aws

Guida per gli sviluppatori

AWS Backup

AWS Backup: Guida per gli sviluppatori

Table of Contents

Che cos'è AWS Backup?

AWS Backup è un servizio completamente gestito che semplifica la centralizzazione e l'automazione della protezione dei dati tra i AWS servizi, nel cloud e in sede. Utilizzando questo servizio, è possibile configurare le politiche di backup e monitorare l'attività AWS delle risorse in un unico posto. Consente di automatizzare e consolidare le attività di backup eseguite service-by-service in precedenza ed elimina la necessità di creare script personalizzati e processi manuali. Con pochi clic nella console di AWS Backup è possibile automatizzare le policy e le pianificazioni di protezione dei dati.

AWS Backup non regola i backup eseguiti nel proprio ambiente esterno. AWS AWS Backup Pertanto, se desideri una end-to-end soluzione centralizzata per i requisiti di conformità aziendale e normativa, inizia a utilizzarla oggi. AWS Backup

Panoramica delle funzionalità

AWS Backup offre molte caratteristiche e funzionalità, tra cui le seguenti.

Gestione dei backup centralizzata

AWS Backup fornisce una console di backup centralizzata, un set di API di backup e AWS Command Line Interface (AWS CLI) per gestire i backup tra i AWS servizi utilizzati dalle applicazioni. Con AWS Backup, puoi gestire centralmente le policy di backup che soddisfano i tuoi requisiti di backup. È quindi possibile applicarle alle AWS risorse di tutti AWS i servizi, in modo da eseguire il backup dei dati delle applicazioni in modo coerente e conforme. La console di backup AWS Backup centralizzata offre una visualizzazione consolidata dei backup e dei registri delle attività di backup, semplificando il controllo dei backup e garantendo la conformità.

Backup basato su policy

Con AWS Backup, è possibile creare politiche di backup note come piani di backup. Utilizza questi piani di backup per definire i requisiti di backup e quindi applicali alle AWS risorse che desideri proteggere nei AWS servizi che utilizzi. È possibile creare piani di backup separati che soddisfino specifici requisiti di conformità alle normative e aziendali. Questo aiuta a garantire che il backup di ogni AWS risorsa venga eseguito in base ai requisiti dell'utente. Con i piani di backup è più facile implementare la propria strategia di backup all'interno dell'organizzazione e nelle applicazioni in modo scalabile.

Per tutte le opzioni di configurazione per i piani di backup, consulta Opzioni e configurazione del piano di backup.

Policy di backup basate su tag

È possibile utilizzarli AWS Backup per applicare piani di backup alle AWS risorse in un'ampia varietà di modi, inclusa l'etichettatura delle stesse. L'applicazione di tag semplifica l'implementazione della strategia di backup in tutte le applicazioni e garantisce il backup e la AWS protezione di tutte le risorse. AWS i tag sono un ottimo modo per organizzare e classificare le AWS risorse. L'integrazione con i AWS tag consente di applicare rapidamente un piano di backup a un gruppo di AWS risorse, in modo che ne venga eseguito il backup in modo coerente e conforme.

Per tutti i modi in cui è possibile assegnare le risorse ai piani di backup, consulta Assegnazione di risorse a un piano di backup.

Policy di gestione del ciclo di vita

AWS Backup consente di soddisfare i requisiti di conformità riducendo al minimo i costi di storage di backup archiviando i backup in un livello di cold storage a basso costo. È possibile configurare le policy di gestione del ciclo di vita in modo tale che determinino la transizione dei backup da storage dei dati attivi a storage dei dati inattivi in base alla pianificazione desiderata.

Per l'elenco delle risorse che possono sottoposti a transizione nell'archiviazione a freddo, consulta Disponibilità delle funzionalità per risorsa. Per la procedura da seguire per attivare la conservazione a freddo nel piano di backup, consulta Ciclo di vita e livelli di archiviazione.

Backup tra regioni

Utilizzando AWS Backup, è possibile copiare i backup su più backup Regioni AWS su richiesta o automaticamente come parte di un piano di backup pianificato. Il backup tra più regioni è particolarmente utile se si devono rispettare requisiti di continuità aziendale o di conformità che richiedono di archiviare i backup a una distanza minima dai dati di produzione. Per ulteriori informazioni, consulta Creazione di copie di backup tra Regioni AWS.

Gestione e backup tra account

È possibile AWS Backup utilizzarlo per gestire i backup in tutta la Account AWS AWS Organizationsstruttura. Con la gestione di più account, è possibile utilizzare automaticamente le policy di backup per applicare i piani di backup agli account Account AWS all'interno

dell'organizzazione. Ciò rende la conformità e la protezione dei dati efficienti su larga scala, riducendo il sovraccarico operativo. Consente inoltre di eliminare la duplicazione manuale dei piani di backup nei singoli account. Per ulteriori informazioni, consulta Gestione delle risorse di AWS Backup su più Account AWS.

Puoi anche copiare i backup su più file diversi Account AWS all'interno della tua struttura di AWS Organizations gestione. In questo modo, è possibile raccogliere i backup in un unico account di repository e quindi distribuirli per una maggiore resilienza. Creazione di copie di backup tra Account AWS.

Prima di poter utilizzare le funzionalità di gestione e conservazione dei backup su più account, è necessario disporre di una struttura organizzativa esistente configurata in AWS Organizations. Un'unità organizzativa (OU) è un gruppo di account che può essere gestito come un'unica entità. AWS Organizations è un elenco di account che possono essere raggruppati in unità organizzative e gestiti come un'unica entità.

Controllo e rendicontazione con AWS Backup Audit Manager

AWS Backup Audit Manager ti aiuta a semplificare la governance dei dati e la gestione della conformità dei tuoi backup in tutto AWS il mondo. AWS Backup Audit Manager fornisce controlli integrati e personalizzabili che è possibile allineare ai requisiti organizzativi. È inoltre possibile utilizzare questi controlli per tenere traccia automaticamente delle attività e delle risorse di backup.

AWS Backup Audit Manager può aiutarti a individuare attività e risorse specifiche che non sono ancora conformi ai controlli che hai definito. Genera inoltre report giornalieri che è possibile utilizzare per dimostrare la conformità ai controlli nel corso del tempo.

Per includere la conformità del backup insieme alla situazione di conformità generale, è possibile importare automaticamente i risultati di AWS Backup Audit Manager in AWS Audit Manager.

Backup incrementali

AWS Backup archivia in modo efficiente i backup periodici in modo incrementale. Il primo backup di una risorsa di AWS esegue il backup di una copia completa dei dati. Per ogni backup incrementale successivo, viene eseguito il backup solo delle modifiche alle AWS risorse. I backup incrementali consentono di approfittare della protezione dei dati garantita da backup frequenti, riducendo al minimo i costi di archiviazione.

Per un elenco delle risorse che supportano i backup incrementali, consulta Disponibilità delle funzionalità per risorsa.

Gestione completa AWS Backup

Alcuni tipi di risorse supportano la AWS Backup gestione completa. I vantaggi della AWS Backup gestione completa includono:

- Crittografia indipendente. AWS Backup cripta automaticamente i backup con la chiave KMS del AWS Backup vault, anziché utilizzare la stessa chiave di crittografia della risorsa di origine. Questo incrementa i livelli di difesa. Per ulteriori informazioni, consulta Crittografia per i backup in AWS Backup.
- Amazon Resource Names (ARN) di **`awsbackup`**. Gli ARN di Backup iniziano con `arn:aws:backup` invece che con `arn:aws:`*`source-resource`*. Ciò consente di creare policy di accesso che si applicano specificamente ai backup e non alle risorse di origine. Per ulteriori informazioni, consulta Controllo accessi.
- Fatturazione di backup centralizzata e tag di allocazione dei costi di Cost Explorer. I costi per AWS Backup (inclusi archiviazione, trasferimento di dati, ripristino ed eliminazione anticipata) vengono visualizzati nella sezione «Backup» della Amazon Web Services fattura, anziché apparire sotto ciascuna risorsa supportata. È inoltre possibile utilizzare i tag di allocazione dei costi di Cost Explorer per tracciare e ottimizzare i costi di backup. Per ulteriori informazioni, consulta Misurazione, costi e fatturazione.

Per vedere quali tipi di risorse sono idonei per la AWS Backup gestione completa, consulta. Disponibilità delle funzionalità per risorsa

Monitoraggio delle attività di backup

AWS Backup fornisce una dashboard che semplifica il controllo delle attività di backup e ripristino tra AWS i servizi. Con pochi clic sulla AWS Backup console, è possibile visualizzare lo stato dei processi di backup recenti. Puoi anche ripristinare i job tra AWS i servizi per garantire che AWS le tue risorse siano adeguatamente protette.

AWS Backup si integra con Amazon CloudWatch e Amazon EventBridge. CloudWatch consente di tenere traccia delle metriche e creare allarmi. EventBridge consente di visualizzare e monitorare AWS Backup gli eventi. Per ulteriori informazioni, consulta Monitoraggio AWS Backup degli eventi utilizzando EventBridge e Monitoraggio delle AWS Backup metriche con CloudWatch.

AWS Backup si integra con. AWS CloudTrail CloudTrail offre una visualizzazione consolidata dei registri delle attività di backup che semplifica e velocizza il controllo delle modalità di backup delle

risorse. AWS Backup si integra anche con Amazon Simple Notification Service (Amazon SNS), fornendoti notifiche sulle attività di backup, ad esempio quando un backup ha esito positivo o è stato avviato un ripristino. Per ulteriori informazioni, consulta Registrazione delle chiamate AWS Backup API con Amazon SNS CloudTrail e utilizzo di Amazon SNS per tenere AWS Backup traccia degli eventi.

Protezione dei dati nei vault di backup

Il contenuto di ogni AWS Backup backup è immutabile, il che significa che nessuno può modificarlo. AWS Backup protegge ulteriormente i backup negli archivi di backup, che li separano in modo sicuro dalle istanze di origine. Ad esempio, il vault conserverà i backup di Amazon EC2 e Amazon EBS in base alla policy del ciclo di vita scelta, anche se si eliminano l'istanza Amazon EC2 di origine e i volumi di Amazon EBS.

I vault di backup offrono crittografia e policy di accesso basate su risorse che permettono di definire chi può accedere ai backup. È possibile definire le policy di accesso per un vault di backup per specificare chi può accedere ai backup all'interno del vault e quali operazioni possono essere eseguite. Ciò offre un modo semplice e sicuro per controllare l'accesso ai backup tra i servizi. AWS Per rivedere AWS le politiche gestite dai clienti per AWS Backup, consulta Politiche gestite per AWS Backup.

Puoi utilizzare AWS Backup Vault Lock per impedire a chiunque (incluso te) di eliminare i backup o alterarne il periodo di conservazione. AWS Backup Vault Lock ti aiuta a far rispettare un modello write-once-read-many(WORM) e ad aggiungere un altro livello di difesa alla tua difesa in profondità. Per iniziare, consulta Vault Lock di AWS Backup.

Supporto per gli obblighi di conformità

AWS Backup ti aiuta a soddisfare i tuoi obblighi di conformità globali. AWS Backup rientra nell'ambito dei seguenti programmi di AWS conformità:

- FedRAMP High
- GDPR
- SOC 1, 2 e 3
- PCI
- HIPAA
- e molti altri

Nozioni di base

Per saperne di più AWS Backup, ti consigliamo di iniziare conIniziare con AWS Backup.

AWS Risorse e applicazioni supportate

Di seguito sono elencate AWS le risorse e le applicazioni di terze parti che è possibile utilizzare per il backup e il ripristino AWS Backup. Per ulteriori informazioni, consulta the section called “Disponibilità delle funzionalità”.

Servizio	Tipi di risorse supportati
Amazon Elastic Compute Cloud (Amazon EC2)	Istanze Amazon EC2 (escluse le AMI supportate dall'archivio dell'istanza)
Amazon Simple Storage Service (Amazon S3)	Dati Amazon S3
Amazon Elastic Block Store (Amazon EBS)	Volumi Amazon EBS
Amazon DynamoDB	Tabelle Amazon DynamoDB
Amazon Relational Database Service (Amazon RDS)	Istanze di database Amazon RDS (inclusi tutti i motori di database); cluster Multi-Availability Zone
Amazon Aurora	Cluster Aurora
Amazon Elastic File System (Amazon EFS)	File system di Amazon EFS
FSx per Lustre	File system FSx per Lustre
FSx per Windows File Server	File system FSx per Windows File Server
Amazon FSx per ONTAP NetApp	File system FSx per ONTAP

Servizio	Tipi di risorse supportati
Amazon FSx per OpenZFS	File system FSx per OpenZFS
AWS Storage Gateway (Volume Gateway)	AWS Storage Gateway volumi
Amazon DocumentDB	Cluster basati su istanze Amazon DocumentDB
Amazon Neptune	Cluster Amazon Neptune
Amazon Redshift	Cluster Amazon Redshift
Amazon Timestream	Tabelle Amazon Timestream
VMware Cloud™ attivo AWS	Macchine virtuali VMware Cloud™ attive AWS
VMware Cloud™ attivo AWS Outposts	Macchine virtuali VMware Cloud™ attive AWS Outposts
AWS CloudFormation	AWS CloudFormation pile
Database SAP HANA	Database SAP HANA su istanze Amazon EC2

Prezzi

Con AWS Backup, paghi per lo storage di backup, il ripristino dei dati, i test di ripristino, il trasferimento di dati tra le regioni e l' AWS Backup Audit Manager. Per ulteriori informazioni, consulta la sezione Prezzi di AWS Backup.

AWS Backup disponibilità delle funzionalità

AWS Backup le funzionalità sono offerte in base alla risorsa e Regione AWS. Le sezioni e le tabelle seguenti permettono di determinare la disponibilità delle funzionalità.

Indice

- Disponibilità delle funzionalità per risorsa
- Disponibilità delle funzionalità tramite Regione AWS
- Servizi supportati da Regione AWS

Funzionalità disponibili per tutte le risorse supportate

AWS Backup offre le seguenti funzionalità per i AWS servizi supportati, nonché per le applicazioni di terze parti supportate. Il supporto di una funzionalità o di un servizio non deve essere presunto a meno che non sia esplicitamente indicato.

- Pianificazioni di backup automatizzate e gestione della conservazione
- Monitoraggio centralizzato dei backup
- Backup crittografati
- Backup incrementali
- Gestione tra account con AWS Organizations
- Audit e report di backup automatizzati con AWS Backup Audit Manager
- Worm (Write-Once, Read-Many) con Vault Lock AWS Backup

Disponibilità delle funzionalità per risorsa

Per essere utilizzato AWS Backup con un AWS servizio supportato in una particolare regione, il servizio deve essere disponibile nella regione. Per determinare la disponibilità del servizio in una regione, visualizza gli endpoint del Riferimenti generali di AWSservizio in.

AWS Backup supporta	Backup tra più regioni	Backup tra account	AWS Backup Audit Manager	Backup incrementali	Backup e point-in-time ripristino continui	Gestione completa	Dal ciclo di vita alla conservazione a freddo	Ripristino a livello di elemento [1]	Test di ripristino
Amazon EC2	✓	✓	✓	✓					✓

AWS Backup supporta	Backup tra più regioni	Backup tra account	AWS Backup Audit Manager	Backup incrementali	Backup e point-in-time ripristino continui	Gestione completa	Dal ciclo di vita alla conservazione a freddo	Ripristino a livello di elemento [1]	Test di ripristino
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
Amazon RDS a istanza singola	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Cluster Amazon RDS	✓ [3]	✓ [3]	✓ [4]	✓					✓
Amazon Aurora	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓
Amazon EFS	✓	✓	✓	✓		✓	✓	✓	✓
FSx per Lustre	✓	✓	✓	✓					✓
FSx per Windows File Server	✓	✓	✓	✓					✓

AWS Backup supporta	Backup tra più regioni	Backup tra account	AWS Backup Audit Manager	Backup incrementali	Backup e point-in-time ripristino continui	Gestione completa	Dal ciclo di vita alla conservazione a freddo	Ripristino a livello di elemento [1]	Test di ripristino
FSx per ONTAP			✓ [2]	✓					✓
FSx per OpenZFS	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon DocumentDB	✓ [3]	✓ [3]	✓						✓
Amazon Neptune	✓ [3]	✓ [3]	✓						✓
Amazon Redshift								✓	
Timestream	✓	✓	✓	✓		✓	✓	✓	
VBS per Windows	✓	✓	✓	✓					
Macchine virtuali	✓	✓	✓	✓		✓	✓	✓	

AWS Backup supporta	Backup tra più regioni	Backup tra account	AWS Backup Audit Manager	Backup incrementali	Backup e point-in-time ripristino continui	Gestione completa	Dal ciclo di vita alla conservazione a freddo	Ripristino a livello di elemento [1]	Test di ripristino
AWS CloudFormation modelli	✓	✓		✓ [5]		✓	✓ [5]		
Amazon DynamoDB			✓						✓
DynamoDB con funzionalità avanzate di AWS Backup	✓	✓	✓			✓	✓		✓
Database SAP HANA su istanze Amazon EC2				✓	✓	✓	✓		

Alcuni tipi di risorse dispongono della funzionalità di backup continuo e di quella di copia in più regioni e in più account. Quando si esegue una copia in più regioni o in più account di un backup continuo, il punto di ripristino copiato (backup) diventa un backup (periodico) snapshot. Amazon RDS e Amazon

S3 supportano copie di snapshot incrementali; Amazon Aurora supporta solo copie di snapshot complete. PITR (ripristino point-in-time) non è disponibile per queste copie.

[1] L' "elemento» in un ripristino a livello di elemento varia a seconda della risorsa supportata. Ad esempio, un elemento del file system è un file o una directory, mentre un elemento di S3 è un oggetto S3. Un elemento VMware è un disco. Per ulteriori informazioni, consulta la sezione Ripristino di un backup relativa alla risorsa supportata.

[2] AWS Backup Audit Manager supporta questa risorsa su tutti i controlli ad eccezione della copia tra account e della copia tra più regioni.

[3] RDS, Aurora, DocumentDB e Neptune non supportano un'azione di copia singola che esegua sia il backup tra regioni che tra più account. È necessario scegliere tra un'opzione o l'altra. È inoltre possibile utilizzare uno AWS Lambda script per ascoltare il completamento della prima copia, eseguire la seconda copia e quindi eliminare la prima copia. Le istanze di database RDS su zone di disponibilità multipla (Multi-AZ) possono essere copiate, ma i cluster Multi-AZ non supportano al momento la copia tra più regioni o più account. Vedi Considerazioni sulla copia in più regioni con risorse specifiche per ulteriori informazioni.

[4] Vedere Backup delle zone a disponibilità multipla RDS per le regioni in cui è disponibile il supporto di Backup Audit Manager.

[5] Nei backup in CloudFormation stack, le risorse annidate mantengono le funzionalità delle risorse di origine. Tuttavia, le risorse all'interno dello stack non mantengono la funzionalità Point-in-Time Restore (PITR) (come Amazon S3 e Amazon RDS). Le proprietà all'interno della matrice precedente si applicano solo ai CloudFormation modelli e non alle risorse all'interno dello stack.

[6] Per Aurora, le istantanee sono complete e il backup incrementale è offerto tramite PITR.

Disponibilità delle funzionalità tramite Regione AWS

AWS Backup è disponibile in tutte le versioni seguenti Regioni AWS. AWS Backup le funzionalità sono disponibili in tutte queste regioni, salvo diversa indicazione nella tabella seguente.

AWS Backup supporti	Backup tra più regioni	Gestione di più account	Backup tra account	AWS Backup Audit Manager e dashboard Jobs	Ripristina i test
Stati Uniti orientali (Virginia settentrionale)	✓	✓	✓	✓	✓
Stati Uniti orientali (Ohio)	✓	✓	✓	✓	✓
Stati Uniti occidentali (California settentrionale)	✓	✓	✓	✓	✓
Stati Uniti occidentali (Oregon)	✓	✓	✓	✓	✓
Africa (Città del Capo)	✓		✓	✓	✓
Asia Pacifico (Hong Kong)	✓		✓	✓	✓
Asia Pacific (Hyderabad)	✓		✓		✓
Asia Pacifico (Giacarta)	✓		✓		✓

AWS Backup supporti	Backup tra più regioni	Gestione di più account	Backup tra account	AWS Backup Audit Manager e dashboard Jobs	Ripristina i test
Asia Pacifico (Melbourne)	✓		✓		✓
Asia Pacifico (Mumbai)	✓	✓	✓	✓	✓
Asia Pacific (Osaka)	✓	✓	✓		✓
Asia Pacific (Seul)	✓	✓	✓	✓	✓
Asia Pacifico (Singapore)	✓	✓	✓	✓	✓
Asia Pacifico (Sydney)	✓	✓	✓	✓	✓
Asia Pacifico (Tokyo)	✓	✓	✓	✓	✓
Canada (Centrale)	✓	✓	✓	✓	✓
Canada occidentale (Calgary)	✓ (eccetto Amazon S3)		✓		
Cina (Pechino)	✓				
China (Ningxia)	✓				

AWS Backup supporti	Backup tra più regioni	Gestione di più account	Backup tra account	AWS Backup Audit Manager e dashboard Jobs	Ripristina i test
Europa (Francoforte)	✓	✓	✓	✓	✓
Europa (Irlanda)	✓	✓	✓	✓	✓
Europa (Londra)	✓	✓	✓	✓	✓
Europa (Milano)	✓		✓	✓	✓
Europa (Parigi)	✓	✓	✓	✓	✓
Europa (Spagna)	✓		✓		✓
Europa (Stoccolma)	✓	✓	✓	✓	✓
Europa (Zurigo)	✓		✓		✓
Israele (Tel Aviv)	✓		✓		
Medio Oriente (Bahrein)	✓		✓	✓	✓

AWS Backup supporti	Backup tra più regioni	Gestione di più account	Backup tra account	AWS Backup Audit Manager e dashboard Jobs	Ripristina i test
Medio Oriente (Emirati Arabi Uniti)	✓		✓		✓
Sud America (San Paolo)	✓	✓	✓	✓	✓
AWS GovCloud (Stati Uniti orientali)	✓	✓	✓	✓	
AWS GovCloud (Stati Uniti occidentali)	✓	✓	✓	✓	

Cina (Pechino) e Cina (Ningxia) supportano la copia tra regioni da una di queste due regioni all'altra. La copia tra più regioni non è supportata da queste regioni verso altre regioni o verso queste regioni da altre. In queste regioni non è supportata la copia tra più account.

La dashboard delle offerte di lavoro non è disponibile in AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali). L'aggregazione della dashboard di Jobs è disponibile solo nelle regioni che supportano la gestione tra account e AWS Backup Audit Manager.

Amazon FSx for Windows File Server e Amazon Neptune non supportano copie di backup interregionali nelle regioni con attivazione.

Servizi supportati da Regione AWS

AWS Backup supporta quanto segue in tutte le regioni supportate:

- Aurora
- DynamoDB
- DynamoDB AWS Backup con funzionalità avanzate
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

La tabella seguente indica il AWS Backup supporto per altri in Servizi AWS base alla regione.

Utenti e regioni	Amazon FSx	SAP HANA su istanze Amazon EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware e Backup
Stati Uniti orientali (Virginia settentrionale)	✓	✓	✓	✓	✓	✓
Stati Uniti orientali (Ohio)	✓	✓	✓	✓	✓	✓
Stati Uniti occidentali (California settentrionale)	Windows; Lustre; ONTAP	✓	✓	✓		✓
US West (Oregon)	Windows; Lustre; ONTAP	✓	✓	✓	✓	✓

Utenti e regioni	Amazon FSx	SAP HANA su istanze Amazon EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware e Backup
Africa (Città del Capo)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Asia Pacifico (Hong Kong)	✓	✓	✓ [1]	✓		✓
Asia Pacific (Hyderabad)	Windows; Lustre; ONTAP		✓ [1]	✓		
Asia Pacifico (Giacarta)	Windows; Lustre; ONTAP		✓	✓		
Asia Pacifico (Melbourne)	Windows; Lustre; ONTAP		✓ [1]	✓		
Asia Pacifico (Mumbai)	✓	✓	✓	✓		✓
Asia Pacifico (Osaka-Locale)	Windows; Lustre	✓	✓ [1]	✓		✓

Utenti e regioni	Amazon FSx	SAP HANA su istanze Amazon EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware e Backup
Asia Pacific (Seul)	✓	✓	✓	✓		✓
Asia Pacifico (Singapore)	✓	✓	✓	✓		✓
Asia Pacifico (Sydney)	✓	✓	✓	✓	✓	✓
Asia Pacifico (Tokyo)	✓	✓	✓	✓	✓	✓
Canada (Centrale)	✓	✓	✓	✓		✓
Canada occidentale (Calgary)						
Cina (Pechino)	Windows; Lustre		✓ [1]	✓	✓	
Cina (Ningxia)	Windows; Lustre		✓ [1]	✓	✓	
Europa (Francoforte)	✓	✓	✓	✓	✓	✓

Utenti e regioni	Amazon FSx	SAP HANA su istanze Amazon EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware e Backup
Europa (Irlanda)	✓	✓	✓	✓	✓	✓
Europa (Londra)	✓	✓	✓	✓		✓
Europa (Milano)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Europa (Parigi)	Windows; Lustre; ONTAP	✓	✓	✓		✓
Europa (Spagna)	Windows; Lustre; ONTAP		✓ [1]	✓		
Europa (Stoccolma)	✓	✓	✓	✓		✓
Europa (Zurigo)	Windows; Lustre; ONTAP		✓ [1]	✓		
Israele (Tel Aviv)	Windows; Lustre; ONTAP		✓ [1]	✓		
Medio Oriente (Bahrein)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓

Utenti e regioni	Amazon FSx	SAP HANA su istanze Amazon EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware e Backup
Medio Oriente (Emirati Arabi Uniti)			✓ [1]	✓		
Sud America (San Paolo)		✓	✓	✓		✓
AWS GovCloud (Stati Uniti occidentali)	Windows; Lustre; ONTAP		✓ [1]	✓		✓
AWS GovCloud (Stati Uniti orientali)	Windows; Lustre; ONTAP		✓ [1]	✓		✓

Un segno di spunta in Amazon FSx indica che FSx for Windows File Server, FSx for Lustre, FSx for ONTAP e FSx for OpenZFS sono tutti supportati in quella regione da; in caso contrario, verranno elencate le configurazioni supportate. AWS Backup

1 La copia tra regioni e più account non è supportata.

AWS Backup: Come funziona

AWS Backup è un servizio di backup completamente gestito che semplifica la centralizzazione e l'automazione del backup dei dati tra i servizi. AWS Con AWS Backup, è possibile creare politiche di backup denominate piani di backup. È possibile utilizzare questi piani per definire i requisiti di backup, ad esempio la frequenza con cui eseguire il backup dei dati e la durata di conservazione di tali backup.

AWS Backup consente di applicare piani di backup alle AWS risorse semplicemente etichettandole. AWS Backup quindi esegue automaticamente il backup AWS delle risorse in base al piano di backup definito.

Le sezioni seguenti descrivono il AWS Backup funzionamento, i dettagli di implementazione e le considerazioni sulla sicurezza.

Argomenti

Come AWS Backup funziona con i servizi supportati AWS

Alcuni AWS servizi AWS Backup supportati offrono le proprie funzionalità di backup autonome. Queste funzionalità sono disponibili per l'utente a prescindere dall'utilizzo di AWS Backup. Tuttavia, i backup creati da altri AWS servizi non sono disponibili per la governance centralizzata. AWS Backup

AWS Backup Per configurare la gestione centralizzata della protezione dei dati per tutti i servizi supportati, è necessario attivare la gestione del servizio con AWS Backup, creare un backup su richiesta o pianificare i backup utilizzando un piano di backup e archiviare i backup in archivi di backup.

