edge ora supporta Rate Limits per distribuire le richieste in un ambiente cluster di server.	19 aprile 2022
Supporto per Snowball Edge con Tape Gateway	Ora puoi ordinare un dispositivo Snowball Edge appositamente configurato per ospitare il servizio Tape Gateway. Questa combinazione di tecnologie facilita la migrazione e sicurezza dei dati del nastro offline.	30 novembre 2021
Supporto per la configurazione del server Network Time Protocol (NTP)	I dispositivi Snowball Edge ora supportano la configurazione server NTP (Network Time Protocol) esterna.	16 novembre 2021
Supporto per il trasferimento di dati offline tramite NFS	I dispositivi Snowball Edge ora supportano il trasferimento di dati offline tramite NFS. Per ulteriori informazioni, consulta Utilizzo di NFS per il trasferimento di dati offline .	4 agosto 2021
Nuovo supporto Regione AWS	I dispositivi Snowball Edge sono ora disponibili in Africa (Città del Capo). Regione AWS Per ulteriori informazioni, consulta Snowball Edge Endpoints and Quotas in. Riferimenti generali di AWS Per informazioni sulla spedizione, consulta Considerazioni sulla spedizione per Snowball Edge .	23 novembre 2020

[Support per l'importazione di immagini personalizzate nel dispositivo](#)

Ora puoi importare un'istanza dell'immagine nel dispositivo Snowball Edge e registrarla come Amazon Machine Image (AMI) EC2 compatibile con Amazon. Per ulteriori informazioni, consulta [Importazione di un'immagine nel dispositivo come Amazon EC2 AMI](#).

9 novembre 2020

[Nuovo supporto Regione AWS](#)

I dispositivi Snowball Edge sono ora disponibili in Europa (Milano). Regione AWS Per ulteriori informazioni, consulta [Snowball Edge Endpoints and Quotas](#) in. Riferimenti generali di AWS Per informazioni sulla spedizione, consulta [Considerazioni sulla spedizione per Snowball Edge](#).

30 settembre 2020

[Ristrutturazione dei contenuti](#)

È stata creata una sezione introduttiva che si allinea al Console di gestione della famiglia di servizi AWS Snowflake di lavoro e ha aggiornato altre sezioni per maggiore chiarezza. Per ulteriori informazioni, consulta [Guida introduttiva a AWS Snowball Edge](#).

17 settembre 2020

<u>Ti presentiamo AWS OpsHub</u>	Snowball Edge ora offre uno strumento intuitivo che puoi utilizzare per gestire i tuoi dispositivi e i servizi locali. AWS OpsHub AWS Per ulteriori informazioni, consulta <u>Utilizzo AWS OpsHub per gestire i dispositivi Snowball.</u>	16 aprile 2020
<u>AWS Identity and Access Management (IAM) è ora disponibile localmente sul dispositivo AWS Snowball Edge</u>	Ora puoi usare AWS Identity and Access Management (IAM) per controllare in modo sicuro l'accesso alle AWS risorse in esecuzione sul tuo AWS Snowball Edge dispositivo. Per ulteriori informazioni, vedere <u>Utilizzo di IAM localmente.</u>	16 aprile 2020
<u>Presentazione di una nuova opzione per dispositivi Snowball Edge Storage Optimized (per il trasferimento dei dati)</u>	Snowball aggiunge ora un nuovo dispositivo ottimizzato per l'archiviazione basato sugli attuali dispositivi ottimizzati per il calcolo e per GPU. Per ulteriori informazioni, consulta Opzioni del <u>dispositivo Snowball Edge.</u>	23 marzo 2020
<u>Supporto per la convalida dei tag NFC</u>	I dispositivi Snowball Edge Compute Optimized (con o senza GPU) sono dotati di tag NFC incorporati. Puoi scansionare questi tag con l'app di AWS Snowball Edge verifica, disponibile su Android. Per ulteriori informazioni consulta <u>Convalida dei tag NFC.</u>	13 dicembre 2018

I gruppi di sicurezza sono ora disponibili per le istanze di calcolo	I gruppi di sicurezza nei dispositivi Snowball Edge sono simili ai gruppi di sicurezza in Cloud AWS, con alcune sottili differenze. Per ulteriori informazioni, consulta Gruppi di sicurezza nei dispositivi Snowball Edge .	26 novembre 2018
Presentazione dell'aggiornamento locale	Ora puoi aggiornare il software che fa funzionare un dispositivo Snowball Edge nell'ambiente locale. Ti ricordiamo che gli aggiornamenti locali richiedono una connessione a Internet. Per ulteriori informazioni, consulta Aggiornamento di uno Snowball Edge .	26 novembre 2018
Presentazione di nuove opzioni di dispositivo per Snowball Edge	I dispositivi Snowball Edge sono disponibili in tre opzioni: ottimizzati per lo storage, ottimizzati per l'elaborazione e con GPU. Per ulteriori informazioni, consulta Opzioni del dispositivo Snowball Edge .	15 novembre 2018
Nuovo supporto Regione AWS	I dispositivi Snowball Edge sono ora disponibili nella regione Asia-Pacifico (Mumbai). Tieni presente che le istanze di calcolo e AWS Lambda powered by non AWS IoT Greengrass sono supportate in questa regione.	24 settembre 2018

[Presentazione del supporto per le istanze EC2 di elaborazione compatibili con Amazon sui dispositivi Snowball Edge](#)

AWS Snowball Edge ora supporta i processi locali utilizzando [istanze di EC2 calcolo Amazon](#) in esecuzione su dispositivi Snowball Edge.

17 luglio 2018

[Migliore risoluzione dei problemi dei contenuti](#)

Il capitolo sulla risoluzione dei problemi è stato aggiornato e riorganizzato.

11 luglio 2018

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.