Argomenti

- Utilizzo dei file system Amazon FSx
- Utilizzo di Amazon EC2
- Utilizzo di Amazon EFS
- Utilizzo di Amazon EBS
- Utilizzo di Amazon RDS e Aurora
- Lavorare con AWS BackInt
- Lavorare con AWS Storage Gateway
- Utilizzo di Amazon DocumentDB
- Utilizzo di Amazon Neptune
- Utilizzo di Amazon Timestream
- Lavorare con AWS Organizations
- Lavorare con AWS CloudFormation
- Lavorare con AWS BackInt, AWS Systems Manager per SAP e SAP HANA
- In che modo AWS i servizi eseguono il backup delle proprie risorse

Attiva la gestione dei servizi con AWS Backup

Quando diventano disponibili nuovi AWS servizi, è necessario AWS Backup abilitarne l'utilizzo. Se si tenta di creare un backup on demand o un piano di backup utilizzando risorse di un servizio non abilitato, viene visualizzato un messaggio di errore e non è possibile completare il processo.

La AWS Backup console offre due modi per includere i tipi di risorse in un piano di backup: assegnare esplicitamente il tipo di risorsa in un piano di backup o includere tutte le risorse. Consulta i punti seguenti per comprendere come funzionano queste selezioni con adesioni al servizio.

- Se le assegnazioni delle risorse si basano solo sui tag, vengono applicate le impostazioni opt-in del servizio.
- Se un tipo di risorsa viene assegnato in modo esplicito a un piano di backup, verrà incluso nel backup anche se l'opt-in non è abilitato per quel particolare servizio. Questo non si applica ad Aurora, Neptune e Amazon DocumentDB. Affinché questi servizi siano inclusi, l'opt-in deve essere abilitato.
- Se in un'assegnazione di risorse sono specificati sia il tipo di risorsa che i tag, i tipi di risorse specificati vengono filtrati per primi, quindi i tag filtrano ulteriormente tali risorse.

Le impostazioni relative all'attivazione del servizio vengono ignorate per la maggior parte dei tipi di risorse. Tuttavia Aurora, Neptune e Amazon DocumentDB richiedono l'attivazione del servizio.

- Per Amazon FSx for NetApp ONTAP, quando utilizzi la selezione delle risorse basata su tag, applica i tag ai singoli volumi anziché all'intero file system.

Le impostazioni di attivazione del servizio sono specifiche di una regione. Quando un account utilizza AWS Backup (crea un archivio di backup o un piano di backup) in una regione, l'account viene automaticamente inserito in tutti i tipi di risorse supportati dalla regione AWS Backup in quel momento. I servizi supportati aggiunti a quella regione in un secondo momento non verranno inclusi automaticamente in un piano di backup. Puoi scegliere di attivare questi tipi di risorse una volta che saranno supportati.

Per configurare i servizi utilizzati con AWS Backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Attivazione del servizio scegliere Configura risorse.
4. Utilizza gli interruttori a levetta per abilitare o disabilitare i servizi utilizzati con. AWS Backup

   > **Important**
   >
   > RDS, Aurora, Neptune e DocumentDB condividono lo stesso nome della risorsa Amazon (ARN). Se si sceglie di gestire uno di questi tipi di risorse, si sceglie di AWS Backup utilizzarli tutti al momento dell'assegnazione a un piano di backup. In ogni caso, si consiglia di acconsentire a tutti per rappresentare in modo accurato lo stato opt-in.

5. Scegli Conferma.

Utilizzo dei dati di Amazon S3

AWS Backup offre backup e ripristino completamente gestiti per i backup di Amazon S3. Per ulteriori informazioni, consulta Backup Amazon S3.

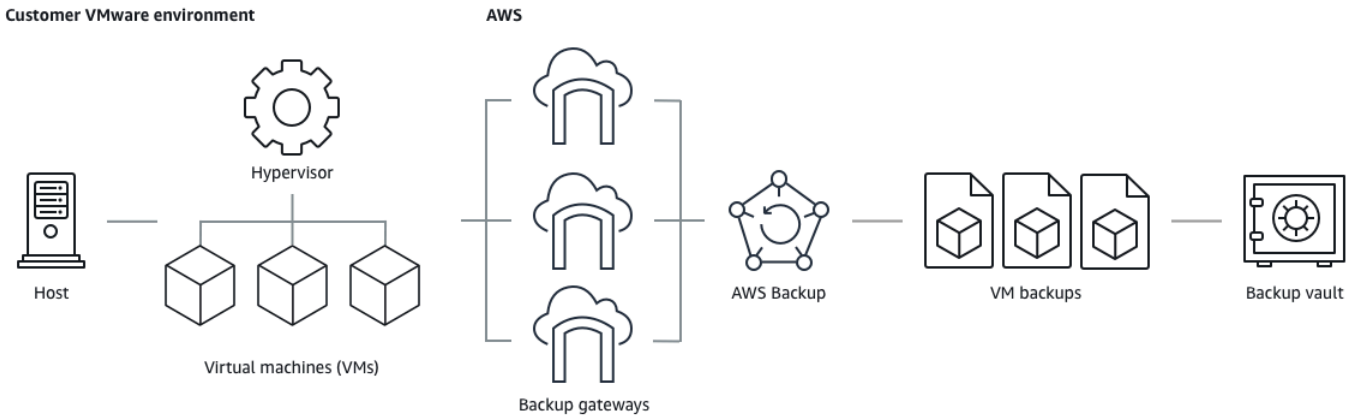
- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare i dati di Amazon S3 utilizzando: AWS BackupRipristino dei dati S3

Per ulteriori informazioni sui dati S3, consulta la documentazione di Amazon S3.

Utilizzo di macchine virtuali VMware

AWS Backup supporta la protezione dei dati centralizzata e automatizzata per le macchine virtuali (VM) VMware locali e le VM in VMware Cloud™ (VMC) on. AWSÈ possibile eseguire il backup dalle macchine virtuali locali e VMC su. AWS Backup Quindi, è possibile eseguire il ripristino da AWS Backup a on-premise o VMC.

Backup gateway è un AWS Backup software scaricabile che si distribuisce sulle macchine virtuali VMware per collegarle. AWS Backup Il gateway si connette al server di gestione delle macchine virtuali per individuare le macchine virtuali, individua le macchine virtuali dell'utente, esegue la crittografia dei dati e li trasferisce in modo efficiente ad AWS Backup. Nel diagramma seguente viene illustrato in che modo Backup gateway si connette alle macchine virtuali:



- Come eseguire il backup delle risorse: Backup di macchine virtuali
- Come ripristinare le risorse VM: Ripristino di una macchina virtuale utilizzando AWS Backup

Utilizzo di Amazon DynamoDB

AWS Backup supporta il backup e il ripristino delle tabelle Amazon DynamoDB. DynamoDB è un servizio di database NoSQL completamente gestito che fornisce prestazioni elevate e prevedibili con una scalabilità senza interruzioni.

Sin dal suo lancio, AWS Backup ha sempre supportato DynamoDB. A partire da novembre 2021, sono state AWS Backup inoltre introdotte funzionalità avanzate per i backup DynamoDB. Queste funzionalità avanzate includono la copia dei backup su più account e più account, la suddivisione dei

backup su più livelli in cold storage Regioni AWS e l'utilizzo di tag per le autorizzazioni e la gestione dei costi.

AWS Backup I nuovi clienti che effettueranno l'onboarding dopo novembre 2021 avranno le funzionalità di backup avanzate di DynamoDB abilitate di default.

Consigliamo a tutti i AWS Backup clienti esistenti di abilitare le funzionalità avanzate per DynamoDB. Non vi è alcuna differenza nel prezzo dello storage di backup a caldo dopo aver abilitato le funzionalità avanzate, inoltre è possibile risparmiare denaro eseguendo la suddivisione livelli dei backup nello storage a freddo e ottimizzare i costi utilizzando i tag di allocazione dei costi.

Per un elenco completo delle funzionalità avanzate e come abilitarle, consulta Backup di DynamoDB avanzato.

- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare le risorse DynamoDB: Ripristino di una tabella Amazon DynamoDB

Per informazioni dettagliate su DynamoDB, consulta Che cos'è Amazon DynamoDB? nella Guida per gli sviluppatori di Amazon DynamoDB.

Utilizzo dei file system Amazon FSx

AWS Backup supporta il backup e il ripristino dei file system Amazon FSx. Amazon FSx fornisce file system di terze parti completamente gestiti con compatibilità e set di funzionalità nativi per i carichi di lavoro. AWS Backup utilizza la funzionalità di backup integrata di Amazon FSx. Pertanto, i backup eseguiti dalla console AWS Backup hanno lo stesso livello di coerenza e prestazioni del file system e le stesse opzioni di ripristino dei backup eseguiti tramite la console di Amazon FSx.

Se gestisci questi backup, ottieni funzionalità aggiuntive, come opzioni di conservazione illimitate e la possibilità di creare backup pianificati con una frequenza ogni ora. AWS Backup Inoltre, AWS Backup conserva i backup anche dopo l'eliminazione del file system di origine. Ciò protegge dall'eliminazione accidentale o dannosa.

AWS Backup Utilizzalo per proteggere i file system Amazon FSx se desideri configurare le politiche di backup e monitorare le attività di backup da una console di backup centrale che estende anche il supporto per altri AWS servizi.

- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare le risorse Amazon FSx: Ripristino di un file system FSX

Per informazioni dettagliate sui file system Amazon FSx, consulta la documentazione di Amazon FSx.

Utilizzo di Amazon EC2

AWS Backup supporta istanze Amazon EC2.

- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare le risorse Amazon EC2: Ripristino di un'istanza Amazon EC2

Puoi pianificare o eseguire processi di backup su richiesta che includono intere istanze EC2, compresi i volumi Amazon EBS. Pertanto, puoi ripristinare un'intera istanza Amazon EC2 da un singolo punto di ripristino, inclusi il volume root, i volumi di dati e alcune impostazioni di configurazione dell'istanza, come il tipo di istanza e la key pair.

Puoi anche eseguire il backup e il ripristino delle applicazioni Microsoft Windows abilitate per VSS. Puoi pianificare backup coerenti con le applicazioni, definire policy del ciclo di vita ed eseguire ripristini coerenti come parte di un backup on demand o di un piano di backup pianificato. Per ulteriori informazioni, consulta Creazione di backup Windows VSS.

AWS Backup non riavvia le istanze EC2 in nessun momento.

Immagini e istantanee

Quando si esegue il backup di un'istanza Amazon EC2 AWS Backup , scatta uno snapshot del volume di storage Amazon EBS principale, delle configurazioni di avvio e di tutti i volumi EBS associati. AWS Backup memorizza determinati parametri di configurazione dell'istanza EC2, tra cui il tipo di istanza, i gruppi di sicurezza, Amazon VPC, la configurazione di monitoraggio e i tag. I dati di backup vengono archiviati come un'Amazon Machine Image (AMI) supportata dal volume Amazon EBS.

Se elimini uno snapshot di Amazon Machine Image (AMI) o Amazon EBS gestito AWS Backup utilizzando AWS Backup e hai configurato il cestino di riciclaggio Amazon EC2, l'immagine o lo snapshot potrebbero essere soggetti a costi in base alla politica del cestino di Amazon EC2. Le istantanee e le immagini nel cestino Amazon EC2 non sono più gestite AWS Backup e non saranno gestite AWS Backup dalle politiche se le ripristini dal cestino.

AWS Backup gli snapshot gestiti di Amazon EBS e gli snapshot associati a un'AMI AWS Backup Amazon EC2 gestita a cui è applicato Amazon EBS Snapshot Lock non possono essere eliminati

come parte del ciclo di vita del punto di ripristino se la durata del blocco degli snapshot supera il ciclo di vita del backup. Questi punti di ripristino avranno lo stato `EXPIRED`. Possono essere eliminati manualmente se scegli di rimuovere prima lo Snapshot Lock di Amazon EBS.

AWS Backup può crittografare gli snapshot EBS associati a un backup Amazon EC2. È simile a come crittografa gli snapshot EBS. AWS Backup utilizza la stessa crittografia applicata ai volumi EBS sottostanti durante la creazione di uno snapshot dell'AMI Amazon EC2 e i parametri di configurazione dell'istanza originale vengono mantenuti nei metadati di ripristino.

Una snapshot ricava la propria crittografia dal volume e la stessa crittografia viene applicata alle istantanee corrispondenti. Le istantanee EBS di un'AMI copiata sono sempre crittografate. Se si specifica una chiave KMS durante la copia, viene applicata la chiave specificata. Se non si specifica una chiave KMS, viene applicata una chiave KMS predefinita.

Per ulteriori informazioni, consulta le istanze di Amazon EC2 nella Amazon EC2 User Guide e la crittografia Amazon EBS nella Amazon EBS User Guide.

Utilizzo di Amazon EFS

AWS Backup supporta Amazon Elastic File System (Amazon EFS).

- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare le risorse Amazon EFS: Ripristino di un file system Amazon EFS

Per informazioni dettagliate sui file system Amazon EFS, consulta Che cos'è Amazon Elastic File System? nella Guida per l'utente di Amazon Elastic.

Utilizzo di Amazon EBS

AWS Backup supporta i volumi Amazon Elastic Block Store (Amazon EBS).

AWS Backup gli snapshot gestiti di Amazon EBS e gli snapshot associati a un'AMI AWS Backup Amazon EC2 gestita a cui è applicato Amazon EBS Snapshot Lock non possono essere eliminati come parte del ciclo di vita del punto di ripristino se la durata del blocco degli snapshot supera il ciclo di vita del backup. Questi punti di ripristino avranno lo stato `EXPIRED`. Possono essere eliminati manualmente se scegli di rimuovere prima lo Snapshot Lock di Amazon EBS.

- Come eseguire il backup delle risorse: Iniziare con AWS Backup

- Come ripristinare i volumi Amazon EBS: Ripristino di un volume Amazon EBS

Per ulteriori informazioni, consulta i volumi Amazon EBS nella Amazon EBS User Guide.

Utilizzo di Amazon RDS e Aurora

AWS Backup supporta i motori di database Amazon RDS e i cluster Aurora.

- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare le risorse Amazon RDS: Ripristino di un database RDS
- Come ripristinare i cluster Aurora: Ripristino di un cluster Amazon Aurora

Per ulteriori informazioni su Amazon RDS, consulta Che cos'è Amazon Relational Database Service nella Guida per l'utente di Amazon RDS.

Per informazioni dettagliate su Aurora, consulta Che cos'è Amazon Aurora? nella Guida per l'utente di Amazon Aurora.

> **Note**
>
> Se avvii un processo di backup dalla console di Amazon RDS, questo può essere in conflitto con un processo di backup dei cluster Aurora, causando l'errore Backup job expired before completion. In tal caso, configura una finestra di backup più lunga in AWS Backup.

> **Note**
>
> RDS Custom for SQL Server e RDS Custom for Oracle non sono attualmente supportati da AWS Backup.

> **Note**
>
> AWS non addebita alcun costo per le istantanee Aurora archiviate in un archivio di backup purché Aurora abbia abilitato i backup automatici e il periodo di conservazione per i backup automatici Aurora sia superiore al periodo di conservazione delle istantanee Aurora.
> Tutti gli snapshot all'interno del vault di backup verranno addebitati se il database degli

snapshot viene eliminato (le eliminazioni possono avvenire accidentalmente o durante l'implementazione blu/verde).
Gli snapshot di grandi dimensioni e i backup frequenti da un database eliminato potrebbero comportare costi di storage significativi. Visita il calcolatore AWS Backup per stimare i costi AWS Backup potenziali.

Lavorare con AWS BackInt

AWS Backup collabora con AWS Backint per supportare il backup e il ripristino del database SAP HANA su istanze Amazon EC2.

- Istruzioni per il backup e il ripristino delle risorse SAP HANA: backup e ripristino delle istanze SAP HANA Amazon EC2
- Configurare AWS Backint Agent AWS : Backint Agent per SAP HANA

Lavorare con AWS Storage Gateway

AWS Backup supporta Storage Gateway Volume Gateway. Puoi anche ripristinare gli snapshot di Amazon EBS come volumi Storage Gateway.

- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare le risorse Storage Gateway: Ripristino di un volume Storage Gateway.

Utilizzo di Amazon DocumentDB

AWS Backup supporta i cluster Amazon DocumentDB.

- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare le risorse di Amazon DocumentDB:. Ripristino di un cluster DocumentDB

Utilizzo di Amazon Neptune

AWS Backup supporta i cluster Amazon Neptune.

- Come eseguire il backup delle risorse: Iniziare con AWS Backup
- Come ripristinare i cluster Amazon Neptune: Ripristino di un cluster Neptune.

Utilizzo di Amazon Timestream

AWS Backup supporta le tabelle Amazon Timestream.

- Come eseguire il backup delle tabelle Timestream.
- Come ripristinare le tabelle Timestream.

Lavorare con AWS Organizations

AWS Backup funziona con AWS Organizations per semplificare il monitoraggio e la gestione tra account

- Creare un account di gestione in Organizations.
- Attivare la gestione di più account.
- Designare gli account amministratore delegato e la delega della policy.

Lavorare con AWS CloudFormation

AWS Backup AWS CloudFormation modelli di supporto e stack di applicazioni

- AWS CloudFormation backup in pila

Lavorare con AWS BackInt, AWS Systems Manager per SAP e SAP HANA

AWS Backup collabora con AWS BackInt e con SSM for SAP per supportare le funzioni di backup e ripristino di SAP HANA.

- Database SAP HANA su backup di istanze Amazon EC2
- Inizia a usare for SAP AWS Systems Manager
- AWS Backint Agent per SAP HANA

In che modo AWS i servizi eseguono il backup delle proprie risorse

È possibile fare riferimento alla documentazione tecnica per il processo di backup e ripristino di un AWS servizio specifico, in particolare quando, durante un ripristino, è necessario configurare una nuova istanza di quel AWS servizio. Di seguito è riportato un elenco di documentazione:

- Servizi correlati Amazon EC2
- Utilizzo AWS Backup con Amazon EFS
- Backup e ripristino on demand per DynamoDB
- Snapshot Amazon EBS
- Backup e ripristino di istanze DB di Amazon RDS
  - Panoramica di backup e ripristino di un cluster di database Aurora
- Utilizzo AWS Backup con FSx for Windows File Server
- Utilizzo AWS Backup con FSx for Lustre
- Eseguire il backup dei volumi in AWS Storage Gateway
- Backup e ripristino in Amazon DocumentDB
- Backup e ripristino di un cluster Amazon Neptune

Misurazione, costi e fatturazione

AWS Backup prezzi

AWS Backup I prezzi correnti sono disponibili alla pagina AWS Backup prezzi.

> **Important**
>
> Per evitare costi aggiuntivi, configura la policy di conservazione con una durata di storage a caldo di almeno una settimana.
> Ad esempio, supponi di eseguire backup giornalieri e di mantenerli per un giorno. Inoltre, supponiamo che le risorse protette siano così grandi da richiedere un'intera giornata per completare il backup. AWS Backup implementa il periodo di conservazione di un giorno e rimuove il backup dalla memoria esterna al termine del processo di backup. Il giorno successivo, AWS Backup non è possibile creare un backup incrementale perché non è disponibile alcun backup nella memoria a caldo. Poiché questo periodo di conservazione non ha seguito le best practice, l'utente si assume il rischio e le spese di creazione di un backup completo ogni giorno.
> Contatta AWS Support per ulteriore assistenza.

AWS Backup fatturazione

Quando un tipo di risorsa supporta la AWS Backup gestione completa, gli addebiti per AWS Backup l'attività (inclusi archiviazione, trasferimento dati, ripristino ed eliminazione anticipata) vengono visualizzati nella sezione «Backup» della Amazon Web Services fattura. Per un elenco dei servizi che supportano la AWS Backup gestione completa, consulta la sezione AWS Backup Gestione completa nella Disponibilità delle funzionalità per risorsa tabella.

Quando un tipo di risorsa non supporta la AWS Backup gestione completa, la fatturazione di alcune AWS Backup attività, come i costi di archiviazione per i backup, viene riflessa dal rispettivo AWS servizio.

Errori del processo di copia

I costi verranno addebitati solo dopo la creazione di un punto di ripristino nel vault di destinazione. Non è previsto alcun addebito quando un processo di copia non va a buon fine e non viene creato alcun punto di ripristino.

Tag di allocazione dei costi

È possibile utilizzare i tag di allocazione dei costi per tracciare e ottimizzare AWS Backup i costi a livello dettagliato e visualizzare e filtrare tali tag utilizzando. AWS Cost Explorer

Per utilizzare i tag di allocazione dei costi, consulta Automating backups and optimizing backup costs for Amazon EFS using AWS Backup e Utilizzo dei tag per l'allocazione dei costi.

AWS Backup Prezzi di Audit Manager

AWS Backup Audit Manager addebita l'utilizzo in base al numero di valutazioni di controllo. Una valutazione di controllo è la valutazione di una risorsa rispetto a un controllo. I costi di valutazione del controllo sono indicati sulla AWS Backup fattura. Per i prezzi correnti di valutazione del controllo, consulta Prezzi di AWS Backup.

Per utilizzare i controlli AWS Backup Audit Manager, è necessario abilitare AWS Config la registrazione per tenere traccia dell'attività di backup. AWS Config addebiti per ogni elemento di configurazione registrato e tali addebiti vengono visualizzati sulla AWS Config fattura. Per i prezzi attualmente registrati degli elementi di configurazione, consulta Prezzi di AWS Config.

Prezzi di Amazon Aurora

Durante il periodo di conservazione configurato per i backup continui di Aurora (fino a 35 giorni), gli snapshot non implicano costi di storage. Gli snapshot mantenuti oltre questa finestra vengono addebitati come backup completi.

AWS Backup blog, video, tutorial e altre risorse

Per ulteriori informazioni su AWS Backup, consulta quanto segue:

- Backup e ripristino di macchine virtuali VMware locali utilizzando. AWS Backup Con Olumuyiwa Koya ed Ezekiel Oyerinde (giugno 2022).
- Utilizzato AWS Backup per proteggere i database Amazon Aurora. Con Chris Hendon, Brandon Rubadou e Thomas Liddle (maggio 2022).
- Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups. Con Evan Peck e Sabith Venkitachalapathy (maggio 2022).
- Automatizza e migliora il tuo livello di sicurezza utilizzando e. AWS BackupAWS PrivateLink Con Bilal Alam (aprile 2022).
- Ottieni report giornalieri aggregati su più account e più regioni. AWS Backup Con Wali Akbari e Sabith Venkitachalapathy (febbraio 2022).
- Automatizza la visibilità dei risultati del backup utilizzando e. AWS Backup AWS Security Hub Con Kanishk Mahajan (gennaio 2022).
- Le 10 migliori pratiche di sicurezza per proteggere i backup in. AWS Con Ibukun Oyewumi (gennaio 2022).
- Ottimizzazione di SAS Grid on AWS con FSx for Lustre (e ottimizzazione del disaster recovery utilizzando). AWS Backup Con Matt Saeger e Shea Lutton (gennaio 2022).
- Centralizzazione della protezione e della conformità dei dati in Amazon Neptune con. AWS Backup Con Brian O'Keefe (novembre 2021).
- Manage backup and restore of Amazon DocumentDB (with MongoDB compatibility) with AWS Backup. Con Karthik Vijayraghavan (novembre 2021).
- Semplifica il controllo delle politiche di protezione dei dati con AWS Backup Audit Manager. Con Jordan Bjorkman e Harshitha Putta (novembre 2021).
- Migliora il livello di sicurezza dei tuoi backup con AWS Backup Vault Lock. Con Rolland Miller (ottobre 2021).

- Come conservare i tag delle risorse nei AWS Backup processi di ripristino. Con Ibukun Oyewumi e Sabith Venkitachalapathy (settembre 2021).
- Gestione dell'accesso ai backup utilizzando le politiche di controllo del servizio con AWS Backup. Con Ibukun Oyewumi e Sabith Venkitachalapathy (agosto 2021).
- Automatizza il backup centralizzato su larga scala in tutti AWS i servizi che utilizzano. AWS Backup Con Ibukun Oyewumi e Sabith Venkitachalapathy (luglio 2.021).
- Blog: Come semplificare il backup di Microsoft SQL Server utilizzando AWS Backup e VSS. Con Siavash Irani e Sepehr Samiei (luglio 2021).
- Automatizza la convalida del ripristino dei dati con. AWS Backup Con Mahanth Jayadeva (giugno 2021).
- Configurazione delle notifiche per monitorare i lavori. AWS Backup Con Virgil Ennes (giugno 2021).
- Automating backups and optimizing backup costs for Amazon EFS using AWS Backup. Con Prachi Gupta e Rohit Verma (giugno 2021).
- Gestione dei costi di backup di Amazon EFS: AWS Backup supporto per i tag di allocazione dei costi. Con Aditya Maruvada (maggio 2021).
- Crea e condividi backup crittografati tra account e regioni utilizzando. AWS Backup Con Prachi Gupta (maggio 2021).
- AWS Backup è ora approvato da FedRAMP High per le tue esigenze di conformità e protezione dei dati. Con Andy Grimes (maggio 2021).
- ZS Associates migliora l'efficienza del backup con. AWS Backup Con Mitesh Naik, Hiranand Mulchandani e Sushant Jadhav (maggio 2021).
- Tutorial: Backup e ripristino di Amazon EBS con AWS Backup. Con Fathima Kamal (aprile 2021).
- Video Tutorial: Managing Cross-Region Copies of Backups. Con David DeLuca (aprile 2021).
- Elimina più punti AWS Backup di ripristino utilizzando AWS Tools for PowerShell. Con Sherif Talaat (aprile 2021).
- Backup tra regioni e più account per l'utilizzo di Amazon FSx. AWS Backup Con Adam Hunter e Fathima Kamal (aprile 2021).
- Amazon CloudWatch Events and Metrics per AWS Backup. Con Rolland Miller (marzo 2021).
- Tutorial: Backup e ripristino di Amazon Relational Database Service (RDS) con. AWS Backup Con Fathima Kamal (marzo 2021).
- oint-in-time Ripristino P e backup continuo per Amazon RDS con AWS Backup. Con Kelly Griffin (marzo 2021).
- Automatizza AWS Backup con AWS Service Catalog. con John Husemoller (gennaio 2021).

- Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup. Con Cher Simon (gennaio 2021).
- AWS Riepilogo di re:Invent: Protezione dei dati e conformità con. AWS Backup Con Nancy Wang (dicembre 2020).
- AWS Backup fornisce una protezione centralizzata dei dati tra le tue risorse. AWS Con Nancy Wang (novembre 2020).
- Tech Talk: Data protection at scale with AWS Backup. Con Kareem Behairy (settembre 2020).
- Gestione centralizzata di più account con utilizzo di copie su più aree geografiche. AWS Backup Con Cher Simon (settembre 2020).
- Tutorial video: Gestione dei backup su larga scala a seconda dell'utilizzo. AWS Organizations AWS Backup Con Ildar Sharafeev (luglio 2020).
- Gestione dei backup su larga scala a seconda del vostro AWS Organizations utilizzo. AWS Backup Con Nancy Wang, Avi Drabkin, Ganesh Sundaresan e Vikas Shah (giugno 2020).
- Recupera file e cartelle Amazon EFS con AWS Backup. Con Abrar Hussain e Gurudath Pai (maggio 2020).
- Scheduling automated backups using Amazon EFS and AWS Backup. Con Rob Barnes (dicembre 2019).
- re:Invent Recording: AWS re:Invent 2019: Approfondimento su ft. AWS Backup Rackspace. Con Nancy Wang e Jason Pavao (dicembre 2019).
- Proteggi i tuoi dati con. AWS Backup Con Anthony Fiore (luglio 2019).
- Marketing Video: Introducing AWS Backup. Gennaio 2019.
- Video: Introduction to AWS Backup. Con AWS formazione e certificazione.

Configurazione AWS per la prima volta

Prima di AWS Backup utilizzarlo per la prima volta, completa le seguenti attività:

1. Registrati per AWS
2. Crea un utente IAM
3. Creazione di un ruolo IAM

Registrati per AWS

Quando ti iscrivi ad Amazon Web Services (AWS), ti Account AWS iscrivi automaticamente a tutti i servizi in AWS, inclusi AWS Backup. Ti vengono addebitati solo i servizi che utilizzi.

Per ulteriori informazioni sui tassi di AWS Backup utilizzo, consulta la pagina AWS Backup dei prezzi.

Se ne hai Account AWS già una, passa all'attività successiva. Se non disponi di un account AWS , utilizza la seguente procedura per crearne uno.

Per creare un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

Annota il tuo Account AWS numero, perché ti servirà per l'attività successiva.

Crea un utente IAM

I servizi in AWS, ad esempio AWS Backup, richiedono l'immissione di credenziali al momento dell'accesso, in modo che il servizio possa determinare se l'utente dispone delle autorizzazioni per

accedere alle sue risorse. AWS consiglia di non utilizzare l'utente Account AWS root per effettuare richieste. Creare invece un utente IAM e concedergli accesso completo. Questi utenti vengono definiti utenti amministratori. È possibile utilizzare le credenziali dell'utente amministratore, anziché le credenziali dell'utente Account AWS root, per interagire AWS ed eseguire attività, come creare un bucket, creare utenti e concedere loro autorizzazioni. Per ulteriori informazioni, consulta Credenziali utente root dell'Account AWS e credenziali utente IAM nella Documentazione di riferimento generale di AWS e Best practice IAM nella Guida per l'utente di IAM.

Se ti sei registrato AWS ma non hai ancora creato un utente IAM, puoi crearne uno utilizzando la console IAM.

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

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

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
(Non consigliato)		di amministrazione nella Guida per l'utente di IAM.	delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.

Per accedere come nuovo utente IAM, esci da AWS Management Console. Quindi usa il seguente URL, dove your_aws_account_id è il tuo Account AWS numero senza i trattini (ad esempio, se il tuo numero è, il tuo ID è): Account AWS `1234-5678-9012` Account AWS `123456789012`

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Immettere il nome utente e la password di IAM appena creati. Una volta effettuato l'accesso, la barra di navigazione visualizza your_user_name@your_aws_account_id.

Se non desideri che l'URL della pagina di accesso contenga il tuo ID, puoi creare un alias per l'account. Account AWS Dal pannello di controllo IAM, fai clic su Crea alias dell'account e immetti un alias, ad esempio il nome dell'azienda. Per effettuare l'accesso dopo aver creato un alias dell'account, utilizzare il seguente URL:

```
https://your_account_alias.signin.aws.amazon.com/console/
```

Per verificare il collegamento di accesso degli utenti IAM all'account, apri la console IAM e controlla in Alias dell'Account AWS sul pannello di controllo.

Creazione di un ruolo IAM

Puoi utilizzare la console IAM per creare un ruolo IAM che conceda le AWS Backup autorizzazioni per accedere alle risorse supportate. Dopo aver creato il ruolo IAM, puoi creare e collegare le policy al ruolo.

Per creare un ruolo IAM con la console

1. Accedi alla console di AWS gestione e apri la console IAM.
2. Nel pannello di navigazione della console IAM, scegli Ruoli e quindi Crea ruolo.
3. Seleziona Ruoli di servizio AWS e scegli Seleziona per AWS Backup. Scegli Successivo: autorizzazioni.
4. Nella pagina Allega policy di autorizzazione, seleziona `AWSBackupServiceRolePolicyForBackup` e `AWSBackupServiceRolePolicyForRestores`. Queste policy AWS gestite concedono AWS Backup l'autorizzazione per il backup e il ripristino di tutte le AWS risorse supportate. Per ulteriori informazioni sulle policy gestite e per visualizzare esempi, consulta Policy gestite.

   Quindi, scegliere Next: Tags (Fase successiva: Tag).
5. Scegli Prossimo: Rivedi.
6. In Role name (Nome ruolo) digita un nome che descriva lo scopo del ruolo. I nomi dei ruoli devono essere univoci all'interno del tuo Account AWS. Poiché varie entità possono fare riferimento al ruolo, non è possibile modificare il nome dopo la creazione.

   Selezionare Crea ruolo.
7. Nella pagina Roles (Ruoli) scegli il ruolo che hai creato per aprire la pagina dei dettagli.

Iniziare con AWS Backup

Questo tutorial mostra i passaggi generici per l'utilizzo AWS Backup di caratteristiche e funzionalità. Come per qualsiasi parte di questa documentazione tecnica, è necessario seguire la Console di AWS gestione nell'altra finestra.

Puoi anche imparare a utilizzarlo AWS Backup con un servizio specifico leggendo questi tutorial:

- Backup e ripristino di Amazon Relational Database Service (Amazon RDS) con AWS Backup
- Tutorial: Backup e ripristino di Amazon EBS con AWS Backup

Argomenti

Prerequisiti

Prima di iniziare, assicurati di disporre di quanto riportato di seguito:

- Un Account AWS. Per ulteriori informazioni, consulta Configurazione AWS per la prima volta.
- Almeno una risorsa supportata da AWS Backup.
- È necessario conoscere i AWS servizi e le risorse di cui si esegue il backup. Consulta l'elenco delle risorse AWS e delle applicazioni di terze parti supportate.

  Quando diventano disponibili nuovi AWS servizi, abilita l'utilizzo AWS Backup di tali servizi.

Per configurare i AWS servizi da utilizzare con AWS Backup

1. Accedere a e aprire la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup. AWS Management Console
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Attivazione del servizio scegliere Configura risorse.
4. Nella pagina Configura risorse, utilizza gli interruttori a levetta per abilitare o disabilitare i servizi utilizzati con. AWS Backup Quando i servizi sono configurati, scegliere Conferma. Assicurati che il AWS servizio che stai optando sia disponibile nel tuo. Regione AWS

Assegnazione di risorse a un piano di backupPer ulteriori informazioni, consulta. La AWS Backup console consente a un utente di assegnare un tipo di risorsa a un piano di backup; questo verrà incluso anche se l'opt-in non è abilitato per quel particolare servizio.

- Assicurati che le risorse di cui stai eseguendo il backup si trovino tutte nella stessa Regione AWS.

Per completare questo tutorial, puoi usare il tuo utente Account AWS root per accedere a. AWS Management Console Tuttavia, AWS Identity and Access Management (IAM) consiglia di non utilizzare l'utente Account AWS root. È preferibile creare un amministratore nell'account e utilizzare le rispettive credenziali per gestire le risorse nel proprio account. Per ulteriori informazioni, consulta Configurazione AWS per la prima volta.

La AWS Backup console offre diverse opzioni per il backup delle risorse. Puoi creare un backup on demand, pianificare e configurare la modalità di backup delle risorse oppure configurare le risorse per eseguire il backup automatico quando la risorsa viene creata.

Nozioni di base 1: attivazione del servizio

La AWS Backup console offre due modi per includere i tipi di risorse in un piano di backup: assegnare esplicitamente il tipo di risorsa in un piano di backup o includere tutte le risorse. Consulta i punti seguenti per comprendere come funzionano queste selezioni con adesioni al servizio.

- Se le assegnazioni delle risorse si basano solo sui tag, vengono applicate le impostazioni opt-in del servizio.
- Se un tipo di risorsa viene assegnato in modo esplicito a un piano di backup, verrà incluso nel backup anche se l'opt-in non è abilitato per quel particolare servizio. Questo non si applica ad

Aurora, Neptune e Amazon DocumentDB. Affinché questi servizi siano inclusi, l'opt-in deve essere abilitato.

- Se in un'assegnazione di risorse sono specificati sia il tipo di risorsa che i tag, i tipi di risorse specificati vengono filtrati per primi, quindi i tag filtrano ulteriormente tali risorse.

  Le impostazioni relative all'attivazione del servizio vengono ignorate per la maggior parte dei tipi di risorse. Tuttavia Aurora, Neptune e Amazon DocumentDB richiedono l'attivazione del servizio.
- Per Amazon FSx for NetApp ONTAP, quando utilizzi la selezione delle risorse basata su tag, applica i tag ai singoli volumi anziché all'intero file system.

Le scelte di attivazione si applicano all'account specifico e. Regione AWS Quando un account utilizza AWS Backup (crea un archivio di backup o un piano di backup) in una regione, l'account viene automaticamente inserito in tutti i tipi di risorse supportati dalla regione AWS Backup in quel momento. I servizi supportati aggiunti a quella regione in un secondo momento non verranno inclusi automaticamente in un piano di backup. Puoi scegliere di attivare questi tipi di risorse una volta che saranno supportati.

Poiché AWS Backup supporta sempre più AWS servizi e applicazioni di terze parti, potrebbe essere necessario rivedere questo passaggio per attivare le nuove risorse supportate.

AWS Backup non governa o gestisce i backup eseguiti in ambienti diversi da. AWS AWS Backup

Da attivare per l'utilizzo per AWS Backup proteggere tutti i tipi di risorse supportati

1. Accedere a e aprire la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup. AWS Management Console
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. In Attivazione del servizio, scegli Configura risorse.
4. Attiva l'accesso AWS Backup a tutte le risorse supportate spostando tutti gli interruttori verso destra.
5. Scegliere Confirm (Conferma).

Passaggi successivi

Per creare un backup su richiesta utilizzando AWS Backup, procedi con. Nozioni di base 2: creazione di un backup on demand

Nozioni di base 2: creazione di un backup on demand

Sulla AWS Backup console, la pagina Risorse protette elenca le risorse di cui è stato eseguito il backup AWS Backup almeno una volta. Se lo utilizzi AWS Backup per la prima volta, in questa pagina non sono elencate risorse, come volumi Amazon EBS o database Amazon RDS. Ciò è vero anche se tale risorsa è stata assegnata a un piano di backup che non abbia eseguito un processo di backup pianificato almeno una volta.

In questa prima fase viene creato un backup on demand delle risorse. La risorsa verrà elencata nella pagina Protected resources (Risorse protette).

Per creare un backup on demand

1. Accedi a e apri AWS Management Console la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Utilizzando il riquadro di navigazione, scegli Risorse protette, quindi Crea backup on demand.
3. Nella pagina Crea backup on demand, scegli il tipo di risorsa di cui desideri eseguire il backup, ad esempio, scegli DynamoDB per le tabelle Amazon DynamoDB.
4. Scegli il nome o l'ID della risorsa che desideri proteggere. Assicurati che la risorsa scelta sia quella desiderata.

   > **Note**
   >
   > Per Amazon FSx per Lustre, sono supportati i tipi di implementazione Persistent e Persistent_2.

5. Verificare che l'opzione Create backup now (Crea backup ora) sia selezionata. In questo modo viene avviato immediatamente un backup e si possono visualizzare prima le proprie risorse salvate nella pagina Protected resources (Risorse protette).
6. Specificare una transizione a un valore di storage di dati inattivi (se appropriato) e a un valore expire.

   > **Note**
   >
   > - Per visualizzare l'elenco di risorse che è possibile trasferire nell'archiviazione a freddo, consulta la sezione "Dal ciclo di vita all'archiviazione a freddo" della tabella Disponibilità delle funzionalità per risorsa. Tutti gli altri tipi di risorse vengono salvati

nello storage a caldo e ignorano l'espressione transizione allo storage a freddo. Il valore Expire è valido per tutti i tipi di risorse.

- Quando i backup scadono e sono contrassegnati per l'eliminazione come parte della politica del ciclo di vita, AWS Backup elimina i backup in un momento scelto casualmente nelle 8 ore successive. Questa finestra aiuta a garantire prestazioni costanti.

7. Scegliere un vault di backup esistente. Scegliendo Create new backup vault (Crea nuovo vault di backup), si apre una nuova pagina in cui è possibile creare un vault e al termine viene visualizzata nuovamente la pagina Create on-demand backup.
8. In Ruolo IAM scegliere Default role (Ruolo di default).

> **Note**
>
> Se il ruolo AWS Backup predefinito non è presente nel tuo account, viene creato un ruolo con le autorizzazioni corrette.

9. Se si desidera assegnare uno o più tag al proprio backup on demand, immettere una chiave e, facoltativamente, un valore, quindi scegliere Aggiungi tag.

> **Note**
>
> - Per le risorse Amazon EC2, copia AWS Backup automaticamente i tag delle risorse individuali e di gruppo esistenti, oltre a tutti i tag aggiunti a questo backup. Per ulteriori informazioni, consulta Copia dei tag nei backup.
> - Quando crei un piano di backup basato su tag, se scegli un ruolo diverso dal ruolo predefinito, assicurati che disponga delle autorizzazioni necessarie per eseguire il backup di tutte le risorse taggate. AWS Backup tenta di elaborare tutte le risorse con i tag selezionati. Se viene rilevata una risorsa a cui non è autorizzato l'accesso, il piano di backup ha esito negativo.

10. Scegliere Create on-demand backup (Crea backup on demand). In questo modo si accede alla pagina Processi, in cui è visualizzato un elenco di processi.
11. Se il tipo di risorsa è EC2, viene visualizzata la sezione Modifica le impostazioni di backup avanzate. Scegli Windows VSS se l'istanza EC2 esegue Microsoft Windows. Ciò consente di eseguire backup di Windows VSS coerenti con le applicazioni.

> **Note**
>
> AWS Backup attualmente supporta backup coerenti con le applicazioni di risorse in esecuzione solo su Amazon EC2. Non tutti i tipi di istanze o applicazioni sono supportati per i backup di Windows VSS. Per ulteriori informazioni, consulta Creazione di backup Windows VSS.

12. Scegliere ID del lavoro di Backup per la risorsa scelta per il backup per visualizzare i dettagli del lavoro.

Passaggi successivi

Per automatizzare l'attività di backup, passa a Nozioni di base 3: creazione di un backup pianificato.

Nozioni di base 3: creazione di un backup pianificato

In questa fase del AWS Backup tutorial, crei un piano di backup, gli assegni risorse e quindi crei un archivio di backup.

Prima di iniziare, assicurati di disporre dei prerequisiti richiesti. Per ulteriori informazioni, consulta Iniziare con AWS Backup.

Argomenti

Fase 1: creare un piano di backup in base a uno esistente

Un piano di backup è l'espressione di una policy che definisce il tempo e il modo in cui si desidera effettuare il backup delle risorse AWS , ad esempio tabelle Amazon DynamoDB o file system Amazon Elastic File System (Amazon EFS). Si assegnano risorse ai piani di backup, AWS Backup quindi si esegue automaticamente il backup e la conservazione dei backup di tali risorse in base al piano di backup. Per ulteriori informazioni, consulta Gestione dei backup mediante i piani di backup.

Esistono due modi per creare un nuovo piano di backup: da zero oppure in base a un piano di backup esistente. Questo esempio utilizza la AWS Backup console per creare un piano di backup modificando un piano di backup esistente.

Per creare un piano di backup da un piano esistente

1. Accedere a e aprire AWS Management Console la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Dal pannello di controllo, scegliere Gestisci i piani di Backup. Oppure, utilizzando il riquadro di navigazione, scegli Piani di backup e seleziona Crea un piano di backup.
3. Scegli Inizia con modello, seleziona un piano dall'elenco (ad esempio, `Daily-Monthly-1yr-Retention`) e immetti un nome della casella Nome del piano di backup.

   > **Note**
   >
   > Se si tenta di creare un piano di backup identico a un piano esistente, viene visualizzato un errore `AlreadyExistsException`.

4. Nella pagina di riepilogo del piano, scegli la regola di backup desiderata, quindi seleziona Modifica.
5. Controlla e scegli i valori per la regola (consulta Opzioni e configurazione del piano di backup per le opzioni della regola).
6. Per il vault di backup, scegli Predefinito o Crea nuovo vault di backup per creare un nuovo vault.
7. (Facoltativo): scegline uno Regione AWS dall'elenco in Regione di destinazione per copiare il backup in un'altra regione. Per aggiungere altre regioni, scegli Aggiungi copia.
8. Una volta completata la modifica della regola, scegli Salva backup.

Nella pagina Riepilogo scegliere Assegna risorse per la preparazione della sezione successiva.

Fase 2: assegnare risorse a un piano di backup

Dopo aver creato un piano di backup, è necessario assegnare le AWS risorse a tale piano. Per ulteriori informazioni sull'assegnazione delle risorse, consulta Assegnazione di risorse a un piano di backup.

Se non disponi già di AWS risorse esistenti da assegnare a un piano di backup, crea alcune nuove risorse da utilizzare per questo esercizio. Crea una o due risorse utilizzando risorse AWS e applicazioni di terze parti supportate.

Per assegnare risorse a un piano di backup

1. Seguendo le fasi precedenti dovrebbe essere visualizzata la pagina Assegna risorse.
2. Digita un Nome assegnazione di risorsa.
3. Per Ruolo IAM, scegli Ruolo predefinito. Se scegli un altro ruolo, devi disporre delle autorizzazioni per eseguire il backup di tutte le risorse assegnate.
4. Nella sezione Assegna risorse, scegli Includi tutti i tipi di risorse. Un tipo di risorsa è un AWS servizio AWS Backup supportato o un'applicazione di terze parti. Questo piano di backup ora proteggerà tutti i tipi di risorse che hai scelto di proteggere utilizzando AWS Backup
5. Scegli Assegna risorse.

Viene nuovamente visualizzata la pagina Riepilogo del piano di backup. Scegli Crea piano di backup per distribuire il primo piano di backup.

Fase 3: creare un vault di backup

Anziché utilizzare il vault di backup di default che viene creato automaticamente nella console di AWS Backup , è possibile creare vault di backup specifici per salvare e organizzare gruppi di backup nello stesso vault.

Per ulteriori informazioni sui vault di backup, consulta Vault di backup.

Per creare un vault di backup

1. Sulla AWS Backup console, nel riquadro di navigazione, scegli Backup vault.

   > **Note**
   >
   > Se il pannello di navigazione non è visibile sul lato sinistro, puoi aprirlo scegliendo l'icona del menu nell'angolo in alto a sinistra della console. AWS Backup

2. Scegliere Create backup vault (Crea vault di backup).

3. Immettere un nome per il vault di backup. È possibile denominare il vault in modo che rifletta ciò che verrà archiviato o per rendere più facile la ricerca dei backup. Ad esempio, si potrebbe assegnare il nome **`FinancialBackups`**.
4. Seleziona un tasto AWS Key Management Service ()AWS KMS. Puoi utilizzare una chiave che hai già creato o selezionare la chiave AWS Backup KMS predefinita.

   > **Note**
   >
   > La AWS KMS chiave specificata qui si applica solo ai backup di servizi che supportano la crittografia AWS Backup indipendente. Per visualizzare l'elenco dei tipi di risorse che supportano la crittografia AWS Backup indipendente, consulta la sezione « AWS Backup Gestione completa» della Disponibilità delle funzionalità per risorsa tabella.

5. Facoltativamente, è possibile aggiungere tag che consentano di cercare e identificare il vault di backup. Ad esempio, si potrebbe aggiungere un tag **`BackupType:Financial`**.
6. Scegliere Crea vault di Backup.
7. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup) e verificare che il vault di backup sia stato aggiunto.

> **Note**
>
> È ora possibile modificare una regola di backup in uno dei piani di backup per archiviare i backup creati da tale regola nel vault di backup appena creato.

Passaggi successivi

Per eseguire specificatamente il backup di file system Amazon EFS, passa a Nozioni di base 4: creazione di backup automatici Amazon EFS.

Nozioni di base 4: creazione di backup automatici Amazon EFS

Quando crei un file system Amazon Elastic File System (Amazon EFS) utilizzando la console Amazon EFS, i backup automatici vengono attivati per impostazione predefinita. Se desideri eseguire automaticamente il backup di un file system Amazon EFS esistente, puoi farlo utilizzando la console, l'API o la CLI di Amazon EFS.

Per eseguire automaticamente il backup di un file system Amazon EFS esistente utilizzando la console

1. Apri la console di Amazon EFS all'indirizzo https://console.aws.amazon.com/efs.
2. Nella pagina File system, scegli un file system per attivare i backup automatici.
3. Scegli Modifica nel pannello delle impostazioni Generale.
4. Per attivare i backup automatici, scegli Abilita i backup automatici.

L'impostazione predefinita del piano di backup è `daily backups, 35-day retention`. La finestra di backup predefinita (l'intervallo di tempo quando il backup verrà eseguito) è impostata per iniziare alle 5 del mattino ora UTC (Coordinated Universal Time) e dura 8 ore.

> **Note**
>
> Il vault di backup automatico `aws/efs/automatic-backup-vault` di Amazon EFS è riservato solo per tali backup automatici.
> Questo archivio non deve essere utilizzato per creare copie su più account o come destinazione per i backup creati da altri piani di backup non automatizzati. Se viene utilizzato come una destinazione per altri piani di backup, si riceverà un errore "privilegi insufficienti".

AWS Backup crea un ruolo collegato al servizio per tuo conto nel tuo account. Questo ruolo dispone delle autorizzazioni richieste per eseguire backup Amazon EFS. Per ulteriori informazioni sui ruoli collegati ai servizi, consulta Utilizzo di ruoli collegati ai servizi per AWS Backup.

Per step-by-step istruzioni su come attivare o disattivare i backup automatici utilizzando la console, l'API o la CLI di Amazon EFS, consulta Backup automatici nella Amazon Elastic File System User Guide.

Passaggi successivi

Per visualizzare i backup creati in precedenza, passa a Nozioni di base 5: visualizzazione dei processi di backup e dei punti di ripristino.

Nozioni di base 5: visualizzazione dei processi di backup e dei punti di ripristino

Con AWS Backup, puoi visualizzare lo stato e altri dettagli delle attività di backup e ripristino tra i AWS servizi che utilizzi.

Nella AWS Backup dashboard è possibile gestire i piani di backup, creare backup su richiesta, ripristinare i backup e visualizzare lo stato dei processi di backup e ripristino.

Argomenti

Visualizzazione dello stato dei processi di backup

Utilizza la AWS Backup dashboard per visualizzare rapidamente lo stato dell'attività di backup e ripristino.

Per visualizzare lo stato del lavoro di backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Per visualizzare lo stato delle operazioni di backup, scegliere Backup jobs details (Dettagli processi di backup). In questo modo si accede alla pagina Lavori di Backup, in cui sono visualizzate tabelle contenenti lavori di backup e lavori di ripristino.
4. È possibile filtrare i lavori visualizzati in base al tempo. Ad esempio, i lavori creati nelle ultime 24 ore, nell'ultima settimana o negli ultimi 30 giorni. È possibile anche impostare il numero di processi da visualizzare per pagina scegliendo l'icona a forma di ingranaggio.

Visualizzazione di tutti i backup presenti in un vault

Segui questi passaggi per visualizzare i backup creati in un vault specifico in AWS Backup.

Visualizzazione di tutti i backup presenti in un vault

1. Sulla AWS Backup console, nel riquadro di navigazione, scegli Backup vault.
2. Scegliere il vault utilizzato durante la creazione di un backup on demand o pianificato e visualizzare tutti i backup in esso creati.

> **Note**
>
> Ogni backup dispone di uno stato, che è di solito Completato. Se per qualche motivo non è AWS Backup possibile eliminare un backup in base alla configurazione del ciclo di vita, contrassegna questo backup come scaduto. Il costo dello storage consumato dai backup con stato Scaduto viene addebitato, pertanto è consigliabile eliminarli.

Visualizzazione dei dettagli delle risorse protette

Nella pagina Protected resources (Risorse protette) è possibile esplorare i dettagli delle risorse sottoposte a backup in AWS Backup.

Visualizzazione delle risorse protette

1. Sulla AWS Backup console, nel riquadro di navigazione, scegli Risorse protette.
2. Visualizza le AWS risorse di cui viene eseguito il backup. Scegliere una risorsa nell'elenco per esplorare i relativi backup.

Passaggi successivi

Per ripristinare un punto di ripristino visualizzato, passa a Nozioni di base 6: ripristino di un backup.

Nozioni di base 6: ripristino di un backup

Dopo aver eseguito il backup almeno una volta, una risorsa viene considerata protetta ed è disponibile per il ripristino AWS Backup. Segui queste fasi per ripristinare una risorsa utilizzando la console di AWS Backup .

Per informazioni sui parametri di ripristino per servizi specifici o sul ripristino di un backup utilizzando AWS CLI o l' AWS Backup API, vedere Ripristino di un backup.

Ripristino di una risorsa

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Risorse protette e l'ID della risorsa che si desidera ripristinare.
3. Viene visualizzato un elenco dei punti di ripristino, incluso il tipo di risorsa, in base a ID risorsa. Scegliere una risorsa per aprire la pagina Dettagli delle risorse.
4. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
5. Specificare i parametri di ripristino. I parametri di ripristino visualizzati sono specifici del tipo di risorsa selezionato.

   > **Note**
   >
   > Se si conserva un solo backup, è possibile ripristinare lo stato del file system solo come era al momento in cui è stato eseguito il backup. Non è possibile eseguire il ripristino da backup incrementali precedenti.

   Per istruzioni su come ripristinare risorse specifiche, consulta Ripristino di un backup.
6. Per Ripristina ruolo, scegliere Ruolo predefinito.

   > **Note**
   >
   > Se il ruolo AWS Backup predefinito non è presente nel tuo account, viene creato un ruolo con le autorizzazioni corrette.
7. Scegli Restore backup (Ripristina backup).

   Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.

> **Note**
>
> Quando si esegue un ripristino per ripristinare elementi specifici all'interno di un'istanza Amazon EFS, è possibile ripristinare tali elementi in un file system nuovo o esistente. Se ripristini gli elementi in un file system esistente, AWS Backup crea una nuova directory

Amazon EFS dalla directory principale per contenere gli elementi. La gerarchia completa degli elementi specificati viene mantenuta nella directory di ripristino. Ad esempio, se la directory A contiene le sottodirectory B, C e D, AWS Backup mantiene la struttura gerarchica quando A, B, C e D.
A prescindere che si esegua un ripristino parziale Amazon EFS su un file system esistente o su un nuovo file system, ogni tentativo di ripristino crea una nuova directory di ripristino al di fuori della directory principale per contenere i file ripristinati. Se si tenta di eseguire più ripristini per lo stesso percorso, potrebbero esistere diverse directory contenenti gli elementi ripristinati.

Per ripristinare un'istanza Amazon EFS

Se stai ripristinando un'istanza Amazon EFS, puoi eseguire un Ripristino completo, che ripristina l'intero file system. In alternativa, puoi ripristinare file e directory specifici utilizzando il ripristino a livello di elemento. I ripristini a livello di elemento hanno dei limiti. Per ulteriori informazioni, consulta Ripristino di un file system EFS. Per informazioni sul ripristino di altri tipi di risorse, consulta Ripristino di un backup.

> **Note**
>
> Per ripristinare un'istanza Amazon EFS, occorre "consentire" `backup:startrestorejob`.

Per informazioni dettagliate sul ripristino di un backup, consulta Ripristino di un backup.

Passaggi successivi

Con AWS Backup Audit Manager, puoi controllare l'attività e le risorse di backup. Inoltre, puoi creare report da utilizzare come prova dei processi di backup, ripristino e copia. Per creare un report, consulta Nozioni di base 7: creazione di un report di audit.

Nozioni di base 7: creazione di un report di audit

NelNozioni di base 5: visualizzazione dei processi di backup e dei punti di ripristino, hai osservato la tua attività di backup nelle viste AWS Backup Dashboard, Backup vault e Protected Resources. Tuttavia, queste viste sono dinamiche e si aggiornano a seconda di quando vengono visitate. Queste

viste non sono necessariamente la prova migliore della conformità continua rispetto ai requisiti e ai controlli di protezione dei dati aziendali nel tempo.

In questo passaggio, creerai un report sui job di backup su richiesta utilizzando AWS Backup Audit Manager.

AWS Backup Audit Manager fornisce una varietà di report di audit in formato CSV, JSON o entrambi i formati ogni giorno e su richiesta al tuo bucket Amazon S3. Puoi verificare la conformità dell'attività e delle risorse di backup rispetto a un numero di controlli personalizzabili. Puoi ricevere report sui processi di backup, copia e ripristino. Il report del processo di backup dimostra che i processi di backup sono stati eseguiti.

Di seguito è riportato un esempio di un piano di backup.

```
{
  "reportItems": [
    {
      "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z",
      "accountId": "112233445566",
      "region": "us-west-2",
      "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC00000",
      "jobStatus": "COMPLETED",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee77800000",
      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-
b489-4301-83ac-4b7dd7200000",
      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e6abcde",
      "creationDate": "2021-07-14T23:53:47.229Z",
      "completionDate": "2021-07-15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5aabcde",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 8589934592,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/
AWSBackupDefaultServiceRole"
    }
  ]
}
```

Per creare un report di backup (incluso un report di backup on demand), crea innanzitutto un piano di report per automatizzare i report e distribuirli in un bucket Amazon S3.

Un piano di report richiede che si disponga di un bucket Amazon S3 per ricevere i report. Per istruzioni sulla configurazione di un nuovo bucket S3, consulta Fase 1: creare il primo bucket S3 nella Guida per l'utente di Amazon Simple Storage Service.

Per creare un piano di report

1. Accedi a e apri la console all' AWS Management Console indirizzo https://console.aws.amazon.com/backup. AWS Backup
2. Nel riquadro di navigazione a sinistra, scegli Report.
3. Scegli Crea piano di report.
4. Seleziona Esegui il backup del report del processo dall'elenco a discesa.
5. Per Nome del piano report, immetti **`TestBackupJobReport`**.
6. Per Formato file, scegli CSV e JSON.
7. Per Nome del bucket S3, seleziona la destinazione per i report dall'elenco a discesa.
8. Scegli Crea piano di report.

Successivamente, devi consentire al tuo bucket S3 di ricevere report da. AWS Backup AWS Backup Audit Manager genera automaticamente una policy di accesso S3 per te.

Per visualizzare e applicare questa policy di accesso

1. Nel riquadro di navigazione a sinistra, scegli Report.
2. In Nome del piano report, scegli il nome del piano di report (`TestBackupJobReport`).
3. Scegli Modifica.
4. Scegli Visualizza la policy di accesso per il bucket S3.
5. Scegli Copia le autorizzazioni.
6. Scegli Modifica la policy del bucket per modificare la policy del bucket S3 di destinazione e consentire la ricezione di report del processo di backup.
7. Copia o aggiungi le autorizzazioni alla policy del bucket S3 di destinazione.

Quindi, crea il primo report del processo di backup.

Per creare un report di backup on demand

1. Nel riquadro di navigazione a sinistra, scegli Report.

2. In Nome del piano report, scegli il nome del piano di report (`TestBackupJobReport`).
3. Scegli Crea report on demand.

Infine, visualizza il report.

Per visualizzare il report

1. Nel riquadro di navigazione a sinistra, scegli Report.
2. In Nome del piano report, scegli il nome del piano di report (`TestBackupJobReport`).
3. Nella sezione Processi di report, scegli il collegamento S3. Questa operazione consente di accedere al bucket S3 di destinazione.
4. Scegli Download (Scarica).
5. Apri il report utilizzando il programma utilizzato per lavorare con i file CSV o JSON.

Passaggi successivi

Per eseguire la pulizia delle risorse per le nozioni di base ed evitare addebiti indesiderati, passa a Nozioni di base 8: pulizia delle risorse.

Nozioni di base 8: pulizia delle risorse

Dopo aver eseguito tutte le attività in Iniziare con AWS Backup, è possibile eliminare le risorse create per evitare l'addebito di costi non necessari.

Argomenti

- Passaggio 1: Eliminare le risorse ripristinate AWS
- Fase 2: eliminare il piano di backup
- Fase 3: eliminare i punti di ripristino
- Fase 4: eliminare il vault di backup
- Fase 5: eliminare il piano di report
- Fase 6: eliminare i report

Passaggio 1: Eliminare le risorse ripristinate AWS

Per eliminare AWS le risorse ripristinate da un punto di ripristino, come i volumi Amazon Elastic Block Store (Amazon EBS) o le tabelle Amazon DynamoDB, usi la console per quel servizio. Ad esempio, per eliminare un file system Amazon Elastic File System (Amazon EFS), utilizza la console di Amazon EFS.

> **Note**
>
> Questa informazione fa riferimento alle risorse ripristinate, non ai punti di ripristino archiviati in un vault di backup.

Fase 2: eliminare il piano di backup

Se non si desidera creare backup pianificati, è necessario eliminare i piani di backup. Prima di poter eliminare un piano di backup, occorre eliminare tutte le assegnazioni di risorse a tale piano di backup.

Segui queste fasi per eliminare un piano di backup:

Eliminazione di un piano di backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup plans (Piani di backup).
3. Nella pagina Backup plans (Piani di backup) scegliere il piano di backup che si desidera eliminare. In questo modo si accede alla pagina dei dettagli per il backup.
4. Per eliminare l'assegnazione di risorse per il proprio piano, scegliere il pulsante di opzione accanto al nome dell'assegnazione, quindi scegliere Elimina.
5. Per eliminare il piano di backup, scegliere Elimina nell'angolo in alto a destra della pagina.
6. Nella pagina di conferma immettere il nome del piano e scegliere Delete plan (Elimina piano).

Fase 3: eliminare i punti di ripristino

Successivamente, è possibile eliminare i punti di ripristino di backup presenti nel vault di backup.

Eliminazione di punti di ripristino

1. Sulla AWS Backup console, nel riquadro di navigazione, scegli Backup vault.

2. Nella pagina Backup vaults (Vault di backup) scegliere il vault di backup in cui sono archiviati i backup.
3. Controlla il punto di ripristino e scegli Elimina.
4. Se stai eliminando più punti di ripristino, procedi come segue:

    a. Se l'elenco contiene un backup continuo, scegli se mantenere o eliminare i dati del backup continuo.

    b. Per eliminare tutti i punti di ripristino elencati, digita **`delete`**, quindi scegli Elimina punti di ripristino.

    Mantieni la scheda del browser aperta finché non vedi il banner verde di esito positivo nella parte superiore della pagina. La chiusura prematura di questa scheda interromperà il processo di eliminazione e alcuni dei punti di ripristino che desideravi eliminare potrebbero essere ignorati. Per ulteriori informazioni, consulta Eliminazione di backup.

Fase 4: eliminare il vault di backup

In genere, non è possibile eliminare il vault di backup predefinito. Tuttavia, se uno o più vault sono presenti in una regione, è possibile eliminare il vault di backup predefinito in tale regione utilizzando AWS CLI.

Puoi eliminare altri vault non predefiniti dopo aver eliminato tutti i backup (punti di ripristino) contenuti al loro interno. A questo scopo, seleziona Elimina nel vault vuoto.

Fase 5: eliminare il piano di report

Il piano di report invia automaticamente un nuovo report ogni giorno. Per evitare che ciò avvenga, elimina il piano di report.

Per eliminare il piano di report

1. Sulla AWS Backup console, nel riquadro di navigazione, scegli Report.
2. In Nome del piano report, scegli il nome del piano di report.
3. Scegli Elimina.
4. Immetti il nome del piano di report, quindi scegli Elimina piano di report.

Fase 6: eliminare i report

Puoi eliminare i report seguendo le istruzioni in Eliminazione di un singolo oggetto per ciascuno dei report. Se il bucket S3 di destinazione non è più necessario, dopo aver eliminato tutti gli oggetti dal bucket, puoi eliminare il bucket seguendo le istruzioni in Eliminazione di un bucket.

Gestione dei backup mediante i piani di backup

Nel AWS Backup, un piano di backup è un'espressione di policy che definisce quando e come eseguire il backup AWS delle risorse, come le tabelle Amazon DynamoDB o i file system Amazon Elastic File System (Amazon EFS). È possibile assegnare risorse ai piani di backup ed eseguire AWS Backup automaticamente il backup e la conservazione dei backup di tali risorse in base al piano di backup. Puoi creare più piani di backup se disponi di carichi di lavoro con requisiti di backup differenti. Per impostazione predefinita, le finestre di backup sono ottimizzate da AWS Backup. È possibile personalizzare la finestra di backup nella console o a livello di codice.

AWS Backup archivia in modo efficiente i backup periodici in modo incrementale. Il primo backup di una risorsa di AWS esegue il backup di una copia completa dei dati. Per ogni backup incrementale successivo, viene eseguito il backup solo delle modifiche alle AWS risorse. I backup incrementali consentono di approfittare della protezione dei dati garantita da backup frequenti, riducendo al minimo i costi di archiviazione.

AWS Backup inoltre, gestisce senza problemi il ciclo di vita del piano di backup in base alle impostazioni di conservazione, consentendoti di eseguire il ripristino quando necessario.

Le sezioni seguenti forniscono le nozioni di base per la gestione della strategia di backup in. AWS Backup

Argomenti

Creazione di un piano di backup

Puoi creare un piano di backup utilizzando la AWS Backup console, l'API, la CLI, l'SDK o un modello. AWS CloudFormation

Argomenti

- Opzioni e configurazione del piano di backup
- AWS CloudFormation modelli per piani di backup

Creazione di piani di backup tramite la console di AWS Backup

Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup. Dal pannello di controllo, scegliere Gestisci i piani di Backup. Oppure, utilizzando il riquadro di navigazione, scegli Piani di backup e seleziona Crea un piano di backup.

Opzioni di avvio

Sono disponibili tre scelte per il nuovo piano di backup:

- Fase 1: creare un piano di backup in base a uno esistente
- Creazione di un nuovo piano
- Creazione di piani di backup utilizzando AWS CLI

In questo tutorial, scegliamo Crea un nuovo piano. Ogni parte della configurazione include un collegamento a una sezione estesa più avanti nella pagina che è possibile selezionare per maggiori dettagli.

1. Inserisci il nome del piano in Nome del piano di backup. Non è possibile modificare il nome di un piano dopo averlo creato.

   Se si tenta di creare un piano di backup identico a un piano esistente, viene visualizzato un `AlreadyExistsException` errore.
2. Facoltativamente, puoi aggiungere i tag al piano di backup.
3. Configurazione regola di backup: nella sezione Configurazione regola di backup imposti la pianificazione, la finestra e il ciclo di vita del backup.
4. Pianifica:

   a. Inserisci il nome della regola di backup nel campo di testo.

   b. Nel menu a discesa per il vault di backup, scegli Predefinito o Crea nuovo vault di backup per creare un nuovo vault.

   c. Nel menu a discesa per la frequenza di backup, scegli la frequenza con cui desideri che questo piano crei un backup.

5. Finestra di backup:
   a. L'ora di inizio predefinita è 00:30 (00:30 nelle 24 ore) nel fuso orario locale del sistema.
   b. Avvia entro è per impostazione predefinita 8 ore. È possibile modificare questa impostazione per specificare una finestra temporale per l'avvio del backup.
   c. Completa entro è per impostazione predefinita 7 giorni.
6. Backup e point-in-time ripristino continui (PITR): È possibile selezionare Abilita backup continui per il ripristino (PITR). point-in-time Per verificare quali risorse sono supportate per questo tipo di backup, consulta la matrice Disponibilità delle funzionalità per risorsa.
7. Ciclo di vita
   a. Archiviazione a freddo: seleziona questa casella per consentire ai tipi di risorse idonei di passare all'archiviazione a freddo in base alla tempistica specificata nel periodo di conservazione totale. Per utilizzare l'archiviazione a freddo, è necessario disporre di un periodo di conservazione totale pari o superiore a 90 giorni.
   b. Archiviazione a freddo per Amazon EBS è Archivio snapshot Amazon EBS. Gli snapshot sottoposti a transizione al livello di archiviazione vengono visualizzati nella console nel livello a freddo. Se l'archiviazione a freddo è abilitata e la frequenza di backup è al massimo mensile, puoi fare in modo che il piano di backup effettui la transizione degli snapshot EBS.
   c. Il periodo di conservazione totale è il numero di giorni di archiviazione della risorsa in AWS Backup. È il numero totale di giorni di archiviazione a caldo e archiviazione a freddo.
8. (Facoltativo) Utilizza Copia nella destinazione per creare una copia in più regioni delle risorse idonee, se desideri archiviare la copia di un backup in un'altra Regione AWS.
9. (Facoltativo) Tag aggiunti ai punti di ripristino.
10. Quando tutte le sezioni sono impostate secondo le tue specifiche, scegli Salva regola di backup.

Creazione di piani di backup utilizzando AWS CLI

Puoi anche definire il piano di backup in un documento JSON e fornirlo utilizzando la console di AWS Backup o AWS CLI. Il seguente documento JSON contiene un piano di backup di esempio che crea un backup giornaliero alle 1:00 ora del Pacifico (l'ora locale si adatta alle condizioni diurne, standard o estive, se applicabile). Elimina automaticamente un backup dopo un anno.

```
{
  "BackupPlan":{
    "BackupPlanName":"test-plan",
```

```
    "Rules":[
      {
        "RuleName":"test-rule",
        "TargetBackupVaultName":"test-vault",
        "ScheduleExpression":"cron(0 1 ? * * *)",
        "ScheduleExpressionTimezone":"America/Los_Angeles",
        "StartWindowMinutes":integer, // Value is in minutes
        "CompletionWindowMinutes":integer, // Value is in minutes
        "Lifecycle":{
          "DeleteAfterDays":integer, // Value is in days
        }
      }
    ]
  }
}
```

È possibile archiviare il documento JSON con un nome a scelta. Il seguente comando CLI mostra l'utilizzo del comando `create-backup-plan` con un file JSON denominato `test-backup-plan.json`:

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

Nota che mentre alcuni sistemi numerano i giorni della settimana da 0 a 6, noi li numeriamo da 1 a 7. Per ulteriori informazioni, consulta le espressioni Cron. Per ulteriori informazioni sui fusi orari, consulta il riferimento TimeZoneall'API Amazon Location Service.

Opzioni e configurazione del piano di backup

Quando definisci un piano di backup nella AWS Backup console, configuri le seguenti opzioni:

Nome del piano di backup

È necessario fornire un nome univoco per il piano di backup.

Se si sceglie un nome identico al nome di un piano esistente, sarà restituito un messaggio di errore.

Regole di backup

I piani di backup sono composti da una o più regole di backup. Per aggiungere regole di backup a un piano di backup o modificare le regole esistenti in un piano di backup:

1. Dalla AWS Backup console, nel riquadro di navigazione a sinistra, scegli Piani di Backup.
2. In Nome del piano di backup, selezionare un piano di backup.
3. Nella sezione Regole di Backup:
   - Per aggiungere una regola di backup, scegliere Aggiungi regola di backup.
   - Per modificare una regola di backup esistente, selezionare la regola, quindi scegliere Modifica.

> **Note**
>
> Se disponi di un piano di backup con più regole e gli intervalli di tempo delle due regole si sovrappongono, AWS Backup ottimizza il backup ed esegue un backup per la regola con il tempo di conservazione più lungo. L'ottimizzazione tiene conto della finestra di avvio completa, non solo del momento in cui viene eseguito il backup giornaliero.

Ogni regola è formata dagli elementi indicati di seguito.

Nome della regola di backup

I nomi delle regole di backup rispettano la distinzione tra lettere maiuscole e minuscole. Devono contenere da 1 a 50 caratteri alfanumerici o trattini.

Frequenza del backup

La frequenza di backup determina la frequenza di AWS Backup creazione di un backup istantaneo. Utilizzando la console è possibile scegliere che venga creato ogni ora, ogni 12 ore, una volta al giorno, una volta alla settimana o una volta al mese. È inoltre possibile creare un'espressione Cron che crea backup snapshot con una frequenza che può arrivare fino a quella oraria. Utilizzando la AWS Backup CLI, è possibile pianificare i backup delle istantanee con una frequenza oraria.

Se si seleziona la frequenza settimanale, è possibile specificare il giorno della settimana in cui creare il backup. Se si seleziona la frequenza mensile, è possibile scegliere il giorno del mese.

Puoi anche selezionare la casella di controllo Abilita backup continui per risorse supportate per creare una regola di backup continuo abilitata al point-in-time ripristino (PITR). A differenza dei backup istantanei, i backup continui consentono di eseguire il ripristino. point-in-time Per ulteriori informazioni sui backup continui, consulta Ripristino Point-in-Time.

Finestra di backup

Le finestre di backup sono costituite dall'ora di inizio della finestra di backup e dalla durata della finestra in ore. I processi di backup vengono avviati all'interno di questa finestra. Le impostazioni predefinite nella console sono:

- 12:30 locali rispetto al fuso orario del sistema (0:30 nei sistemi con 24 ore su 24)
- Avvio entro 8 ore
- Completamento entro 7 giorni

  (il parametro Completa entro non si applica alle risorse Amazon FSx)

È possibile personalizzare la frequenza di backup e l'ora di inizio della finestra di backup utilizzando un'espressione Cron. Per vedere i sei campi delle espressioni AWS cron, consulta Cron Expressions nella Amazon CloudWatch Events User Guide. Due esempi di espressioni AWS cron sono `15 * ? * * *` (eseguire un backup ogni ora a 15 minuti dopo l'ora) e `0 12 * * ? *` (eseguire un backup ogni giorno alle 12:00 UTC). Per una tabella di esempi, fai clic sul collegamento precedente e scorri la pagina verso il basso.

AWS Backup valuta le espressioni cron tra 00:00 e 23:59. Se si crea una regola di backup che prevede l'avvio "ogni 12 ore" ma si indica un'ora di avvio successiva alle 11:59, questa verrà eseguita solo una volta al giorno.

I backup e il point-in-time ripristino continui (PITR) fanno riferimento alle modifiche registrate in un periodo di tempo; pertanto, non possono essere programmati con un'espressione time o cron.

> **Note**
>
> In generale, i servizi di AWS database non possono avviare i backup 1 ora prima o durante la finestra di manutenzione e Amazon FSx non può avviare i backup 4 ore prima o durante la finestra di manutenzione o la finestra di backup automatico (Amazon Aurora è esente da questa restrizione della finestra di manutenzione). I backup di snapshot pianificati in questi orari non andranno a buon fine.
> Quando si sceglie di utilizzare AWS Backup sia per i backup snapshot che per quelli continui per un servizio supportato si verifica un'eccezione. AWS Backup pianificherà automaticamente le finestre di backup per evitare conflitti. Consulta Point-in-Time Recovery per un elenco dei servizi supportati e istruzioni su come utilizzarli per eseguire backup continui. AWS Backup

Regole di backup sovrapposte

A volte, un piano di backup può contenere più regole sovrapposte. Quando le finestre di avvio di regole diverse si sovrappongono, AWS Backup conserva il backup in base alla regola con il periodo di conservazione più lungo. Ad esempio, si consideri un piano di backup con due regole:

1. Backup con frequenza oraria, con una finestra di avvio di 1 ora e conservazione per 1 giorno.
2. Backup ogni 12 ore, con una finestra di avvio di 8 ore e conservazione per 1 settimana.

Dopo 24 ore, la seconda regola crea due backup (perché prevede il periodo di conservazione più lungo). La prima regola crea otto backup (poiché la finestra di avvio di 8 ore della seconda regola ha impedito l'esecuzione di ulteriori backup ogni ora). Nello specifico:

Durante questa finestra di avvio	Questa regola crea 1 Backup
Da mezzanotte alle 8:00	12 ore
Dalle 8:00 alle 9:00	Orario
Dalle 9:00 alle 10:00	Orario
Dalle 10:00 alle 11:00	Orario
Dalle 11:00 a mezzogiorno	Orario
Da mezzogiorno alle 20:00	12 ore
Dalle 8:00 alle 9:00	Orario
Dalle 9:00 alle 10:00	Orario
Dalle 10:00 alle 11:00	Orario
Dalle 23:00 a mezzanotte	Orario

Durante la finestra di avvio, il processo di backup rimane in stato `CREATED` finché non viene avviato correttamente o fino alla scadenza della finestra di avvio. Se all'interno della finestra di avvio AWS Backup viene visualizzato un errore che consente di riprovare il processo, AWS Backup riproverà automaticamente a riavviare il processo almeno ogni 10 minuti fino all'avvio corretto del backup (lo

stato del processo cambia in`RUNNING`) o fino a quando lo stato del processo non cambia a `EXPIRED` (cosa che dovrebbe verificarsi al termine della finestra di inizio).

Ciclo di vita e livelli di archiviazione

I backup vengono archiviati per il numero di giorni specificato, noto come ciclo di vita del backup. I backup possono essere ripristinati fino alla fine del ciclo di vita.

Viene impostato come periodo di conservazione totale nella sezione relativa al ciclo di vita della configurazione delle regole di backup nella console. AWS Backup

Se si utilizza AWS CLI, questo viene impostato utilizzando il parametro. `DeleteAfterDays` Il periodo di conservazione degli snapshot può variare da 1 giorno a 100 anni (o a tempo indeterminato se non ne viene specificato uno), mentre il periodo di conservazione per i backup continui può variare da 1 giorno a 35 giorni. La data di creazione di un backup è la data di inizio del processo di backup, non la data di completamento. Se il processo di backup non viene completato nella stessa data di inizio, utilizza la data di inizio per calcolare i periodi di conservazione.

I backup vengono mantenuti in un livello di archiviazione. Ogni livello comporta un costo diverso per l'archiviazione e per il ripristino, come indicato in Prezzi di AWS Backup. Ogni backup viene creato e archiviato in un'archiviazione a caldo. A seconda del periodo di archiviazione scelto per il backup, è possibile passare il backup a un livello più economico chiamato archiviazione a freddo. In Disponibilità delle funzionalità per risorsa sono indicate le risorse che dispongono di questa funzionalità opzionale.

Console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Crea o modifica un piano di backup.
3. Nella sezione relativa al ciclo di vita della configurazione della regola di backup, seleziona la casella Sposta i backup dall'archiviazione a caldo a quella a freddo.
4. (Facoltativo) Se Amazon EBS è una delle risorse di cui esegui il backup e la frequenza di backup è al massimo mensile, puoi eseguire la transizione al livello a freddo utilizzando l'archiviazione degli snapshot EBS.
5. Immettete il valore (in giorni) per cui desiderate che i backup rimangano in una memoria calda. AWS Backup consiglia almeno 8 giorni.

6. Inserisci un valore (in giorni) per il periodo di conservazione totale. La differenza tra il periodo di conservazione totale e il tempo dell'archiviazione a caldo sarà il numero di giorni in cui i backup rimangono nell'archiviazione a freddo.

AWS CLI

1. Utilizza `create-backup-plan` o `update-backup-plan`.
2.
3. Includi il parametro booleano `OptInToArchiveForSupportedResources` per le risorse EBS.
4. Includere il parametro `MoveToColdStorageAfterdays`.
5. Utilizzo del parametro `DeleteAfterDays`. Questo deve essere il valore immesso per `MoveToColdStorageAfterDays` più 90 (giorni).

L'archiviazione a freddo è attualmente disponibile per i seguenti tipi di risorse:

Tipo di risorsa	Backup incrementale o completo nell'archiviazione a freddo
AWS CloudFormation	Incrementale
DynamoDB con funzionalità avanzate di	Backup completo, nessun backup incrementale in nessun livello
Amazon EBS (utilizzando l'archiviazione degli snapshot EBS)	Completo, i backup incrementali diventano completi dopo la transizione
Amazon EFS	Incrementale
Database SAP HANA eseguiti su istanze Amazon EC2	Incrementale
Amazon Timestream	Incrementale
Macchine virtuali VMware	Incrementale

Dopo aver abilitato la transizione all'archiviazione a freddo tramite la console o la riga di comando, per i backup nell'archiviazione a freddo si applicano le seguenti condizioni:

- I backup trasferiti devono essere conservati in celle frigorifere per un minimo di 90 giorni, oltre al periodo di conservazione a caldo. AWS Backup richiede che la conservazione sia impostata per 90 giorni in più rispetto all'impostazione «transizione al freddo dopo giorni». Non è possibile modificare l'impostazione "giorni per la transizione a storage dei dati inattivi" dopo che è stata eseguita la transizione di un backup allo storage dei dati inattivi.
- Alcuni servizi supportano i backup incrementali. Per i backup incrementali, è necessario disporre di almeno un backup completo a caldo. AWS Backup consiglia di configurare le impostazioni del ciclo di vita in modo da non spostare il backup in cold storage fino a dopo almeno 8 giorni. Se il backup completo viene trasferito alla conservazione a freddo troppo presto (ad esempio, una transizione alla conservazione a freddo dopo 1 giorno), AWS Backup verrà creato un altro backup completo a caldo.
- Per i tipi di risorse che supportano i backup incrementali, AWS Backup trasferisce i dati dalla memorizzazione a caldo a quella a freddo se i dati trasferiti non sono più referenziati dai backup a caldo. I dati dei backup mantenuti nell'archiviazione a freddo a cui fanno riferimento solo altri backup dell'archiviazione a freddo vengono fatturati ai prezzi del livello di archiviazione a freddo. Gli altri backup continuano a utilizzare i prezzi del livello di archiviazione a caldo.

Vault di backup

Un vault di backup è un container che permette di organizzare i backup. I backup creati da una regola di backup sono organizzati nel vault di backup specificato nella regola di backup. È possibile utilizzare gli archivi di backup per impostare la chiave di crittografia AWS Key Management Service (AWS KMS) utilizzata per crittografare i backup nell'archivio di backup e per controllare l'accesso ai backup nell'archivio di backup. È anche possibile aggiungere tag ai vault di backup per facilitarne l'organizzazione. Se non si desidera utilizzare il vault di default, è possibile crearne uno personalizzato. Per step-by-step istruzioni sulla creazione di un archivio di backup, vedere. Fase 3: creare un vault di backup

Copia nelle regioni

Come parte del piano di backup, è possibile creare una copia di un backup in un'altra Regione AWS. Per ulteriori informazioni sulle copie di backup, consulta Creazione di copie di backup tra Regioni AWS.

Quando si definisce una copia di un backup, è possibile configurare le seguenti opzioni:

Regione di destinazione

La regione di destinazione della copia del backup.

(Impostazioni avanzate) Vault di backup

Il vault di backup di destinazione della copia.

(Impostazioni avanzate) Ruolo IAM

Il ruolo IAM AWS Backup utilizzato durante la creazione della copia. Il ruolo deve inoltre essere AWS Backup elencato come entità attendibile, che consente AWS Backup di assumere il ruolo. Se scegli Predefinito e il ruolo AWS Backup predefinito non è presente nel tuo account, viene creato un ruolo con le autorizzazioni corrette.

(Impostazioni avanzate) Ciclo di vita

Specifica quando trasferire la copia del backup allo storage dei dati inattivi e quando far scadere (eliminare) la copia. I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Non è possibile modificare questo valore dopo il trasferimento di una copia nello storage dei dati inattivi.

Scadenza specifica il numero di giorni dopo la creazione prima che la copia venga eliminata. Questo valore deve essere maggiore di 90 giorni rispetto al valore di Transizione allo storage dei dati inattivi.

Tag aggiunti ai punti di ripristino

In questo campo sono elencati i tag che vengono aggiunti automaticamente ai backup quando vengono creati.

Tag aggiunti ai piani i backup

Questi tag sono associati al piano di backup stesso e permettono di organizzarlo e monitorarlo.

Impostazioni di backup e avanzate

Consente backup coerenti dell'applicazione per applicazioni di terze parti eseguite su istanze Amazon EC2. Attualmente AWS Backup supporta i backup Windows VSS. AWS Backup esclude tipi specifici di istanze Amazon EC2 dai backup Windows VSS. Per ulteriori informazioni, consulta Creazione di backup Windows VSS.

AWS CloudFormation modelli per piani di backup

Forniamo due AWS CloudFormation modelli di esempio come riferimento. Il primo modello crea un semplice piano di backup. Il secondo modello abilita i backup VSS in un piano di backup.

> **Note**
>
> Se si utilizza il ruolo di servizio predefinito, sostituire il *ruolo di servizio* con `AWSBackupServiceRolePolicyForBackup`.

```
Description: backup plan template to back up all resources daily at 5am UTC, and tag
 all recovery points with backup:daily.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
```

```
        BackupPlanRule:
          - RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"
    DependsOn: BackupVaultWithDailyBackups

  DDBTableWithDailyBackupTag:
    Type: "AWS::DynamoDB::Table"
    Properties:
      TableName: "TestTable"
      AttributeDefinitions:
        - AttributeName: "Album"
          AttributeType: "S"
      KeySchema:
        - AttributeName: "Album"
          KeyType: "HASH"
      ProvisionedThroughput:
        ReadCapacityUnits: "5"
        WriteCapacityUnits: "5"
      Tags:
        - Key: "backup"
          Value: "daily"

  BackupRole:
    Type: "AWS::IAM::Role"
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "backup.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/service-role/service-role"

  TagBasedBackupSelection:
    Type: "AWS::Backup::BackupSelection"
    Properties:
      BackupSelection:
        SelectionName: "TagBasedBackupSelection"
        IamRoleArn: !GetAtt BackupRole.Arn
```

```
        ListOfTags:
          - ConditionType: "STRINGEQUALS"
            ConditionKey: "backup"
            ConditionValue: "daily"
      BackupPlanId: !Ref BackupPlanWithDailyBackups
    DependsOn: BackupPlanWithDailyBackups
```

```
Description: backup plan template to enable Windows VSS and add backup rule to take
 backup of assigned resources daily at 5am UTC.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        AdvancedBackupSettings:
          - ResourceType: EC2
            BackupOptions:
              WindowsVSS: enabled
        BackupPlanRule:
```

```
        - RuleName: "RuleForDailyBackups"
          TargetBackupVault: !Ref BackupVaultWithDailyBackups
          ScheduleExpression: "cron(0 5 ? * * *)"

    DependsOn: BackupVaultWithDailyBackups
```

Assegnazione di risorse a un piano di backup

L'assegnazione delle risorse specifica quali risorse AWS Backup verranno protette utilizzando il piano di backup. AWS Backup offre sia semplici impostazioni predefinite che controlli dettagliati per assegnare risorse al piano di backup. Ogni volta che viene eseguito il piano di backup, analizza tutte le risorse che soddisfano i Account AWS criteri di assegnazione delle risorse. Questo livello di automazione consente di definire il piano di backup e l'assegnazione delle risorse esattamente una volta. AWS Backup semplifica il lavoro di ricerca e backup di nuove risorse che si adattino all'assegnazione di risorse definita in precedenza.

Puoi assegnare qualsiasi tipo di risorsa AWS Backup supportata che hai scelto di gestire. AWS Backup Per istruzioni su come attivare altri tipi di risorse AWS Backup supportati, vedi Guida introduttiva 1: Service Opt-in.

La AWS Backup console offre due modi per includere i tipi di risorse in un piano di backup: assegnare esplicitamente il tipo di risorsa in un piano di backup o includere tutte le risorse. Consulta i punti seguenti per comprendere come funzionano queste selezioni con adesioni al servizio.

- Se le assegnazioni delle risorse si basano solo sui tag, vengono applicate le impostazioni opt-in del servizio.
- Se un tipo di risorsa viene assegnato in modo esplicito a un piano di backup, verrà incluso nel backup anche se l'opt-in non è abilitato per quel particolare servizio. Questo non si applica ad Aurora, Neptune e Amazon DocumentDB. Affinché questi servizi siano inclusi, l'opt-in deve essere abilitato.
- Se in un'assegnazione di risorse sono specificati sia il tipo di risorsa che i tag, i tipi di risorse specificati vengono filtrati per primi, quindi i tag filtrano ulteriormente tali risorse.

  Le impostazioni relative all'attivazione del servizio vengono ignorate per la maggior parte dei tipi di risorse. Tuttavia Aurora, Neptune e Amazon DocumentDB richiedono l'attivazione del servizio.
- Quando un account utilizza AWS Backup (crea un archivio di backup o un piano di backup) in una regione, l'account viene automaticamente attivato per tutti i tipi di risorse supportati dalla AWS

Backup regione in quel momento. I servizi supportati aggiunti a quella regione in un secondo momento non verranno inclusi automaticamente in un piano di backup. Puoi scegliere di attivare questi tipi di risorse una volta che saranno supportati.

- Per Amazon FSx for NetApp ONTAP, quando utilizzi la selezione delle risorse basata su tag, applica i tag ai singoli volumi anziché all'intero file system.

L'assegnazione delle risorse può includere (o escludere) tipi di risorse e risorse.

- Un tipo di risorsa include ogni istanza o risorsa di un AWS servizio AWS Backup supportato o di un'applicazione di terze parti. Ad esempio, il tipo di risorsa DynamoDB fa riferimento a tutte le tabelle DynamoDB.
- Una risorsa è una singola istanza di un tipo di risorsa, ad esempio una delle proprie tabelle DynamoDB. È possibile specificare una risorsa utilizzando il relativo ID risorsa univoco.

È possibile rifinire ulteriormente l'assegnazione delle risorse utilizzando tag e operatori condizionali.

Argomenti

Assegnazione delle risorse tramite la console

Per accedere alla pagina Assegna risorse:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Scegli Piani di backup.
3. Scegli Crea piano di backup.
4. Seleziona un qualsiasi modello nell'elenco a discesa Scegli modello, quindi scegli Crea piano.
5. Digita il Nome del piano di backup.
6. Seleziona Crea piano.
7. Scegli Assegna risorse.

Per iniziare l'assegnazione delle risorse, nella sezione Generale:

1. Digita un Nome assegnazione di risorsa.
2. Scegli il Ruolo predefinito o Scegli un ruolo IAM.

> **Note**
>
> Se scegli un ruolo IAM, verifica che disponga delle autorizzazioni per eseguire il backup di tutte le risorse che stanno per essere assegnate. Se viene rilevata una risorsa a cui non è autorizzato l'accesso, il piano di backup ha esito negativo.

Per assegnare le risorse, nella sezione Assegna risorse, scegli una delle due opzioni in Definisci selezione delle risorse:

- Includi tutti i tipi di risorse. Questa opzione configura il piano di backup per proteggere tutte le risorse AWS Backup supportate attuali e future assegnate al piano di backup. Utilizzare questa opzione per proteggere rapidamente e facilmente il patrimonio di dati.

  Quando si sceglie questa opzione, è possibile scegliere facoltativamente come passaggio successivo Migliora la selezione utilizzando i tag.
- Includi tipi di risorse specifici. Quando scegli questa opzione, devi operare nella sezione Selezionare tipi di risorse specifici con i seguenti passaggi:

  1. Utilizzando il menu a discesa Seleziona tipi di risorse, assegna uno o più tipi di risorse.

     > **Important**
     >
     > RDS, Aurora, Neptune e DocumentDB condividono lo stesso nome della risorsa Amazon (ARN). Se si acconsente alla gestione di uno di questi tipi di risorse con AWS Backup , si acconsente alla gestione di tutte le relative risorse durante l'assegnazione a un piano di backup. Per affinare la selezione, utilizza tag e operatori condizionali.

     Al termine, AWS Backup presenta l'elenco dei tipi di risorse selezionati e la relativa impostazione predefinita, che prevede la protezione di tutte le risorse per ogni tipo di risorsa selezionato.
  2. Facoltativamente, se desideri escludere risorse specifiche da un tipo di risorsa selezionato:

     1. Utilizza il menu a discesa Scegli le risorse e deseleziona l'opzione predefinita.

2. Seleziona le risorse specifiche da assegnare al tuo piano di backup.

3. Facoltativamente, puoi Escludi ID di risorse specifici dai tipi di risorse selezionati. Utilizza questa opzione se desideri escludere una o poche risorse tra le tante, poiché questa operazione potrebbe essere più rapida rispetto alla selezione di molte risorse nel passaggio precedente. È necessario includere un tipo di risorsa prima di poter escludere risorse da quel tipo di risorsa. Escludi un ID di risorsa utilizzando i seguenti passaggi:

   1. In Escludi ID di risorse specifici dai tipi di risorse selezionati, scegli uno o più tipi di risorse che hai incluso utilizzando Seleziona tipi di risorse.
   2. Per ogni tipo di risorsa, utilizza il menu Scegli risorse per selezionare una o più risorse da escludere.

Oltre alle scelte precedenti, puoi effettuare selezioni ancora più granulari utilizzando la funzionalità opzionale Migliora la selezione utilizzando i tag. Questa funzionalità consente di affinare la selezione corrente al fine di includere un sottoinsieme delle risorse che utilizzano i tag.

I tag sono coppie chiave-valore che puoi assegnare a risorse specifiche per aiutarti a identificare, organizzare e filtrare le risorse. I tag rispettano la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Assegnazione di tag alle risorse AWS nella Documentazione generale di riferimento di AWS .

Quando affini la selezione utilizzando due o più tag, l'effetto è una condizione AND. Ad esempio, se affini la selezione utilizzando due tag `env: prod` e `role: application`, assegni al piano di backup solo risorse che presentano ENTRAMBI i tag.

Per affinare la selezione utilizzando i tag:

1. In Migliora la selezione utilizzando i tag, scegli una Chiave dall'elenco a discesa.
2. Scegli una Condizione per il valore dall'elenco a discesa.
   - Il campo Valore fa riferimento al valore di input successivo, il valore della coppia chiave-valore.
   - Condizione può essere di tipo `Equals`, `Contains`, `Begins with` o `Ends with` oppure di uno dei tipi inversi: `Does not equal`, `Does not contain`, `Does not begin with` o `Does not end with`.
3. Scegli un Valore dall'elenco a discesa.
4. Per rifinire ulteriormente il risultato utilizzando un altro tag, scegli Aggiungi tag.

Assegnazione di risorse a livello di codice

È possibile definire un'assegnazione di risorse in un documento JSON. Questo esempio di assegnazione di risorse assegna tutte le istanze Amazon EC2 al piano di backup *BACKUP-PLAN-ID*:

```
{
  "BackupPlanId":"BACKUP-PLAN-ID",
  "BackupSelection":{
    "SelectionName":"resources-list-selection",
    "IamRoleArn":"arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources":[
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
}
```

Supponendo che questo JSON sia archiviato come `backup-selection.json`, puoi assegnare queste risorse al tuo piano di backup utilizzando il seguente comando CLI:

```
aws backup create-backup-selection --cli-input-json file://PATH-TO-FILE/backup-selection.json
```

Di seguito sono riportati alcuni esempi di assegnazione delle risorse, insieme al documento JSON corrispondente. Per facilitare la lettura di questa tabella, negli esempi vengono omessi i campi `"BackupPlanId"`, `"SelectionName"` e `"IamRoleArn"`. Il carattere jolly `*` rappresenta zero o più caratteri diversi dagli spazi bianchi.

Example Esempio: seleziona tutte le risorse nel mio account

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ]
  }
}
```

Example Esempio: seleziona tutte le risorse nel mio account, ma escludi i volumi EBS

```
{
  "BackupSelection":{
```

```
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ]
  }
}
```

Example Esempio: seleziona tutte le risorse contrassegnate con"backup":"true", ma escludi i volumi EBS

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example Esempio: seleziona tutti i volumi EBS e le istanze DB RDS contrassegnati con entrambi e "backup":"true""stage":"prod"

L'aritmetica booleana è simile a quella delle policy IAM, in cui quelle "Resources" sono combinate utilizzando un OR booleano mentre quelle in `"Conditions"` sono combinate utilizzando un AND booleano.

L'espressione `"Resources"` `"arn:aws:rds:*:*:db:*"` permette la selezione delle sole istanze DB RDS perché non esistono risorse Aurora, Neptune o DocumentDB corrispondenti.

```
{
```

```
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        },
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"prod"
        }
      ]
    }
  }
}
```

Example Esempio: seleziona tutti i volumi EBS e le istanze RDS contrassegnati con ma non "backup":"true""stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
```

```
  }
}
```

Example Esempio: seleziona tutte le risorse contrassegnate con "key1" e un valore che inizia con "include" ma non con "key2" e un valore che contiene la parola "exclude"

È possibile utilizzare il carattere jolly all'inizio, alla fine e al centro di una stringa. Nota l'uso del carattere jolly (*) in `include*` e `*exclude*` nell'esempio precedente. È inoltre possibile utilizzare il carattere jolly al centro di una stringa, come mostrato nell'esempio precedente, `arn:aws:rds:*:*:db:*`.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/key1",
          "ConditionValue":"include*"
        }
      ],
      "StringNotLike":[
        {
          "ConditionKey":"aws:ResourceTag/key2",
          "ConditionValue":"*exclude*"
        }
      ]
    }
  }
}
```

Example Esempio: selezionare tutte le risorse contrassegnate con "backup":"true" tranne i file system FSx e le risorse RDS, Aurora, Neptune e DocumentDB

Gli elementi in `NotResources` vengono combinati utilizzando l'OR booleano.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
```

```
    ],
    "NotResources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example Esempio: seleziona tutte le risorse contrassegnate con un tag e un valore qualsiasi "backup"

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"*"
        }
      ]
    }
  }
}
```

Example Esempio: selezionare tutti i file system FSx, il cluster Aurora e tutte le risorse contrassegnate con "my-aurora-cluster""backup":"true", ad eccezione delle risorse contrassegnate con "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
```

```
      "arn:aws:fsx:*",
      "arn:aws:rds:*:*:cluster:my-aurora-cluster"
    ],
    "ListOfTags":[
      {
        "ConditionType":"StringEquals",
        "ConditionKey":"backup",
        "ConditionValue":"true"
      }
    ],
    "Conditions":{
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example Esempio: seleziona tutte le risorse contrassegnate con tag **`"backup":"true"`** ad eccezione dei volumi EBS contrassegnati con **`"stage":"test"`**

Per selezionare questo gruppo di risorse, utilizza due comandi CLI per creare due selezioni. La prima selezione si applica a tutte le risorse a eccezione dei volumi EBS. La seconda selezione si applica ai volumi EBS.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
```

```
    }
  }
}
```

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Assegnazione di risorse utilizzando AWS CloudFormation

Questo end-to-end AWS CloudFormation modello crea un'assegnazione di risorse, un piano di backup e un archivio di backup di destinazione:

- Un archivio di backup denominato. *`CloudFormationTestBackupVault`*
- Un piano di backup denominato *`CloudFormationTestBackupPlan`*. Questo piano contiene due regole di backup, entrambe le quali eseguono i backup ogni giorno alle 12:00 UTC e li conservano per 210 giorni.
- Una selezione di risorse denominata *`BackupSelectionName`*.
- • L'assegnazione delle risorse esegue il backup delle seguenti risorse:
  - Qualsiasi risorsa contrassegnata con la coppia chiave-valore `backupplan:dsi-sandbox-daily`.
  - Qualsiasi risorsa contrassegnata con il valore `prod` o valori che iniziano con `prod/`.

- L'assegnazione delle risorse non esegue il backup delle seguenti risorse:
  - Qualsiasi cluster RDS, Aurora, Neptune o DocumentDB.
  - Qualsiasi risorsa contrassegnata con il valore `test` o valori che iniziano con `test/`.

```
Description: "Template that creates Backup Selection and its dependencies"
Parameters:
  BackupVaultName:
    Type: String
    Default: "CloudFormationTestBackupVault"
  BackupPlanName:
    Type: String
    Default: "CloudFormationTestBackupPlan"
  BackupSelectionName:
    Type: String
    Default: "CloudFormationTestBackupSelection"
  BackupPlanTagValue:
    Type: String
    Default: "test-value-1"
  RuleName1:
    Type: String
    Default: "TestRule1"
  RuleName2:
    Type: String
    Default: "TestRule2"
  ScheduleExpression:
    Type: String
    Default: "cron(0 12 * * ? *)"
  StartWindowMinutes:
    Type: Number
    Default: 60
  CompletionWindowMinutes:
    Type: Number
    Default: 120
  RecoveryPointTagValue:
    Type: String
    Default: "test-recovery-point-value"
  MoveToColdStorageAfterDays:
    Type: Number
    Default: 120
  DeleteAfterDays:
    Type: Number
```

```
    Default: 210
Resources:
  CloudFormationTestBackupVault:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: !Ref BackupPlanName
        BackupPlanRule:
          - RuleName: !Ref RuleName1
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
          - RuleName: !Ref RuleName2
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
      BackupPlanTags:
        test-key-1: !Ref BackupPlanTagValue
    DependsOn: CloudFormationTestBackupVault

  TestRole:
    Type: "AWS::IAM::Role"
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
```

```
              Service:
                - "backup.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-
role/AWSBackupServiceRolePolicyForBackup"
  BasicBackupSelection:
    Type: 'AWS::Backup::BackupSelection'
    Properties:
      BackupPlanId: !Ref BasicBackupPlan
      BackupSelection:
        SelectionName: !Ref BackupSelectionName
        IamRoleArn: !GetAtt TestRole.Arn
        ListOfTags:
          - ConditionType: STRINGEQUALS
            ConditionKey: backupplan
            ConditionValue: dsi-sandbox-daily
        NotResources:
          - 'arn:aws:rds:*:*:cluster:*'
        Conditions:
          StringEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod
          StringNotEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test
          StringLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod/*
          StringNotLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test/*
```

Quote relative all'assegnazione di risorse

A una singola assegnazione di risorse si applicano le seguenti quote:

- 500 Amazon Resource Name (ARN) senza caratteri jolly
- 30 ARN con espressioni jolly
- 30 condizioni
- 30 tag per assegnazione di risorse (e un numero illimitato di risorse per tag)

Eliminazione di un piano di backup

È possibile eliminare un piano di backup solo dopo che sono state eliminate tutte le selezioni di risorse associate. Queste selezioni sono note anche come assegnazioni di risorse. Se queste non sono state eliminate prima dell'eliminazione del piano di backup, la console visualizzerà l'errore: «Le selezioni del piano di backup correlate devono essere eliminate prima dell'eliminazione del piano di backup». Usa la console o usa `DeleteBackupSelection`.

L'eliminazione di un piano di backup elimina la versione corrente del piano. La versione corrente e quelle precedenti, se presenti, sono ancora esistenti ma non sono più elencate nella console in Piani di backup.

> **Note**
>
> Quando si elimina un piano di backup, i backup esistenti non vengono eliminati. Per rimuovere i backup esistenti, eliminarli dal vault di backup seguendo i passaggi indicati in Eliminazione dei backup.

Per eliminare un piano di backup utilizzando la AWS Backup console

1. Accedere a e aprire la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup. AWS Management Console
2. Nel riquadro di navigazione a sinistra scegli Piani di backup.
3. Scegli il piano di backup nell'elenco.
4. Seleziona le assegnazioni di risorse associate al piano di backup.
5. Scegli Elimina.

Aggiornamento di un piano di backup

Dopo aver creato un piano di backup, è possibile modificarlo. È possibile, ad esempio, aggiungere tag oppure aggiungere, modificare o eliminare regole di backup. Tutte le modifiche apportate a un piano di backup non hanno effetti sui backup esistenti creati dal piano di backup. Le modifiche vengono applicate solo ai backup creati a partire da quel momento.

Ad esempio, quando si aggiorna il periodo di retention in una regola di backup, il periodo di retention dei backup creati prima dell'aggiornamento rimane invariato. I backup creati successivamente in base a questa regola riflettono il periodo di retention aggiornato.

Non è possibile modificare il nome di un piano dopo averlo creato.

Per modificare un piano di backup utilizzando la AWS Backup console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup plans (Piani di backup).
3. Nel secondo riquadro, Piani di Backup, vengono visualizzati i backplan esistenti. Seleziona il link sottolineato nella colonna Nome del piano di backup per visualizzare i dettagli del piano di backup scelto.
4. È possibile modificare una regola di backup, visualizzare le assegnazioni delle risorse, visualizzare i processi di backup, gestire i tag o modificare le impostazioni di Windows VSS.
5. Per aggiornare una regola di backup, selezionare il nome della regola di backup.

   Seleziona Gestisci tag per aggiungere o eliminare tag.

   Seleziona Modifica accanto a Impostazioni di backup avanzate per attivare o disattivare Windows VSS.
6. Modifica le impostazioni che preferisci, quindi seleziona Salva.

Vault di backup

> **Note**
>
> A partire dal 9 agosto 2023, offrirà AWS Backup un'anteprima per l'utilizzo di un vault logicamente isolato.
> `<Per iscriverti a questa anteprima, invia una richiesta via e-mail a @amazon`
> Le funzionalità possono cambiare o essere modificate durante e dopo il periodo di anteprima. Quando il servizio diventerà Generally Available (GA), i dati e le configurazioni forniti durante l'anteprima non saranno più disponibili. Con l'anteprima, AWS consiglia di utilizzare dati di test anziché dati di produzione.

In AWS Backup, un archivio di backup è un contenitore che archivia e organizza i backup.

Quando si crea un archivio di backup, è necessario specificare la chiave di crittografia AWS Key Management Service (AWS KMS) che crittografa alcuni dei backup inseriti in questo archivio. La crittografia per altri backup è gestita dai relativi servizi di origine. AWS Per ulteriori informazioni sulla crittografia dei backup, consulta la tabella Crittografia per i backup in AWS.

Il tuo account disporrà sempre di un archivio di backup predefinito. Se hai bisogno di chiavi crittografiche o policy di accesso diverse per gruppi di backup diversi, puoi creare più vault di backup.

Questa sezione fornisce una panoramica su come gestire i vault di backup in AWS Backup.

Argomenti

Vault logicamente isolati (anteprima)

> **Note**
>
> A partire dal 9 agosto 2023, offrirà AWS Backup un'anteprima per l'utilizzo di un vault logicamente isolato.
> `<Per iscriverti a questa anteprima, invia una richiesta via e-mail a @amazon`
> Le funzionalità possono cambiare o essere modificate durante e dopo il periodo di anteprima. Quando il servizio diventerà Generally Available (GA), i dati e le configurazioni forniti durante l'anteprima non saranno più disponibili. Con l'anteprima, AWS consiglia di utilizzare dati di test anziché dati di produzione.

Panoramica

AWS Backup sta visualizzando in anteprima un tipo di archivio secondario in grado di archiviare copie dei backup in altri vault. Un vault logicamente isolato è un vault specializzato che offre funzionalità di sicurezza avanzate oltre a quelle di un vault di backup, nonché la possibilità di condividere l'accesso al vault con altri account e organizzazioni in modo che i tempi di ripristino (RTO) possano essere più rapidi e flessibili in caso di incidente che richieda il ripristino rapido delle risorse.

Le casseforti con sistema logico sono dotate di funzionalità di protezione aggiuntive: ognuna di queste casseforti è crittografata con una chiave AWS proprietaria e ogni vault ha un blocco del vault impostato in modalità di conformità.

È possibile scegliere di condividere un vault logicamente isolato tra organizzazioni e account in modo che i backup archiviati al suo interno possano essere ripristinati da un account con cui il vault è condiviso, se necessario.

Durante il periodo di anteprima non sono previsti costi aggiuntivi per l'archiviazione in vault logicamente isolato. Anche se le copie dei backup memorizzati nei vault logicamente isolati non vengono addebitate, i backup nei vault di backup standard e nelle copie interregionali verranno comunque addebitati secondo le tariffe pubblicate (vedi i prezzi).

Caso d'uso

Un vault logicamente isolato è un vault secondario che fa parte di una strategia di protezione dei dati. Questo vault può aiutare a migliorare la conservazione e il ripristino organizzativi quando si desidera un vault per i backup che

- Sia impostato automaticamente con un blocco del vault in modalità Compliance
- Contenga backup che possono essere condivisi e ripristinati da un account diverso da quello che ha creato il backup
- Viene crittografato con una chiave proprietaria AWS

Le risorse supportate in un vault logicamente isolato includono

- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon EFS
- Amazon RDS

Questa anteprima dei vault logicamente isolati è disponibile solo nella Regione Stati Uniti orientali (Virginia settentrionale). Poiché questa funzionalità è attualmente disponibile solo in una regione, la copia tra più regioni non è supportata durante questo periodo di anteprima.

Confronto con un vault di backup standard

Un deposito di backup è il tipo di deposito principale e standard utilizzato in. AWS Backup Ogni backup viene archiviato in un vault di backup al momento della creazione del backup. È possibile assegnare policy basate sulle risorse per gestire i backup archiviati nel vault, ad esempio per definire il ciclo di vita dei backup archiviati all'interno del vault.

Un vault logicamente isolato è un vault specializzato con sicurezza aggiuntiva e condivisione flessibile per tempi di ripristino (RTO) più rapidi. Questo vault archivia le copie dei backup inizialmente creati e archiviati in un vault di backup standard.

I vault di backup possono essere crittografati con una chiave, un meccanismo di sicurezza che limita l'accesso ai soli utenti previsti. Queste chiavi possono essere gestite o AWS gestite dal cliente. Inoltre, un vault di backup può essere ulteriormente protetto da un vault lock. I vault logicamente isolati sono dotati di un blocco del vault in modalità Compliance.

Se la AWS KMS chiave non è stata modificata manualmente o impostata come chiave gestita dal cliente (CMK) al momento della creazione della risorsa iniziale, un backup non può essere copiato in un archivio logico.

Funzionalità	Vault di backup	Vault logicamente isolato (anteprima)
Creazione di un backup	Quando viene creato un backup, questo viene archiviato come punto di ripristino	Al momento della creazione i backup non vengono archiviati in questo vault
Archiviazione di un backup	Può archiviare i backup iniziali delle risorse e le copie dei backup	Può archiviare copie di backup da altri vault
Sicurezza	Facoltativamente può essere crittografato con una chiave (gestita o gestita dal cliente) AWS Opzionalmente può essere bloccato con un blocco del vault	È crittografato con una chiave AWS proprietaria È sempre bloccato con un blocco del vault in modalità Compliance
Condivisibilità	L'accesso può essere gestito tramite policy e AWS Organizations Non compatibile con AWS Resource Access Manager	Opzionalmente può essere condiviso tra più account utilizzando AWS RAM
Ripristino	I backup possono essere ripristinati dallo stesso account proprietario del vault	I backup possono essere ripristinati da un account diverso da quello proprietario del backup se il vault è condiviso con tale account separato
Regionalità	Disponibile in tutte le regioni in cui AWS Backup opera	Disponibile nella Regione Stati Uniti orientali (Virginia settentrionale) durante la fase di anteprima

Funzionalità	Vault di backup	Vault logicamente isolato (anteprima)
Risorse	Può archiviare backup che contengono tutte le risorse AWS Backup supportate	Può archiviare backup che contengono dati di Amazon EC2, Amazon EBS, Amazon EFS, Amazon S3 o Amazon RDS

Creazione di un vault logicamente isolato dalla console

> **Important**
>
> Una volta creato il vault, il nome, il tipo e i periodi di conservazione minimo e massimo del vault non possono essere modificati. Inoltre, il vault lock non può essere rimosso.
> Quando il servizio diventa Generalmente Disponibile, i dati e le configurazioni forniti durante l'anteprima non saranno più disponibili. AWS consiglia di utilizzare i dati di test anziché i dati di produzione con l'anteprima.

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione seleziona Vault.
3. Verranno visualizzati entrambi i tipi di vault. Seleziona Crea nuovo vault.
4. Immettere un nome per il vault di backup. È possibile denominare il vault in modo che rifletta ciò che verrà archiviato o per rendere più facile la ricerca dei backup. Ad esempio, si potrebbe assegnare il nome `FinancialBackups`.
5. Seleziona il pulsante di opzione per creare un Crea un vault con isolamento logico air gap.
6. Imposta il Periodo di conservazione minimo.

   Questo valore (in giorni, mesi o anni) è il periodo di tempo minimo per cui un backup deve essere conservato in questo vault. I backup con periodi di conservazione inferiori a questo valore non possono essere copiati in questo vault.
7. Imposta il Periodo di conservazione massimo.

Questo valore (in giorni, mesi o anni) è il periodo di tempo massimo per cui un backup deve essere conservato in questo vault. I backup con periodi di conservazione superiori a questo valore non possono essere copiati in questo vault.

8. (Facoltativo) Aggiungi tag che ti aiuteranno a trovare e identificare il tuo vault logicamente isolato. Ad esempio, si potrebbe aggiungere un tag `BackupType:Financial`.
9. Seleziona Crea vault.
10. Verifica le impostazioni. Se tutte le impostazioni risultano valorizzate come previsto, seleziona Crea un vault con isolamento logico air gap.
11. La console ti porterà alla pagina dei dettagli del nuovo vault. Verifica che i dettagli del vault siano quelli previsti.

Visualizza i dettagli del vault logicamente isolato nella console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, seleziona Vault.
3. Sotto le descrizioni dei vault sono visualizzati due elenchi, Vault di proprietà di questo account e Vault condivisi con questo account. Seleziona la scheda desiderata per visualizzare i vault.
4. In Nome vault, fai clic sul nome del vault per aprire la pagina dei dettagli. Puoi visualizzare il riepilogo, i punti di ripristino, le risorse protette, la condivisione dell'account, la policy di accesso e i dettagli dei tag.

Copia da un vault di backup standard a un vault logicamente isolato nella console

I vault logicamente isolati possono essere solo la destinazione di un processo di copia in un piano di backup o una destinazione per un processo di copia su richiesta.

Per avviare un processo di copia, è necessario disporre di

- Un vault di backup
- Un vault logicamente isolato
- Un backup contenente dati di Amazon EC2, Amazon EBS, Amazon RDS, Amazon S3 o Amazon EFS
- L'autorizzazione `kms:CreateGrant` per il ruolo utilizzato per creare la copia.

- Nessun backup crittografato con una chiave AWS gestita come parte del processo di copia nel vault con sistema logico

Dopo aver confermato quanto sopra,

1. Apri la console all'indirizzo https://console.aws.amazon.com/backup. AWS Backup
2. Nel riquadro di navigazione a sinistra, seleziona Vault.
3. Nella pagina dei dettagli del vault, vengono visualizzati tutti i punti di ripristino all'interno del vault. Metti un segno di spunta accanto al punto di ripristino che desideri copiare.
4. Scegli Operazioni e seleziona Copia dal menu a discesa.
5. Nella schermata successiva, inserisci i dettagli della destinazione.
    a. La Regione deve essere impostata su Stati Uniti orientali (Virginia settentrionale)
    b. Il menu a discesa associato al vault di backup di destinazione mostra i vault di destinazione idonei. Selezionane uno con il tipo `logically air-gapped vault`
6. Seleziona Copia una volta che tutti i dettagli sono impostati in base alle tue preferenze.

Nella pagina Processi della console, puoi selezionare i processi Copia per visualizzare i processi di copia correnti.

Per ulteriori informazioni, consulta Copia di un backup, Backup tra regioni e Backup tra account.

Condivisione di un vault logicamente isolato dalla console

> **Note**
>
> Solo gli account con determinati privilegi IAM possono condividere e gestire la condivisione degli account.

Puoi utilizzarlo AWS RAM per condividere un vault con intercapedine logiche con altri account da te designati. Per condividerlo utilizzando AWS RAM, assicurati di disporre di quanto segue:

- Due o più account a cui è possibile accedere AWS Backup
- Un account che intende eseguire la condivisione e che dispone delle autorizzazioni RAM necessarie. Per l'esecuzione di questa procedura è necessaria l'autorizzazione

`ram:CreateResourceShare`. La policy `AWSResourceAccessManagerFullAccess` contiene le autorizzazioni necessarie.

- Almeno un vault logicamente isolato

Per condividere un vault logicamente isolato,

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, seleziona Vault.
3. Sotto le descrizioni dei vault saranno visualizzati due elenchi, Vault di proprietà di questo account e Vaults condivisi con questo account. Seleziona l'elenco desiderato per visualizzare i vault.
4. In Nome vault, fai clic sul nome del vault logicamente isolato per aprire la pagina dei dettagli.
5. Il riquadro condivisione account mostra con quali account viene condiviso il vault.
6. Per iniziare la condivisione con un altro account o per modificare gli account con cui è già condiviso, seleziona Gestione della condivisione.

AWS RAM la console si apre quando è selezionata l'opzione Gestisci condivisione. Per la procedura di condivisione di una risorsa tramite AWS RAM, vedi Creazione di una condivisione di risorse nella AWS RAM.

Verifica di disporre delle autorizzazioni appropriate. Backup Administrator IAM Policy [AWSBackupFullAccess] e Backup Operator IAM Policy [AWSBackupOperatorAccess] contengono l'autorizzazione richiesta per visualizzare gli account condivisi; tuttavia, il ruolo utilizzato per la condivisione richiede le autorizzazioni di scrittura di Resource Access Manager per condividere l'account dalla RAM, ad `ram:CreateResourceShare` esempio.

L'account che riceve un invito per partecipare alla condivisione dispone di 12 ore per accettarlo. Consulta Accettazione e rifiuto degli inviti alla condivisione di risorse nella Guida per l'utente di AWS RAM.

Se i passaggi di condivisione sono stati completati e accettati, la pagina di riepilogo del vault verrà visualizzata in Condivisione account = "Condiviso - vedere la tabella di condivisione dell'account riportata di seguito".

Ripristino di un vault logicamente isolato dalla console

È possibile ripristinare un backup archiviato in un vault logicamente isolato dall'account proprietario del vault o da qualsiasi account con cui il vault è condiviso.

Per informazioni sul ripristino di punti di ripristino, consulta Ripristino di un backup.

Eliminazione di un vault logicamente isolato dalla console

> **Important**
>
> Quando il servizio diventa Generalmente Disponibile, i dati e le configurazioni forniti durante l'anteprima non saranno più disponibili. AWS consiglia di utilizzare i dati di test anziché i dati di produzione con l'anteprima.

Consulta Eliminare un vault di backup per eliminare un vault. I vault non possono essere eliminati se contengono ancora backup (punti di ripristino). Assicurati che il vault sia privo di backup prima di iniziare un'operazione di eliminazione.

Vault logicamente isolati tramite CLI/API

È possibile utilizzarlo AWS CLI per eseguire in modo programmatico operazioni per casseforti con intercapedine logiche. Ogni CLI è specifica per il AWS servizio da cui proviene. I comandi relativi alla condivisione sono preceduti da `aws ram`, tutti gli altri comandi devono essere preceduti da `aws backup`.

Crea

Il seguente comando CLI di esempio `CreateLogicallyAirGappedBackupVault` può essere modificato per creare un vault di backup logicamente isolato:

```
aws backup create-logically-air-gapped-backup-vault \
--region us-east-1 \
--backup-vault-name sampleName \
--min-retention-days 7 \
--max-retention-days 35 \
--creator-request-id 123456789012-34567-8901 // optional
```

Visualizzazione dei dettagli

Il seguente comando CLI di esempio `DescribeBackupVault` può essere modificato per ottenere dettagli su un vault:

```
aws backup describe-backup-vault \
```

```
--region us-east-1  \
--backup-vault-name testvaultname
```

Condivisione

> **Note**
>
> Solo gli account con autorizzazioni IAM sufficienti possono condividere e gestire la condivisione degli account.

Puoi condividere un vault logicamente isolato tramite AWS Resource Access Manager (RAM), un servizio che aiuta gli utenti a condividere le risorse.

AWS RAM utilizza il comando CLI. `create-resource-share` L'accesso a questo comando è disponibile solo per gli account amministratore con autorizzazioni sufficienti. Consulta Creazione di una condivisione di risorse in AWS RAM per i passaggi della CLI.

I passaggi da 1 a 4 devono essere eseguiti con l'account proprietario del vault logicamente isolato. I passaggi da 5 a 8 devono essere eseguiti con l'account con cui il vault logicamente isolato sarà condiviso.

1. Accedi all'account proprietario OPPURE richiedi che un utente della tua organizzazione che dispone di credenziali sufficienti per accedere all'account di origine completi questi passaggi.
   - Se in precedenza è stata creata una condivisione di risorse e desideri aggiungerne una aggiuntiva, utilizza invece il comando CLI `associate-resource-share` con l'ARN del nuovo vault.
2. Recupera le credenziali di un ruolo con autorizzazioni sufficienti per la condivisione tramite RAM. Inserisci tali credenziali nella CLI.
   - Per l'esecuzione di questa procedura è necessaria l'autorizzazione `ram:CreateResourceShare`. La policy AWSResourceAccessManagerFullAccesscontiene tutte le autorizzazioni relative alla RAM.
3. Usa. create-resource-share
   a. Includi l'ARN del vault logicamente isolato.
   b. Input di esempio:

```
aws ram create-resource-share \
--name MyLogicallyAirGappedVault \
--resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-vault-1
 \
--principals 123456789012 \
--region us-east-1
```

Output di esempio:

```
{
   "resourceShare":{
      "resourceShareArn":"arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
      "name":"MyLogicallyAirGappedVault",
      "owningAccountId":"123456789012",
      "allowExternalPrincipals":true,
      "status":"ACTIVE",
      "creationTime":"2021-09-14T20:42:40.266000-07:00",
      "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
   }
}
```

4. Copia l'ARN della condivisione di risorse nell'output (necessario per i passaggi successivi). Fornisci l'ARN all'operatore dell'account che stai invitando a ricevere la condivisione.
5. Ottieni l'ARN della condivisione di risorse
   a. Se non hai eseguito i passaggi resourceShareArn da 1 a 4, richiedili a chi l'ha fatto.
   b. Esempio: `arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543`
6. Nella CLI, assumi le credenziali dell'account del destinatario.
7. Ricevi un invito alla condivisione delle risorse con `get-resource-share-invitations`. Per ulteriori informazioni, consulta Accettare e rifiutare gli inviti nella Guida per l'utente di AWS RAM .
8. Accetta l'invito nell'account di destinazione (ripristino).
   - Utilizza `accept-resource-share-invitation` (può anche utilizzare `reject-resource-share-invitation`).

Elenco

Il comando CLI `ListBackupVaults` può essere modificato per elencare tutti i vault di proprietà e presenti nell'account:

```
aws backup list-backup-vaults \
--region us-east-1
```

Per elencare solo i vault logicamente isolati, aggiungi il parametro

```
--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

Per elencare i vault condivisi con l'account, usa

```
aws backup list-backup-vaults \
--region us-east-1 \
--by-shared
```

Copia

Un vault logicamente isolato può essere solo la destinazione di un processo di copia di un backup, non la destinazione di un processo di backup iniziale. Utilizza `StartCopyJob` per copiare un backup esistente in un vault logicamente isolato.

Il ruolo utilizzato per creare il processo di copia nel vault logicamente isolato deve contenere l'autorizzazione `kms:CreateGrant`.

Input CLI di esempio:

```
aws backup start-copy-job \
--region us-east-1 \
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567 \
--source-backup-vault-name sourcevaultname \
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-
vault:destinationvaultname \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

Ripristino

Una volta che un backup è stato condiviso da un vault logicamente isolato ed è stato collegato al tuo account, puoi utilizzare `StartRestoreJob` per ripristinare il backup. Input CLI di esempio:

```
aws backup start-restore-job \
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-
point:RecoveryPointID \
--metadata {\"availabilityzone\":\"us-east-1d\"} \
--idempotency-token TokenNumber \
--resource-type ResourceType \
--iam-role arn:aws:iam::number:role/service-role/servicerole \
--region us-east-1
```

Eliminazione

Il seguente comando CLI di esempio `DeleteBackupVault` può essere utilizzato per eliminare un vault. Un vault può essere eliminato solo se non contiene backup al suo interno (punti di ripristino).

```
aws backup delete-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

Altre opzioni programmatiche disponibili includono:

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

Creazione di un vault di backup

È necessario creare almeno un vault prima di creare un piano di backup o avviare un processo di backup.

Quando si utilizza per la prima volta la AWS Backup console in un Regione AWS archivio, la console crea automaticamente un archivio predefinito.

Tuttavia, se si utilizza AWS Backup tramite AWS SDK o AWS CloudFormation, non viene creato un archivio predefinito. AWS CLIÈ necessario creare il proprio vault.

Autorizzazioni richieste

È necessario disporre delle seguenti autorizzazioni per creare un vault di backup utilizzando. AWS Backup

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource":
 "arn:aws:kms:region:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault"
      ],
      "Resource": "arn:aws:backup:region:444455556666:backup-vault:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule"
      ],
      "Resource": "*"
    }
  ]
}
```

Creazione di un vault di backup (console)

Per step-by-step istruzioni sulla creazione di un archivio di backup utilizzando la AWS Backup console, consulta Fase 3: creare un vault di backup la guida introduttiva.

Creazione di un vault di backup (utilizzando il codice)

Il AWS Command Line Interface comando seguente crea un archivio di backup:

```
aws backup create-backup-vault --backup-vault-name test-vault
```

È inoltre possibile specificare le seguenti configurazioni per un vault di backup.

Nome del vault di backup

I nomi dei vault di backup rispettano la distinzione tra lettere maiuscole e minuscole. Devono contenere da 2 a 50 caratteri alfanumerici, trattini o trattini bassi.

AWS KMS chiave di crittografia

La chiave di AWS KMS crittografia protegge i backup in questo archivio di backup. Per impostazione predefinita, AWS Backup crea per l'utente una chiave KMS con l'alias `aws/backup`. Puoi scegliere tale chiave o qualsiasi altra chiave disponibile nel tuo account (le chiavi KMS per più account possono essere utilizzate tramite CLI).

Puoi creare una nuova chiave crittografica seguendo la procedura di Creazione delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service .

Dopo aver creato un archivio di backup e impostato la chiave di AWS KMS crittografia, non è più possibile modificare la chiave per tale archivio di backup.

La chiave di crittografia specificata in un AWS Backup archivio si applica ai backup di determinati tipi di risorse. Per ulteriori informazioni sulla crittografia di backup, consulta Crittografia per i backup in AWS Backup nella sezione relativa alla sicurezza. I backup di tutti gli altri tipi di risorse vengono eseguiti utilizzando la chiave usata per crittografare la risorsa di origine.

Tag del vault di backup

Questi tag sono associati al vault di backup per permettere di organizzarlo e monitorarlo.

Imposta le policy di accesso ai vault di backup

Con AWS Backup, è possibile assegnare politiche agli archivi di backup e alle risorse in essi contenute. L'assegnazione di policy permette di eseguire operazioni come concedere l'accesso agli utenti per creare piani di backup e backup on demand, ma limita la possibilità di eliminare i punti di ripristino dopo la creazione.

Per informazioni sull'utilizzo delle policy per concedere o limitare l'accesso alle risorse, consulta Policy basate sulle identità e policy basate su risorse nella Guida per l'utente di IAM. Puoi controllare l'accesso anche utilizzando i tag.

È possibile utilizzare le politiche di esempio seguenti come guida per limitare l'accesso alle risorse quando si lavora con AWS Backup i vault. A differenza di altre policy basate su IAM, le policy di AWS Backup accesso non supportano una jolly nella chiave. `Action`

Per un elenco di Amazon Resource Name (ARN) che è possibile utilizzare per identificare i punti di ripristino per diversi tipi di risorse, consulta AWS Backup ARN di risorse per gli ARN dei punti di ripristino specifici delle risorse.

Le policy di accesso di Vault controllano solo l'accesso degli utenti alle API. AWS Backup Utilizzando le API di tali servizi è inoltre possibile accedere ad alcuni tipi di backup, ad esempio gli snapshot Amazon Elastic Block Store (Amazon EBS) e Amazon Relational Database Service (Amazon RDS). In IAM è possibile creare policy di accesso separate che controllano l'accesso a queste API per offrire il controllo completo dell'accesso ai backup.

Indipendentemente dalla politica di accesso del AWS Backup vault, l'accesso tra account per qualsiasi azione diversa `backup:CopyIntoBackupVault` verrà rifiutato, ovvero AWS Backup rifiuterà qualsiasi altra richiesta proveniente da un account diverso dall'account della risorsa a cui si fa riferimento.

Argomenti

- Negare l'accesso a un tipo di risorsa in un vault di backup
- Negare l'accesso a un vault di backup
- Negare l'accesso all'eliminazione dei punti di ripristino in un vault di backup

Negare l'accesso a un tipo di risorsa in un vault di backup

Questa policy nega l'accesso alle operazioni API specificate per tutte le snapshot Amazon EBS di un vault di backup.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:UpdateRecoveryPointLifecycle",
                "backup:DescribeRecoveryPoint",
                "backup:DeleteRecoveryPoint",
                "backup:GetRecoveryPointRestoreMetadata",
                "backup:StartRestoreJob"
            ],
            "Resource": ["arn:aws:ec2:Region::snapshot/*"]
        }
    ]
}
```

Negare l'accesso a un vault di backup

Questa policy nega l'accesso alle operazioni API specificate eseguite su un vault di backup.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:DescribeBackupVault",
                "backup:DeleteBackupVault",
                "backup:PutBackupVaultAccessPolicy",
                "backup:DeleteBackupVaultAccessPolicy",
```

```
                "backup:GetBackupVaultAccessPolicy",
                "backup:StartBackupJob",
                "backup:GetBackupVaultNotifications",
                "backup:PutBackupVaultNotifications",
                "backup:DeleteBackupVaultNotifications",
                "backup:ListRecoveryPointsByBackupVault"
            ],
            "Resource": "arn:aws:backup:Region:Account ID:backup-vault:backup vault
 name"
        }
    ]
}
```

Negare l'accesso all'eliminazione dei punti di ripristino in un vault di backup

La possibilità di accedere ai vault e di eliminare i punti di ripristino in essi archiviati è determinata dal tipo di accesso concesso agli utenti.

Segui questi passaggi per creare una policy di accesso basata sulle risorse in un vault di backup che impedisca l'eliminazione di qualsiasi backup al suo interno.

Per creare una policy di accesso basata su risorse per un vault di backup

1. Accedi a e apri AWS Management Console la console all'indirizzo https://console.aws.amazon.com/backup. AWS Backup
2. Nel riquadro di navigazione a sinistra scegliere Vault di backup.
3. Scegliere un vault di backup nell'elenco.
4. Nella sezione Access policy (Policy di accesso) incollare l'esempio JSON riportato di seguito. Questa policy impedisce a chiunque non sia l'entità principale di eliminare un punto di ripristino nel vault di backup di destinazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:userId": [
                        "AAAAAAAAAAAAAAAAAAAAA:",
                        "BBBBBBBBBBBBBBBBBBBBB",
                        "112233445566"
                    ]
                }
            }
        }
    ]
}
```

Per consentire alle identità IAM elencate di utilizzare il proprio ARN, utilizzare a chiave di condizione globale `aws:PrincipalArn` nell'esempio seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "ArnNotEquals": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::112233445566:role/mys3role",
                        "arn:aws:iam::112233445566:user/shaheer",
                        "112233445566"
                    ]
                }
            }
        }
    ]
}
```

Per informazioni su come ottenere un ID univoco per un'entità IAM, consulta Ottenere l'identificatore univoco nella Guida per l'utente di IAM.

Se si desidera limitare l'accesso a tipi di risorsa specifici, invece di `"Resource": "*"`, è possibile includere esplicitamente i tipi di punti di ripristino a cui negare l'accesso. Ad esempio, per gli snapshot di Amazon EBS, modificare il tipo di risorsa nel modo seguente.

```
"Resource": ["arn:aws:ec2::Region::snapshot/*"]
```

5. Scegliere Attach policy (Collega policy).

AWS Backup Vault Lock

> **Note**
>
> AWS Backup Vault Lock è stato valutato da Cohasset Associates per l'uso in ambienti soggetti alle normative SEC 17a-4, CFTC e FINRA. Per ulteriori informazioni su come AWS Backup Vault Lock si rapporta a queste normative, consulta la valutazione della conformità di Cohasset Associates.

AWS Backup Vault Lock è una funzionalità opzionale di un archivio di backup, che può essere utile per fornire maggiore sicurezza e controllo sui vault di backup. Quando un blocco è attivo in modalità Compliance e il periodo di tolleranza è scaduto, la configurazione del vault non può essere modificata o eliminata da un cliente, dal proprietario dell'account/dei dati o da AWS. Ogni vault può disporre di un solo blocco del vault.

AWS Backup assicura che i backup siano disponibili fino alla scadenza dei periodi di conservazione. Se un utente (incluso l'utente root) tenta di eliminare un backup o modificare le proprietà del ciclo di vita in un archivio bloccato, AWS Backup negherà l'operazione.

- Nel caso di vault bloccati in modalità Governance, il blocco può essere rimosso da utenti con autorizzazioni IAM sufficienti.
- Nel caso di vault bloccati in modalità Compliance, questi non possono essere eliminati una volta scaduto il periodo di riflessione ("periodo di tolleranza"). Durante il periodo di tolleranza, è comunque possibile rimuovere il blocco del vault e modificare la configurazione del blocco.

Modalità di blocco del vault

Quando si crea un blocco del vault, è possibile scegliere tra due modalità: modalità Governance o modalità Compliance. La modalità Governance ha lo scopo di consentire la gestione di un vault solo da parte di utenti con privilegi IAM sufficienti. La modalità Governance permette a un'organizzazione di soddisfare i requisiti di governance, garantendo che solo il personale designato possa apportare

modifiche a un vault di backup. La modalità Compliance è destinata ai vault di backup in cui si prevede che il vault (e, per estensione, il suo contenuto) non venga mai eliminato o modificato fino al termine del periodo di conservazione dei dati. Una volta bloccato un vault in modalità Compliance, questo è immutabile, vale a dire che il blocco non può essere rimosso.

Un vault bloccato in modalità Governance può essere gestito o eliminato dagli utenti che dispongono delle autorizzazioni IAM appropriate.

Un blocco del vault in modalità Compliance non può essere modificato o eliminato da nessun utente né da AWS. Un blocco del vault in modalità di Compliance prevede un periodo di tolleranza impostato dall'utente prima che il blocco si attivi e diventi immutabile.

Vantaggi del blocco del vault

AWS Backup Vault Lock offre diversi vantaggi, tra cui:

- Configurazione WORM (write-once, read-many) per tutti i backup archiviati e creati in un vault di backup.
- Un ulteriore livello di difesa che protegge i backup (punti di ripristino) negli vault di backup da eliminazioni involontarie o dolose.
- Applicazione di periodi di conservazione, che impediscono l'eliminazione anticipata da parte degli utenti privilegiati (incluso l'utente Account AWS root) e soddisfano le politiche e le procedure di protezione dei dati dell'organizzazione.

Blocco di un vault di backup tramite la console

Puoi aggiungere un blocco del vault al tuo AWS Backup Vault utilizzando la console di Backup.

Per aggiungere un blocco al vault di backup:

1. Accedi a e apri AWS Management Console la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, individuare Vault di backup. Fare clic sul link annidato all'interno di Vault di backup denominato Lock del vault.
3. Nella sezione Come funzionano i blocchi del vault o Blocco del vault, fare clic su + Crea blocco del vault.
4. Nel riquadro Dettagli del blocco del vault, scegliere a quale vault si intende applicare il blocco.

5. In Modalità di blocco del vault, scegli in quale modalità bloccare il vault. Per ulteriori informazioni sulla scelta delle modalità, consulta la sezione Modalità di blocco del vault all'inizio di questa pagina.
6. Alla voce Periodo di conservazione, scegliere i periodi di conservazione minimo e massimo (l'indicazione dei periodi di conservazione è opzionale). I nuovi processi di backup e copia creati nel vault non andranno a buon fine se non sono conformi ai periodi di conservazione impostati. Questi periodi non si applicheranno ai punti di ripristino già presenti nel vault.
7. Se si sceglie la modalità Compliance, viene visualizzata una sezione denominata Data di inizio del blocco di vault. Se si sceglie la modalità Governance, questa sezione non verrà visualizzata e il presente passaggio può essere ignorato.

   In modalità Compliance, un blocco del vault è associato a un periodo di riflessione dalla creazione del blocco fino a quando il vault e il relativo blocco diventano immutabili e immodificabili. L'utente può scegliere la durata di questo periodo, denominato periodo di tolleranza, anche se deve essere di almeno 3 giorni (72 ore).

   > **Important**
   >
   > Una volta scaduto il periodo di tolleranza, il vault e il relativo blocco diventano immutabili. Non può più essere modificato o eliminato da nessun utente né da AWS.

8. Quando si è soddisfatti delle scelte di configurazione, fare clic su Crea blocco del vault.
9. Per confermare che si desidera creare questo blocco nella modalità scelta, digitare `confirm` nella casella di testo, quindi selezionare la casella per confermare che la configurazione è quella prevista.

Se i passaggi sono stati completati correttamente, nella parte superiore della console verrà visualizzato il banner "Operazione riuscita".

Creazione di un blocco di un vault utilizzando il codice

Per configurare AWS Backup Vault Lock, usa l'API`PutBackupVaultLockConfiguration`. I parametri da includere dipenderanno dalla modalità di blocco del vault desiderata. Se desideri creare un blocco del vault in modalità Governance, non includere `ChangeableForDays`. Se questo parametro è incluso, il blocco del vault verrà creato in modalità Compliance.

Ecco un esempio di creazione di un blocco del vault in modalità Compliance attraverso l'uso della CLI:

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --changeable-for-days 3 \
        --min-retention-days 7 \
        --max-retention-days 30
```

Ecco un esempio di creazione di un blocco del vault in modalità Governance attraverso l'uso della CLI:

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --min-retention-days 7 \
        --max-retention-days 30
```

È possibile configurare quattro opzioni.

1. **`BackupVaultName`**

   Il nome del vault da bloccare.

2. **`ChangeableForDays`** (da includere solo per la modalità Compliance)

   Questo parametro indica di AWS Backup creare il blocco del vault in modalità di conformità. Ometti questo parametro se intendi creare il blocco in modalità Governance.

   Questo valore deve essere espresso in giorni. Deve essere un numero non inferiore a 3 e non superiore a 36.500. In caso contrario, verrà restituito un errore.

   Dalla creazione di questo blocco del vault fino alla scadenza della data specificata, il blocco può essere rimosso dal vault utilizzando `DeleteBackupVaultLockConfiguration`. In alternativa, durante questo periodo, è possibile modificare la configurazione utilizzando `PutBackupVaultLockConfiguration`.

   A partire dalla data specificata determinata da questo parametro, il vault di backup sarà immutabile e non potrà più essere modificato o eliminato.

3. **`MaxRetentionDays`** (opzionale)

Questo è un valore numerico che deve essere espresso in giorni. Questo è il periodo di conservazione massimo durante il quale il vault conserva i punti di ripristino.

Il periodo di conservazione massimo scelto deve essere in linea con le policy dell'organizzazione in tema di conservazione dei dati. Se l'organizzazione richiede che i dati debbano essere conservati per un certo periodo, questo valore può essere impostato su tale periodo (in giorni). Ad esempio, potrebbe essere necessario conservare i dati finanziari o bancari per 7 anni (circa 2.557 giorni, a seconda del numero di anni bisestili).

Se non specificato, AWS Backup Vault Lock non applicherà un periodo di conservazione massimo. Se specificato, i processi di backup e copia in questo vault con periodi di conservazione del ciclo di vita superiori al periodo di conservazione massimo avranno esito negativo. I punti di ripristino già salvati nel vault prima dell'applicazione del Vault Lock non sono interessati. Il periodo di conservazione massimo più lungo che è possibile specificare è di 36500 giorni (circa 100 anni).

4. **`MinRetentionDays`**(opzionale; obbligatorio per) CloudFormation

   Questo è un valore numerico che deve essere espresso in giorni. Questo è il periodo di conservazione minimo durante il quale il vault conserva i punti di ripristino. Questa impostazione deve essere valorizzata in base al periodo di tempo per il quale la tua organizzazione è obbligata a conservare i dati. Ad esempio, se i regolamenti o le leggi richiedono la conservazione dei dati per almeno sette anni, il valore in giorni sarebbe di circa 2.557, a seconda del numero di anni bisestili.

   Se non specificato, AWS Backup Vault Lock non applicherà un periodo di conservazione minimo. Se specificato, i processi di backup e copia in questo vault con periodi di conservazione del ciclo di vita inferiori al periodo di conservazione minimo avranno esito negativo. I punti di ripristino già salvati nel vault prima di AWS Backup Vault Lock non sono interessati. Il periodo di conservazione minimo più breve che è possibile specificare è di 1 giorno.

Controlla la configurazione di un archivio di backup per verificarne AWS Backup la configurazione di Vault Lock

Puoi rivedere i dettagli di AWS Backup Vault Lock su un vault in qualsiasi momento tramite chiamate o API. `DescribeBackupVault` `ListBackupVaults`

Per determinare se hai applicato un blocco del vault a un vault di backup, invoca `DescribeBackupVault` e controlla la proprietà `Locked`. Se`"Locked": true`, come nell'esempio seguente, hai applicato AWS Backup Vault Lock al tuo vault di backup.

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 1,
    "Locked": true,
    "MinRetentionDays": 7,
    "MaxRetentionDays": 30,
    "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

L'output precedente conferma le opzioni seguenti:

1. `Locked`è un valore booleano che indica se è stato applicato AWS Backup Vault Lock a questo archivio di backup. `True`significa che AWS Backup Vault Lock causa il fallimento delle operazioni di eliminazione o aggiornamento dei punti di ripristino archiviati nel vault (indipendentemente dal fatto che sia ancora in corso il periodo di tolleranza).
2. `LockDate` è la data e ora UTC in cui termina il periodo di tolleranza legato al periodi di riflessione. Trascorso questo periodo, non è più possibile eliminare o modificare il blocco di questo vault. Utilizza qualsiasi convertitore orario disponibile pubblicamente per convertire questa stringa nell'ora locale.

Se `"Locked":false`, come nell'esempio seguente, non hai applicato un blocco del vault (o ne è stato eliminato uno precedente applicato).

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 3,
    "Locked": false
}
```

Rimozione del blocco del vault durante il periodo di tolleranza (modalità Compliance)

Per eliminare il blocco del vault durante il periodo di prova (il periodo dopo il blocco del vault ma prima del) utilizzando la console, `LockDate` AWS Backup

1. Accedi a e apri AWS Management Console la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nella barra di navigazione a sinistra sotto Il mio account, fare clic su Vault di backup, quindi su Vault Lock di AWS Backup.
3. Fare clic sul blocco del vault che si desidera rimuovere, quindi fare clic su Gestisci blocco del vault.
4. Fare clic su Elimina vault.
5. Apparirà una finestra di avviso che chiederà di confermare l'intenzione di eliminare il blocco del vault. Digitare `confirm` nella casella di testo, quindi fare clic su conferma.

Dopo che i passaggi sono stati tutti completati correttamente, nella parte superiore della schermata della console verrà visualizzato il banner "Operazione riuscita".

Per eliminare il blocco del vault durante il periodo di tolleranza utilizzando un comando CLI, utilizzare `DeleteBackupVaultLockConfiguration` come in questo esempio di CLI:

```
aws backup delete-backup-vault-lock-configuration \
          --backup-vault-name my_vault_to_lock
```

Account AWS chiusura con un caveau chiuso

Quando chiudi un archivio Account AWS che contiene un archivio di backup AWS e AWS Backup sospendi il tuo account per 90 giorni con i backup intatti. Se non riapri l'account durante questi 90 giorni, AWS elimina il contenuto del tuo archivio di backup, anche se Vault Lock era attivo. AWS Backup

Ulteriori considerazioni sulla sicurezza

AWS Backup Vault Lock aggiunge un ulteriore livello di sicurezza alla difesa approfondita della protezione dei dati. Vault Lock può essere combinato con queste altre funzionalità di sicurezza:

- Crittografia per i punti di ripristino
- AWS Backup politiche di accesso ai vault e ai punti di ripristino, che consentono di concedere o negare le autorizzazioni a livello di vault,
- AWS Backup le migliori pratiche di sicurezza, inclusa la libreria di policy gestite dai clienti che consentono di concedere o negare le autorizzazioni di backup e ripristino tramite il servizio supportato, e AWS
- AWS Backup Audit Manager, che consente di automatizzare i controlli di conformità per i backup rispetto a un elenco di controlli definito dall'utente.

  Consulta Creazione di framework utilizzando l'API AWS Backup per il controllo I backup sono protetti da AWS Backup Vault Lock con AWS Backup Audit Manager per garantire che le risorse previste siano protette con un blocco del vault.
- I meccanismi che rendono inattive le risorse possono influire sulla capacità di ripristinarle. Sebbene non possano ancora essere eliminate in un archivio chiuso, possono trovarsi in uno stato diverso da quello attivo. Ad esempio, l'impostazione Amazon Elastic Compute Cloud che consente di disabilitare un'AMI può bloccare temporaneamente la possibilità di ripristinare i backup delle istanze EC2. Ciò influisce su tutti i punti di ripristino EC2, anche sui backup interessati dal blocco del vault o dalla conservazione a fini legali.

  Se un backup EC2 è disabilitato, puoi riattivare un'AMI disabilitata. Una volta riattivato, può essere ripristinato. Per bloccare la funzionalità di disabilitazione dell'AMI, puoi utilizzare le politiche IAM per non consentire`ec2:DisableImage`.

> **Note**
>
> AWS Backup Vault Lock non è la stessa funzionalità di Amazon S3 Glacier Vault Lock, che è compatibile solo con S3 Glacier.

Eliminazione di un vault di backup

Per evitare eliminazioni di massa accidentali o dolose, puoi eliminare un vault di backup in AWS Backup solo dopo aver eliminato tutti i punti di ripristino al suo interno (o dopo che l'eliminazione è avvenuta a opera del sistema di gestione del ciclo di vita del piano di backup). Per eliminare i punti di ripristino manualmente, consulta Pulire le risorse.

Quando si elimina un vault di backup, aggiornare i piani di backup in modo che puntino al nuovo vault di backup. Un piano di backup che punta a un backup eliminato compromette la creazione del backup.

> **Note**
>
> Non è possibile eliminare due archivi di backup: l'archivio di backup AWS Backup predefinito e l'archivio di backup automatico di Amazon EFS.

Per eliminare un archivio di backup utilizzando la console AWS Backup

1. Accedere a e aprire AWS Management Console la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Scegli il nome dell'archivio di backup per aprirne la pagina dei dettagli.
4. Scegliere ed eliminare i backup associati al vault di backup.
5. Scegli Elimina vault. Quando viene richiesta la conferma, inserisci il nome del vault e quindi scegli Elimina Backup vault.

Utilizzo dei backup

Un backup, o punto di ripristino, rappresenta il contenuto di una risorsa, ad esempio un volume Amazon Elastic Block Store (Amazon EBS) o una tabella Amazon DynamoDB, in un determinato momento. Punto di ripristino è un termine che si riferisce generalmente ai diversi backup nei AWS servizi, come gli snapshot di Amazon EBS e i backup DynamoDB. I termini punto di ripristino e backup vengono utilizzati in modo intercambiabile.

AWS Backup salva i punti di ripristino nelle casseforti di backup, che puoi organizzare in base alle tue esigenze aziendali. Ad esempio, è possibile salvare un set di risorse che contengono informazioni finanziarie per l'anno fiscale 2020. Quando è necessario ripristinare una risorsa, è possibile utilizzare la AWS Backup console o AWS Command Line Interface (AWS CLI) per trovare e ripristinare la risorsa necessaria.

Ogni punto di ripristino ha un ID univoco. L'ID univoco si trova alla fine del nome della risorsa Amazon (ARN) del punto di ripristino. Per esempi di ARN e ID univoci dei punti di ripristino, consulta la tabella in Risorse e operazioni.

> **Important**
>
> Per evitare costi aggiuntivi, configura la policy di conservazione con una durata di storage a caldo di almeno una settimana. Per ulteriori informazioni, consulta Misurazione, costi e fatturazione.

Le seguenti sezioni forniscono una panoramica delle attività di gestione di backup di base in AWS Backup.

Argomenti

- Creazione di un backup
- Copia di un backup
- Eliminazione di backup
- Modifica di un backup
- Ripristino di un backup
- Test di ripristino

- Visualizzazione di un elenco di backup

Creazione di un backup

Con AWS Backup, è possibile creare backup automaticamente utilizzando piani di backup o manualmente avviando un backup su richiesta.

Creazione di backup automatici

Quando vengono creati automaticamente dai piani di backup, vengono configurati con le impostazioni del ciclo di vita definite nel piano di backup. Sono organizzati nel vault di backup specificato nel piano di backup. Vengono inoltre assegnati i tag elencati nel piano di backup. Per ulteriori informazioni sui piani di backup, consulta Gestione dei backup mediante i piani di backup.

Creazione di backup on demand

Quando si crea un backup on demand, è possibile configurare per il backup queste impostazioni. Quando un backup viene creato automaticamente o manualmente, viene avviato un processo di backup. Per informazioni su come creare un backup on demand, consulta Creazione di un backup su richiesta utilizzando AWS Backup.

Nota: un backup on demand crea un processo di backup; lo stato del processo di backup passerà a `Running` entro un'ora (o quando specificato). Puoi scegliere un backup on demand se desideri creare un backup in un momento diverso dall'ora pianificata definita in un piano di backup. Un backup on demand può essere utilizzato, ad esempio, per eseguire il test del backup e della funzionalità in qualsiasi momento.

I backup su richiesta non possono essere utilizzati con point-in-time ripristino (PITR) poiché un backup su richiesta preserva le risorse nello stato in cui si trovano quando viene eseguito il backup, mentre il PITR utilizza backup continui che registrano le modifiche per un periodo di tempo.

Stati del processo di backup

Ogni processo di backup dispone di un ID univoco. Ad esempio, `D48D8717-0C9D-72DF-1F56-14E703BF2345`.

È possibile visualizzare lo stato di un processo di backup nella pagina Processi della console di AWS Backup . Gli stati dei processi di Backup includono `CREATED` `PENDINGRUNNING`,`ABORTING`,`ABORTED`,,`COMPLETED`, `FAILEDEXPIRED`, e`PARTIAL`.

Funzionamento dei backup incrementali

Molte risorse supportano il backup incrementale con. AWS Backup Un elenco completo è disponibile nella sezione relativa al backup incrementale della tabella Disponibilità delle funzionalità per risorsa.

Sebbene ogni backup successivo al primo sia incrementale (ovvero acquisisce solo le modifiche rispetto al backup precedente), tutti i backup eseguiti con AWS Backup conservano i dati di riferimento necessari per consentire un ripristino completo. Ciò è vero anche se il backup originale (completo) ha raggiunto la fine del suo ciclo di vita ed è stato eliminato.

Ad esempio, se il backup del giorno 1 (completo) è stato eliminato a causa di una policy del ciclo di vita di 3 giorni, sarà comunque possibile eseguire un ripristino completo con i backup dei giorni 2 e 3. A tale scopo, AWS Backup mantiene i dati di riferimento necessari dal giorno 1.

Accesso alle risorse di origine

AWS Backup necessita dell'accesso alle risorse di origine per eseguirne il backup. Per esempio:

- Per eseguire il backup di un'istanza Amazon EC2, l'istanza può trovarsi nello stato `stopped` o `running`, ma non nello stato `terminated`. Questo perché un'`stopped`istanza `running` or può comunicare con AWS Backup, ma un'`terminated`istanza no.
- Per eseguire il backup di una macchina virtuale, il Backup gateway del relativo hypervisor deve essere nello stato `ONLINE`. Per ulteriori informazioni, consulta Comprendere lo stato dell'hypervisor.
- Per eseguire il backup di un database Amazon RDS, Amazon Aurora o un cluster Amazon DocumentDB, lo stato di tali risorse deve essere `AVAILABLE`.
- Per eseguire il backup di un Amazon Elastic File System (Amazon EFS), lo stato deve essere `AVAILABLE`.
- Per eseguire il backup di un file system Amazon FSx, lo stato deve essere `AVAILABLE`. Se lo stato è `UPDATING`, la richiesta di backup viene accodata fino a quando lo stato del file system non diventa `AVAILABLE`.

  FSx per ONTAP non supporta il backup di determinati tipi di volume, inclusi volumi DP (protezione dei dati), volumi LS (condivisione del carico), volumi completi o volumi su file system completi. Per ulteriori informazioni, consulta FSx for ONTAP Working with backups.

AWS Backup conserva i backup creati in precedenza coerenti con la politica del ciclo di vita, indipendentemente dallo stato della risorsa di origine.

Argomenti

Creazione di un backup su richiesta utilizzando AWS Backup

Sulla AWS Backup console, la pagina Risorse protette elenca le risorse di cui è stato eseguito il backup AWS Backup almeno una volta. Se lo utilizzi AWS Backup per la prima volta, non ci sono risorse (come volumi Amazon EBS o database Amazon RDS) elencate in questa pagina. Ciò è vero anche è stata assegnata una risorsa a un piano di backup che non ha eseguito un lavoro di backup pianificato almeno una volta.

Nota: un backup on demand inizia immediatamente a eseguire il backup della risorsa. Puoi scegliere un backup on demand se desideri creare un backup in un momento diverso dall'ora pianificata definita in un piano di backup. Un backup on demand può essere utilizzato, ad esempio, per eseguire il test del backup e della funzionalità in qualsiasi momento.

I backup su richiesta non possono essere utilizzati con point-in-time restore (PITR) poiché un backup su richiesta preserva le risorse nello stato in cui si trovano quando viene eseguito il backup, mentre PITR utilizza backup continui che registrano le modifiche nel corso di un periodo di tempo.

Considerazioni

- Se il ruolo AWS Backup predefinito non è presente nel tuo account, ne viene creato uno con le autorizzazioni corrette.
- Quando i backup scadono e sono contrassegnati per l'eliminazione come parte della policy del ciclo di vita, AWS Backup elimina i backup in un momento scelto in modo casuale nelle 8 ore successive. Questa finestra aiuta a garantire prestazioni costanti.
- Per le risorse Amazon EC2, copia AWS Backup automaticamente i tag delle risorse individuali e di gruppo esistenti, oltre ai tag aggiunti in questo passaggio.
- AWS Backup esegue i backup EC2 con «nessun riavvio» come comportamento predefinito. AWS Backup attualmente supporta risorse in esecuzione su Amazon EC2 e alcuni tipi di istanze non sono supportati. Per ulteriori informazioni, consulta Creazione di backup Windows VSS.

Per creare un backup on demand

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Dal pannello di controllo scegliere Crea backup on demand. In alternativa, utilizzando il riquadro di navigazione, scegliere Risorse protette, quindi Crea backup on demand.
3. Per la pagina Tipo di risorsa, scegli il tipo di risorsa di cui desideri eseguire il backup. Ad esempio, scegli DynamoDB per le tabelle Amazon DynamoDB.
4. Scegli il nome o l'ID della risorsa da proteggere. Ad esempio, scegli il nome della tabella DynamoDB per Amazon DynamoDB.
5. Verificare che l'opzione Create backup now (Crea backup ora) sia selezionata.
6. Se il tipo di risorsa supporta la transizione alla conservazione a freddo, è presente la conservazione a freddo. Per ulteriori informazioni, consulta la colonna dal ciclo di vita alla conservazione a freddo nella tabella Disponibilità delle funzionalità per risorsa.

   Per specificare quando il backup deve essere archiviato in celle frigorifere, scegli Sposta i backup dalla conservazione a caldo a quella a freddo, quindi specifica la durata della conservazione a caldo.
7. Per Periodo di conservazione totale, specifica il numero di giorni. Se è stato specificato un periodo di conservazione a freddo, il periodo di conservazione viene suddiviso tra conservazione a caldo e a freddo.

8. Scegliere un Vault di Backup esistente o crearne uno nuovo. Scegliendo Crea nuovo vault di Backup, si apre una nuova pagina in cui è possibile creare un vault e al termine viene visualizzata nuovamente la pagina Crea backup on demand.
9. Per il ruolo IAM, scegli il ruolo predefinito o un ruolo che hai creato.
10. Per assegnare un tag al backup su richiesta, espandi Tag aggiunti ai punti di ripristino, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
11. Se il tipo di risorsa è EC2, sono presenti le impostazioni di backup avanzate. Per scattare istantanee coerenti con l'applicazione utilizzando Windows Volume Shadow Copy Service (VSS), scegli Windows VSS.
12. Scegliere Create on-demand backup (Crea backup on demand). Si apre la pagina Lavori, in cui è possibile visualizzare un elenco di lavori e visualizzare lo stato dei lavori.

Backup e point-in-time ripristino continui (PITR)

Argomenti

Per alcune risorse, AWS Backup supporta backup e point-in-time ripristino continui (PITR) oltre ai backup con snapshot.

Con i backup continui, puoi ripristinare la risorsa AWS Backup supportata riavvolgendola a un'ora specifica a tua scelta, entro 1 secondo di precisione (fino a un massimo di 35 giorni). Il backup continuo funziona creando innanzitutto un backup completo della risorsa e quindi eseguendo costantemente il backup dei log delle transazioni della risorsa. Il ripristino PITR funziona accedendo al backup completo e riproducendo il registro delle transazioni fino all'ora indicata per il ripristino. AWS Backup

In alternativa, i backup snapshot possono essere eseguiti con frequenza oraria. I backup snapshot possono essere archiviati per un massimo di 100 anni. Gli snapshot possono essere copiati per backup completi o incrementali.

Poiché i backup continui e i backup snapshot offrono diversi vantaggi, si consiglia di proteggere le risorse con regole di backup continui e snapshot.

Nota: un backup on demand inizia immediatamente a eseguire il backup della risorsa. Puoi scegliere un backup on demand se desideri creare un backup in un momento diverso dall'ora pianificata definita in un piano di backup. Un backup on demand può essere utilizzato, ad esempio, per eseguire il test del backup e della funzionalità in qualsiasi momento.

I backup su richiesta non possono essere utilizzati con il point-in-time ripristino (PITR) poiché un backup su richiesta preserva le risorse nello stato in cui si trovano quando viene eseguito il backup, mentre il PITR utilizza backup continui che registrano le modifiche nel corso di un periodo di tempo.

È possibile attivare i backup continui per le risorse supportate quando si crea un piano di backup utilizzando la console o l'API. AWS Backup AWS Backup

Per abilitare i backup continui tramite la console

1. Accedi a e AWS Management Console apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Piani di backup e seleziona Crea un piano di backup.
3. In Regole di backup, scegli Aggiungi regola di backup.
4. Nella sezione Configurazione regola di backup, seleziona Abilita backup continui per le risorse supportate.

Servizi supportati per il backup continuo/ripristino point-in-time (PITR)

AWS Backup supporta backup e point-in-time ripristino continui per i seguenti servizi e applicazioni:

Amazon S3

Per attivare PITR per i backup S3, i backup continui devono far parte del piano di backup.

Sebbene il PITR possa essere attivo per questo backup originale del bucket di origine, le copie di destinazione tra regioni o tra account non dispongono di PITR e il ripristino da queste copie verrà eseguito al momento in cui sono state create (le copie saranno copie snapshot) anziché a un momento specificato.

RDS

Pianificazioni di backup: quando un AWS Backup piano crea sia istantanee di Amazon RDS che backup AWS Backup continui, pianifica in modo intelligente le finestre di backup in modo da coordinarle con la finestra di manutenzione di Amazon RDS per evitare conflitti. Per prevenire ulteriormente i conflitti, la configurazione manuale della finestra di backup automatizzata di Amazon RDS non è disponibile. RDS acquisisce snapshot una volta al giorno a prescindere che il piano di backup disponga di una frequenza dei backup snapshot diversa da una volta al giorno.

Impostazioni: dopo aver applicato una regola di backup AWS Backup continuo a un'istanza Amazon RDS, non puoi creare o modificare le impostazioni di backup continuo per quell'istanza in Amazon RDS; le modifiche devono essere eseguite tramite la AWS Backup console o la CLI. AWS Backup

Trasferisci il controllo del backup continuo per un'istanza Amazon RDS ad Amazon RDS:

Console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup plans (Piani di backup).
3. Elimina tutti i piani di backup di Amazon RDS con un backup continuo che protegge tale risorsa.
4. Scegliere Vault di Backup. Elimina il punto di ripristino del backup continuo dal vault di backup. In alternativa, attendi che scada il periodo di conservazione, in modo che il punto AWS Backup di ripristino venga eliminato automaticamente.

   Dopo aver completato questi passaggi, AWS Backup trasferirai il controllo continuo del backup della tua risorsa ad Amazon RDS.

AWS CLI

Chiama l'operazione API `DisassociateRecoveryPoint`.

Per ulteriori informazioni, consulta DisassociateRecoveryPoint.

Autorizzazioni IAM richieste per i backup continui Amazon RDS

- AWS Backup Per configurare backup continui per il tuo database Amazon RDS, verifica che l'autorizzazione API `rds:ModifyDBInstance` esista nel ruolo IAM definito dalla configurazione del tuo piano di backup. Per ripristinare i backup continui Amazon RDS, devi aggiungere

l'autorizzazione `rds:RestoreDBInstanceToPointInTime` al ruolo IAM inviato per il processo di ripristino. Puoi utilizzare il `AWS Backup default service role` per eseguire backup e ripristini.

- Per descrivere l'intervallo di tempo disponibile per il point-in-time ripristino, AWS Backup chiamate. `rds:DescribeDBInstanceAutomatedBackupsAPI` Nella AWS Backup console, è necessario disporre dell'autorizzazione `rds:DescribeDBInstanceAutomatedBackups` API prevista dalla policy gestita AWS Identity and Access Management (IAM). Puoi utilizzare le policy gestite `AWSBackupFullAccess` o `AWSBackupOperatorAccess`. Entrambe le policy dispongono di tutte le autorizzazioni richieste. Per ulteriori informazioni, consulta l'argomento relativo alle policy gestite.

Periodi di conservazione: quando modifichi il periodo di conservazione PITR, AWS Backup le chiamate `ModifyDBInstance` e le applicazioni cambiano immediatamente. Se si dispone di altri aggiornamenti di configurazione in attesa della finestra di manutenzione successiva, la modifica del periodo di conservazione del PITR applicherà immediatamente anche tali aggiornamenti di configurazione. Per ulteriori informazioni, consulta `ModifyDBInstance` nella Documentazione di riferimento delle API di Amazon Relational Database Service.

Copie dei backup continui di Amazon RDS:

- I processi di copia snapshot incrementali vengono elaborati più rapidamente rispetto ai processi di copia snapshot completi. La conservazione di una copia snapshot precedente fino al completamento del nuovo processo di copia può ridurre la durata del processo di copia. Se si sceglie di copiare snapshot da istanze database RDS, è importante notare che l'eliminazione delle copie precedenti comporterà innanzitutto la creazione di copie snapshot complete (anziché incrementali). Per ulteriori informazioni sull'ottimizzazione della copia, consulta Copia snapshot incrementale degli snapshot nella Guida per l'utente di Amazon RDS
- Creazione di copie di backup continui di Amazon RDS: non puoi creare copie di backup continui di Amazon RDS perché AWS Backup Amazon RDS non consente la copia dei log delle transazioni. Invece, AWS Backup crea un'istantanea e la copia con la frequenza specificata nel piano di backup.

Ripristini: puoi eseguire un point-in-time ripristino utilizzando uno dei due AWS Backup o Amazon RDS. Per istruzioni AWS Backup sulla console, consulta Ripristino di un database Amazon RDS. Per le istruzioni su Amazon RDS, consulta Ripristino a un'ora specifica per un'istanza database nella Guida per l'utente di Amazon RDS.

> **Tip**
>
> Un'istanza di database multi AZ (zona di disponibilità) impostata su non `Always On` dovrebbe avere una conservazione del backup impostata su zero. Se si verificano errori, utilizza AWS CLI il comando `disassociate-recovery-point` anzichédelete-`recovery-point`, quindi modifica l'impostazione di conservazione su 1 nelle impostazioni di Amazon RDS.

Per informazioni generali sull'utilizzo di Amazon RDS, consulta la Guida per l'utente di Amazon RDS.

Aurora

Per abilitare il backup continuo delle risorse Aurora, consulta i passaggi nella prima sezione di questa pagina.

La procedura per ripristinare un cluster Aurora in un punto temporale è una variazione dei passaggi per ripristinare uno snapshot di un cluster Aurora.

Quando si esegue un ripristino point-in-time, la console visualizza una sezione ora di ripristino. Consulta Ripristino di un backup continuo più avanti in questa pagina in Lavorare con backup continui.

SAP HANA su istanze Amazon EC2

Puoi effettuare backup continui, che possono essere utilizzati con point-in-time restore (PITR) (tieni presente che i backup su richiesta preservano le risorse nello stato in cui sono state acquisite; mentre PITR utilizza backup continui che registrano le modifiche in un periodo di tempo).

Con i backup continui, puoi ripristinare il database SAP HANA su un'istanza EC2 riportandola a un momento specifico scelto, entro 1 secondo di precisione (tornando indietro fino a un massimo di 35 giorni). Il backup continuo funziona creando innanzitutto un backup completo della risorsa e quindi eseguendo costantemente il backup dei log delle transazioni della risorsa. Il ripristino PITR funziona accedendo al backup completo e riproducendo il registro delle transazioni fino all'ora indicata per il ripristino. AWS Backup

Puoi attivare i backup continui quando crei un piano di backup AWS Backup utilizzando la AWS Backup console o l'API.

Per abilitare i backup continui tramite la console

1. Accedi a e AWS Management Console apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Piani di backup e seleziona Crea un piano di backup.
3. In Regole di backup, scegli Aggiungi regola di backup.
4. Nella sezione Configurazione regola di backup, seleziona Abilita backup continui per le risorse supportate.

Dopo aver disabilitato PITR (point-in-timeripristino) per i backup del database SAP HANA, i log continueranno a essere inviati AWS Backup fino alla scadenza del punto di ripristino (stato uguale). `EXPIRED`) Puoi passare a una posizione di backup dei log alternativa in SAP HANA per interrompere la trasmissione dei log ad AWS Backup.

Un punto di ripristino continuo con uno stato pari a `STOPPED` indica che un punto di ripristino continuo è stato interrotto; ovvero, i log trasmessi da SAP HANA a che mostrano le modifiche incrementali a AWS Backup un database presentano una lacuna. I punti di ripristino che si verificano entro questo gap di intervallo di tempo presentano uno stato `STOPPED`..

Per i problemi che si possono verificare durante i processi di ripristino dei backup continui (punti di ripristino), consulta la sezione Risoluzione dei problemi relativi al ripristino di SAP HANA di questa guida.

Trovare un backup continuo

È possibile utilizzare la AWS Backup console per trovare il backup continuo.

Per trovare un backup continuo utilizzando la AWS Backup console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di spostamento, scegli Vault di backup, quindi seleziona il vault di backup dall'elenco.
3. Nella sezione Backup, nella colonna Tipo di backup, ordina per punti di ripristino continui. Puoi anche ordinare in base all'ID punto di ripristino per il prefisso continuo.

Ripristino di un backup continuo

Per ripristinare un backup continuo utilizzando la AWS Backup console

- Durante il processo di ripristino PITR, la AWS Backup console visualizza una sezione relativa alla durata del ripristino. In questa sezione, effettua una delle operazioni seguenti:
  - Scegli di ripristinare l'Ora ripristinabile più recente.
  - Scegli Specificare data e ora per immettere la data e l'ora desiderate entro il periodo di conservazione.

Per ripristinare un backup continuo utilizzando l'API AWS Backup

1. Per Amazon S3, consulta Utilizzare l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino S3.
2. Per Amazon RDS, consulta Utilizzare l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino Amazon RDS.

Interruzione o eliminazione di backup continui

Puoi interrompere la creazione di backup continui o eliminare backup specifici (o punti PITR). point-in-time-recovery

Se desideri interrompere i backup continui, devi eliminare la regola di backup continuo dal piano di backup. Se desideri interrompere i backup continui per una o più risorse ma non per tutte le risorse, crea un nuovo piano di backup con la regola di backup continuo per le risorse di cui desideri continuare il backup. Se invece elimini solo un punto di ripristino di backup continuo dal vault di backup, il piano di backup continuerà comunque a eseguire la regola di backup continuo, creando un nuovo punto di ripristino.

Tuttavia, anche dopo aver eliminato la regola di backup continuo, AWS Backup ricorda il periodo di conservazione della regola di backup ora eliminata. Eliminerà automaticamente il punto di ripristino del backup continuo dal vault di backup in base al periodo di conservazione specificato.

Quando elimini i punti di ripristino Amazon RDS, considera:

- Un'istanza di database multi AZ (zona di disponibilità) impostata su non `Always On` dovrebbe avere una conservazione del backup impostata su zero. Se si verificano errori, utilizza AWS CLI

il comando `disassociate-recovery-point` anzichédelete-recovery-point, quindi modifica l'impostazione di conservazione su 1 nelle impostazioni di Amazon RDS.

- Quando viene eliminato un punto di point-in-time ripristino (un backup creato da un backup continuo) per Amazon RDS, viene attivato un riavvio del database e i log binari vengono disabilitati. Per ulteriori dettagli, consulta Periodo di retention dei backup nella Guida per l'utente di Amazon RDS.

Quando elimini i punti di ripristino Aurora, considera:

Se è selezionato per un punto di ripristino Amazon Aurora, AWS Backup imposta il periodo di conservazione su 1 giorno. I backup Aurora non possono essere eliminati completamente finché non viene eliminato anche il cluster di origine.

Copia di backup continui

Se una regola di backup continuo specifica anche una copia tra account o tra regioni, AWS Backup acquisisce uno snapshot del backup continuo e copia lo snapshot nel vault di destinazione. Per ulteriori informazioni sulla copia dei punti di ripristino tra account e regioni, consulta Copia di un backup.

I backup continui creano backup periodici in base alla frequenza impostata nella regola del piano di backup nell'account e/o nella regione di destinazione.

AWS Backup non supporta copie su richiesta di backup continui.

Modifica del periodo di conservazione

È possibile utilizzarlo AWS Backup per aumentare o diminuire il periodo di conservazione della regola di backup continuo esistente. Il periodo di conservazione minimo è 1 giorno. Il periodo di conservazione massimo è 35 giorni.

Se si aumenta il periodo di conservazione, l'effetto è immediato. Se riduci il periodo di conservazione, AWS Backup aspetterai che sia trascorso un periodo di tempo sufficiente prima di applicare la modifica per prevenire la perdita di dati. Ad esempio, se riduci il periodo di conservazione da 35 a 20 giorni, AWS Backup continuerà a conservare 35 giorni di backup continuo fino a quando non saranno trascorsi 15 giorni. Questo design protegge gli ultimi 15 giorni di backup nel momento in cui è stata effettuata la modifica.

Rimozione dell'unica regola di backup continuo da un piano di backup

Quando si crea un piano di backup con una regola di backup continuo e poi si rimuove tale regola, AWS Backup ricorda il periodo di conservazione indicato nella regola ora eliminata. Il backup continuo verrà eliminato dal vault di backup allo scadere del periodo di conservazione.

Backup continui sovrapposti sulla stessa risorsa

In generale, è necessario proteggere ogni risorsa con non più di una regola di backup continuo. Questo perché i backup continui aggiuntivi sono ridondanti. Tuttavia, man mano che si amplia lo spazio di backup, è possibile che più piani, regole e archivi di backup si sovrappongano su un'unica risorsa. AWS Backup gestisce queste sovrapposizioni come segue.

Se includi la stessa risorsa in più di un piano di backup con una regola di backup continuo, AWS Backup creerà un backup continuo solo per il primo piano di backup valutato. Per tutti gli altri piani di backup verranno creati backup snapshot.

Se si includono più regole di backup continuo in un singolo piano di backup:

- Se le tue regole fanno riferimento allo stesso archivio di backup, crea un backup continuo AWS Backup solo per la regola con il periodo di conservazione più lungo. Tutte le altre regole vengono ignorate.
- Se le tue regole fanno riferimento a diversi archivi di backup, AWS Backup rifiuta il piano in quanto non valido.

oint-in-time Considerazioni sul ripristino

Tieni presente le seguenti considerazioni per point-in-time il ripristino:

- Fallback automatico a snapshot: se AWS Backup non è in grado di eseguire un backup continuo, proverà invece a eseguire un backup snapshot.
- Nessun supporto per i backup continui su richiesta: AWS Backup non supporta il backup continuo su richiesta perché il backup su richiesta registra un point-in-time, mentre i record di backup continui cambiano in un periodo di tempo.
- Nessun supporto per la transizione allo storage a freddo: i backup continui non supportano la transizione allo storage a freddo perché questa richiede un periodo di transizione minimo di 90 giorni, mentre i backup continui hanno un periodo di conservazione massimo di 35 giorni.

- Ripristino di attività recenti: l'attività di Amazon RDS consente il ripristino fino agli ultimi 5 minuti di attività; Amazon S3 consente il ripristino fino agli ultimi 15 minuti di attività.

Backup Amazon S3

AWS Backup supporta il backup e il ripristino centralizzati delle applicazioni che archiviano i dati solo in S3 o insieme ad altri AWS servizi per database, archiviazione ed elaborazione. Sono disponibili molte funzionalità per i backup S3, incluso Backup Audit Manager.

È possibile utilizzare un'unica policy di backup per AWS Backup automatizzare centralmente la creazione di backup dei dati delle applicazioni. AWS Backup organizza automaticamente i backup su diversi AWS servizi e applicazioni di terze parti in un'unica posizione centralizzata e crittografata (nota come backup vault) in modo da poter gestire i backup dell'intera applicazione attraverso un'esperienza centralizzata. Per S3, puoi creare backup continui e ripristinare i dati delle applicazioni archiviati in S3 e ripristinare i backup su un file con un solo clic. point-in-time

Con AWS Backup, puoi creare i seguenti tipi di backup dei tuoi bucket S3, inclusi dati di oggetti, tag, elenchi di controllo degli accessi (ACL) e metadati definiti dall'utente:

- I backup continui consentono di eseguire il ripristino a un momento qualsiasi negli ultimi 35 giorni. I backup continui per un bucket S3 devono essere configurati solo in un piano di backup.

  Consulta Ripristino point-in-time per un elenco di servizi supportati e istruzioni su come utilizzare AWS Backup per effettuare backup continui.
- I backup periodici utilizzano snapshot dei dati per consentire di mantenere i dati per la durata specificata massima di 99 anni. Puoi pianificare backup periodici con frequenze di 1 ora, 12 ore, 1 giorno, 1 settimana o 1 mese. AWS Backup esegue backup periodici durante la finestra di backup definita nel piano di backup.

  Vedi Creazione di un piano di backup per capire come AWS Backup applicare il piano di backup alle tue risorse.

Per i backup S3 sono disponibili copie su più account e più regioni, ma le copie dei backup continui non dispongono di funzionalità di ripristino. point-in-time

I backup continui e periodici di bucket S3 devono risiedere entrambi nello stesso vault di backup.

Per entrambi i tipi di backup, il primo backup è un backup completo, mentre i backup successivi sono incrementali a livello di oggetto.

> **Note**
>
> È necessario abilitare il controllo delle versioni S3 sul bucket S3 da utilizzare per Amazon AWS Backup S3. Questo prerequisito è stato mantenuto perché in AWS il controllo delle versioni S3 è consigliato come una best practice per la protezione dei dati.
> Ti consigliamo di impostare un periodo di scadenza del ciclo di vita per le versioni S3. La mancata impostazione di un periodo di scadenza del ciclo di vita potrebbe aumentare i costi di S3 perché AWS Backup esegue il backup e l'archiviazione di tutte le versioni non scadute dei dati S3. Per ulteriori informazioni sulla configurazione delle policy del ciclo di vita di S3, segui le istruzioni in questa pagina.

Confronto dei tipi di backup S3

La strategia di backup per le risorse S3 può includere solo backup continui, solo backup (snapshot) periodici o una combinazione di entrambi. Le informazioni riportate di seguito consentono di scegliere la soluzione migliore per l'organizzazione in uso:

Solo backup continui:

- Dopo che il primo backup completo dei dati esistenti è stato completato, le modifiche ai dati del bucket S3 vengono monitorate mentre si verificano.
- Le modifiche tracciate consentono di utilizzare PITR (point-in-time ripristino) per il periodo di conservazione del backup continuo. Per eseguire un processo di ripristino, scegli il punto temporale in cui desideri eseguire il ripristino.
- Il periodo di conservazione di ogni backup continuo è composto da un massimo di 35 giorni.

Solo backup (snapshot) periodici, pianificati o on demand:

- AWS Backup esegue la scansione dell'intero bucket S3, recupera l'ACL e i tag di ogni oggetto e avvia una richiesta Head per ogni oggetto presente nell'istantanea precedente ma non trovato nell'istantanea creata.
- Il point-in-time backup è coerente.
- La data e l'ora di backup registrate sono l'ora in cui viene AWS Backup completato l'attraversamento del bucket, non il momento in cui è stato creato un job di backup.
- Il primo backup di un bucket è un backup completo. Ogni backup successivo è incrementale e rappresenta la modifica dei dati dall'ultimo snapshot.

- Lo snapshot acquisito dal backup periodico può avere un periodo di conservazione massimo 99 anni.

Backup continui combinati con backup periodici/+snapshot:

- Al termine del primo backup completo dei dati esistenti (ogni bucket), le modifiche nel bucket vengono monitorate mentre si verificano.
- È possibile eseguire un point-in-time ripristino da un punto di ripristino continuo.
- Le istantanee sono point-in-time coerenti.
- Gli snapshot vengono acquisiti direttamente dal punto di ripristino continuo, eliminando la necessità di ripetere la scansione di un bucket per consentire processi più rapidi.
- Gli snapshot e i punti di ripristino continui condividono la derivazione dei dati; lo storage dei dati tra snapshot e punti di ripristino continui non è duplicato.

Classi di storage S3 supportate

AWS Backup consente di eseguire il backup dei dati S3 archiviati nelle seguenti classi di storage S3:

- S3 Standard
- Standard S3 - Accesso infrequente (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- Piano intelligente S3 (S3 INT)

I backup di un oggetto nella classe di storage S3 Intelligent-Tiering (INT) accedono a tali oggetti. Questo accesso attiva S3 Intelligent-Tiering per spostare automaticamente tali oggetti su Frequent Access.

I backup che accedono ai livelli Infrequent Access, incluse le classi S3 Standard - Infrequent Access (IA) e S3 One Zone-IA, rientrano nella tariffa di storage S3 di Frequent Access (si applica ai livelli Infrequent Access o Archive Instant Access).

Ad eccezione di Glacier Instant Retrieval, le classi di storage archiviate non sono supportate.

Per ulteriori informazioni sui prezzi di storage per Amazon S3, consulta la pagina dei prezzi di Amazon S3.

Considerazioni AWS Backup per Amazon S3

Quando si esegue il backup di risorse S3, occorre tenere presenti le considerazioni seguenti:

- Supporto mirato ai metadati degli oggetti: AWS Backup supporta i seguenti metadati: tag, liste di controllo degli accessi (ACL), metadati definiti dall'utente, data di creazione originale e ID della versione. Puoi anche ripristinare tutti i dati e i metadati di backup a eccezione della data di creazione originale, l'ID versione, la classe di storage e gli e-tag.
- Un nome della chiave dell'oggetto S3 può essere costituito dalla maggior parte delle stringhe codificabili UTF-8. I seguenti caratteri Unicode sono consentiti. `#x9` | `#xA` | `#xD` | `#x20 to #xD7FF` | `#xE000 to #xFFFD` | `#x10000 to #x10FFFF`.

  I nomi delle chiavi degli oggetti che includono caratteri non presenti in questo elenco possono essere esclusi dai backup. Per maggiori informazioni consulta le specifiche W3C per i caratteri.
- Transizione all'archiviazione a freddo: AWS Backup la politica di gestione del ciclo di vita di S3 consente di definire la tempistica di scadenza dei backup, ma al momento la transizione alla memorizzazione a freddo dei backup S3 non è attualmente supportata.
- I backup di bucket S3 con molte versioni dello stesso oggetto creati nello stesso secondo non sono attualmente supportati.
- Per i backup periodici, AWS Backup fa del suo meglio per tenere traccia di tutte le modifiche ai metadati degli oggetti. Tuttavia, se un tag o un'ACL viene aggiornato più volte nell'arco di 1 minuto, AWS Backup potrebbe non essere in grado di acquisire tutti gli stati intermedi.
- AWS Backup attualmente non offre supporto per i backup di oggetti crittografati con SSE-C. AWS Backup inoltre, attualmente non supporta i backup delle configurazioni dei bucket, tra cui la policy del bucket, le impostazioni, il nome o il punto di accesso.
- AWS Backup attualmente non supporta i backup di S3 su. AWS Outposts

> **Important**
>
> Negli account che registrano gli eventi di lettura dei dati, i bucket S3 con CloudTrail log abilitati devono salvare i log di accesso in un bucket di destinazione diverso; se i CloudTrail log vengono salvati nello stesso bucket, vengono registrati, si forma un ciclo infinito. Questo ciclo può innescare addebiti imprevisti e indesiderati.
> Per ulteriori informazioni, consulta Data events nella Guida per l'utente. CloudTrail

Finestre di completamento del backup S3

La tabella seguente mostra bucket di esempio di varie dimensioni che forniscono linee guida delle stime del tempo di completamento del backup completo iniziale di un bucket S3. I tempi di backup variano in base a dimensioni, contenuto, configurazione e impostazioni di ciascun bucket.

Dimensione bucket	Numero di oggetti	Tempo stimato per il completamento del backup iniziale
425 GB (gigabyte)	135 milioni	31 ore
800 TB (terabyte)	670 milioni	38 ore
6 PB (petabyte)	5 miliardi	100 ore
370 TB (terabyte)	7,5 miliardi	180 ore

Autorizzazioni e policy per il backup e il ripristino di Amazon S3

Per eseguire il backup, la copia e il ripristino delle risorse S3, è necessario disporre delle policy corrette nel proprio ruolo. Per aggiungere queste policy, passa a Policy gestite da AWS. Aggiungi AWSBackupServiceRolePolicyForS3Backupe AWSBackupServiceRolePolicyForS3Restoreai ruoli che intendi utilizzare per il backup e il ripristino dei bucket S3.

Se non disponi di autorizzazioni sufficienti, richiedi al responsabile dell'account amministrativo (amministratore) dell'organizzazione di aggiungere le policy ai ruoli previsti.

Per ulteriori informazioni, consulta Policy gestite e policy inline nella Guida per l'utente IAM.

AWS Backup per S3 si basa sulla ricezione di eventi S3 tramite Amazon. EventBridge Se questa impostazione è disabilitata nelle impostazioni di notifica dei bucket S3, i backup continui verranno interrotti per tali bucket con l'impostazione disattivata. Per ulteriori informazioni, consulta Using. EventBridge

Procedure consigliate e considerazioni sui costi per i backup di S3

Best practice

Per bucket con più di 300 milioni di oggetti:

- Per i bucket con più di 300 milioni di oggetti, la velocità di backup può raggiungere i 17.000 oggetti al secondo durante il backup completo iniziale del bucket (i backup incrementali avranno una velocità diversa); i bucket contenenti meno di 300 milioni di oggetti eseguono il backup a una velocità vicina a 1.000 oggetti al secondo.
- Si consigliano backup continui.
- Se il ciclo di vita del backup è pianificato per più di 35 giorni, è anche possibile abilitare i backup snapshot per il bucket nello stesso vault in cui sono archiviati i backup continui.

Considerazioni sui costi

- Le policy del ciclo di vita di S3 hanno una funzionalità opzionale chiamata Elimina i contrassegni di eliminazione degli oggetti scaduti. Quando questa funzionalità viene interrotta, i contrassegni di eliminazione, a volte in quantità di milioni, scadono senza alcun piano di pulizia. Quando si esegue il backup di bucket senza questa funzionalità, due problemi influiscono su tempi e costi:
  - I contrassegni di eliminazione vengono sottoposti a backup, al pari degli oggetti. Il tempo di backup e il tempo di ripristino possono essere influenzati a seconda del rapporto tra oggetti e contrassegni di eliminazione.
  - Ogni oggetto e contrassegno di cui viene eseguito il backup ha un costo minimo. A ogni contrassegno di eliminazione viene addebitata la stessa tariffa di un oggetto da 128 KiB.
- Per gli account che eseguono backup almeno giornalmente o con maggiore frequenza, è possibile ottenere vantaggi in termini di costi utilizzando backup continui se i dati all'interno dei backup presentano modifiche minime tra i backup.
- I bucket più grandi che non cambiano frequentemente possono trarre vantaggio dai backup continui, poiché ciò può comportare una riduzione dei costi quando non è necessario eseguire scansioni dell'intero bucket insieme a più richieste per oggetto su oggetti preesistenti (oggetti che sono invariati rispetto al backup precedente).
- I bucket che contengono più di 100 milioni di oggetti e che hanno un tasso di eliminazione basso rispetto alla dimensione complessiva del backup potrebbero ottenere vantaggi in termini di costi con un piano di backup contenente un backup continuo con un periodo di conservazione di 2 giorni e snapshot di un periodo di conservazione più lungo.
- Il tempo del backup (snapshot) periodico è allineato all'inizio del processo di backup quando non è necessaria la scansione di un bucket. Le scansioni non sono necessarie in un bucket contenente backup continui e snapshot, poiché in questi casi gli snapshot vengono acquisiti da un punto di ripristino continuo.

- Per ogni oggetto in una singola S3-GIR (Amazon S3 Glacier Instant Retrieval), AWS Backup esegue più chiamate, il che comporterà costi di recupero quando viene eseguito un backup.

  Costi di recupero simili si applicano ai bucket con oggetti nelle classi di storage S3-IA e S3 One Zone-IA.

- AWS KMS CloudTrail, e CloudWatch le funzionalità di Amazon che fanno parte della tua strategia di backup possono comportare costi aggiuntivi rispetto allo storage dei dati con bucket S3. Per informazioni sulla regolazione di queste funzionalità, consulta le seguenti sezioni:
  - Riduzione del costo di SSE-KMS con le chiavi bucket Amazon S3 nella Guida per l'utente di Amazon S3.
  - Puoi ridurre CloudTrail i costi escludendo AWS KMS gli eventi e disabilitando gli eventi relativi ai dati S3:
    - Escludi AWS KMS eventi: nella Guida per l'CloudTrail utente, la creazione di un percorso nella console (selettori di eventi di base) consente di escludere AWS KMS gli eventi per filtrarli dal percorso (l'impostazione predefinita include tutti gli eventi KMS):
    - L'opzione per registrare o escludere gli eventi KMS è disponibile solo se gli eventi di gestione vengono registrati sul trail. Se scegli di non registrare gli eventi di gestione, gli eventi KMS non vengono registrati e non puoi modificare le impostazioni di registrazione degli eventi KMS.
    - AWS KMS azioni come `EncryptDecrypt`, e `GenerateDataKey` in genere generano un grande volume (oltre il 99%) di eventi. Queste operazioni vengono ora registrate come eventi Read (Lettura). Le operazioni KMS a basso volume pertinenti, come `Disable`, `Delete` e `ScheduleKey` (che in genere rappresentano meno dello 0,5% del volume degli eventi KMS), vengono registrate come eventi Write (Scrittura).
    - Per escludere eventi a volume elevato come `Encrypt`, `Decrypt` e `GenerateDataKey`, ma registrare comunque eventi rilevanti come `Disable`, `Delete` e `ScheduleKey`, scegli di registrare gli eventi di gestione Scrittura e deseleziona la casella di controllo Escludi eventi AWS KMS .
    - Disabilita eventi di dati S3: per impostazione predefinita, i trail e gli archivi dati di eventi non registrano gli eventi di dati. Disattiva gli eventi di dati S3 prima del backup iniziale per ridurre i costi.
  - Per ridurre CloudWatch i costi, puoi interrompere l'invio di CloudTrail eventi ai CloudWatch registri quando aggiorni un percorso per disabilitare le impostazioni CloudWatch dei registri.

Ripristino di backup S3

Puoi ripristinare i dati S3 di cui hai eseguito il backup utilizzando AWS Backup la classe S3 Standard Storage. Puoi ripristinare i dati S3 in un bucket esistente, incluso il bucket originale. Durante il ripristino, puoi anche creare un nuovo bucket S3 come destinazione di ripristino. Puoi ripristinare i backup S3 solo nello stesso Regione AWS luogo in cui si trova il backup.

Puoi ripristinare l'intero bucket S3 o le cartelle o gli oggetti all'interno del bucket. AWS Backup ripristina la versione corrente di tale oggetto.

Per ripristinare i dati S3 utilizzando AWS Backup, consulta. Ripristino dei dati S3

Backup di macchine virtuali

AWS Backup supporta la protezione dei dati centralizzata e automatizzata per le macchine virtuali (VM) VMware locali insieme alle VM in VMware Cloud™ (VMC) on e VMware Cloud™ (VMC) on. AWS AWS OutpostsÈ possibile eseguire il backup dalle macchine virtuali locali e VMC su. AWS Backup Quindi, puoi ripristinare da AWS Backup su VM on-premise, VM nel VMC o il VMC su AWS Outposts.

AWS Backup offre inoltre funzionalità di gestione del backup delle VM completamente gestite e AWS native, come l'individuazione delle macchine virtuali, la pianificazione dei backup, la gestione della conservazione, un livello di storage a basso costo, la copia tra regioni e più account, il supporto per Vault Lock e AWS Backup Audit Manager, la crittografia indipendente dai dati di origine AWS Backup e le politiche di accesso ai backup. Per un elenco completo delle funzionalità e dei dettagli, consulta la tabella Disponibilità delle funzionalità per risorsa.

Puoi utilizzarle per proteggere le tue macchine virtuali su VMware Cloud AWS Backup ™ on. AWS Outposts AWS Backup archivia i backup delle macchine virtuali nell'area Regione AWS a cui è connesso VMware Cloud™ on. AWS Outposts È possibile utilizzarlo AWS Backup per proteggere VMware Cloud™ on AWS Backup VM quando si utilizza VMware Cloud™ on AWS Outposts per soddisfare le esigenze di bassa latenza e di elaborazione locale dei dati delle applicazioni. In base ai requisiti di residenza dei dati, puoi scegliere di archiviare i backup dei dati delle tue applicazioni nell'unità principale AWS Backup a cui sei connesso. Regione AWS AWS Outposts

Macchine virtuali supportate

AWS Backup può eseguire il backup e il ripristino di macchine virtuali gestite da un VMware vCenter.

Attualmente supportato:

- vSphere 8, 7.0 e 6.7
- Dimensioni dei dischi virtuali che sono multipli di 1 KiB
- Datastore NFS, VMFS e VSAN in locale e in VMC su AWS
- Modalità di trasporto SCSI Hot-Add e Network Block Device Secure Sockets Layer (NBDSSL) per la copia dei dati dalle macchine virtuali di origine verso sistemi VMware locali AWS
- Modalità Hot-Add per proteggere le macchine virtuali su VMware Cloud on AWS

Attualmente non supportata:

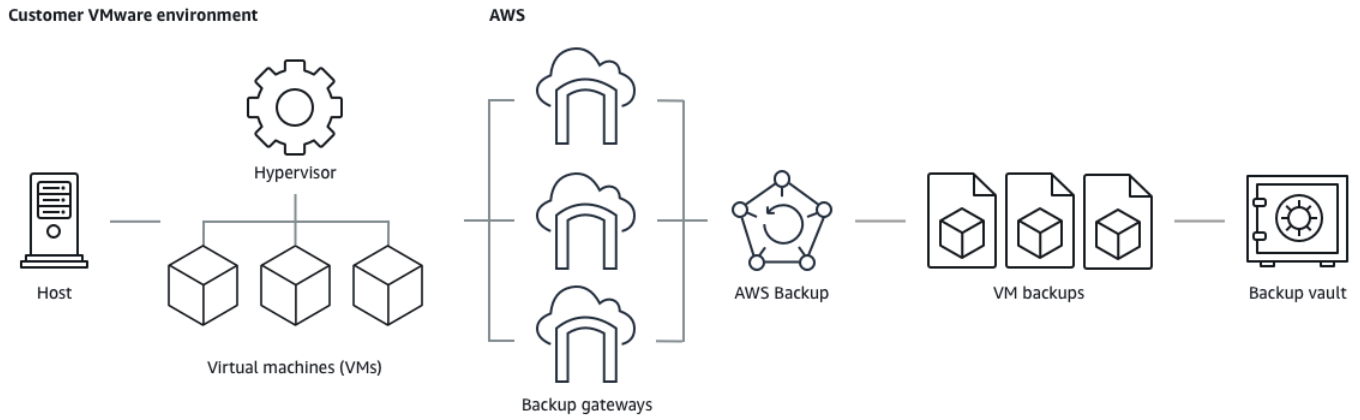
- Dischi RDM (raw disk mapping) o controller NVMe e relativi dischi
- Modalità disco indipendenti persistenti e indipendenti non persistenti

Coerenza del backup

Per impostazione predefinita,AWS Backup acquisisce backup coerenti con le applicazioni delle VM utilizzando l'impostazione di quiescenza VMware Tools sulla macchina virtuale. I backup sono coerenti con le applicazioni se le applicazioni sono compatibili con VMware Tools. Se la funzionalità di quiescenza non è disponibile, acquisisce backup coerenti con gli arresti anomali. AWS Backup Verifica che i backup soddisfino le esigenze dell'organizzazione eseguendo il test dei ripristini.

Backup gateway

Backup gateway è un AWS Backup software scaricabile che viene distribuito nell'infrastruttura VMware a cui connettere le macchine virtuali VMware. AWS Backup Il gateway si connette al server di gestione delle macchine virtuali per individuare le macchine virtuali, individua le macchine virtuali dell'utente, esegue la crittografia dei dati e li trasferisce in modo efficiente ad AWS Backup. Nel diagramma seguente viene illustrato in che modo Backup gateway si connette alle macchine virtuali:



Per scaricare il software Backup gateway, segui la procedura perUtilizzo di gateway.

Per informazioni sugli endpoint VPC (Virtual Private Cloud), consulta AWS Backup e connettività. AWS PrivateLink

Backup gateway è dotato di una propria API che viene gestita separatamente dall'API AWS Backup . Per visualizzare un elenco di azioni API Backup gateway, consulta Operazioni di Backup gateway. Per visualizzare un elenco dei tipi di dati dell'API Backup gateway, consulta Tipi di dati di Backup gateway.

Endpoints

Gli utenti esistenti che attualmente utilizzano un endpoint pubblico e che desiderano passare a un endpoint VPC (Virtual Private Cloud), possono creare un nuovo gateway con un endpoint VPC utilizzando AWS PrivateLink, associare l'hypervisor esistente al gateway e quindi eliminare il gateway contenente l'endpoint pubblico.

Configurazione dell'infrastruttura per utilizzare Backup gateway

Backup gateway richiede le seguenti configurazioni di rete, firewall e hardware per il backup e il ripristino delle macchine virtuali.

Configurazione della rete

Backup gateway richiede determinate porte per essere abilitato a questa operazione. Consentire le seguenti porte:

1. TCP 443 in uscita

- Origine: Backup gateway
- Destinazione: AWS
- Utilizzo: consente la comunicazione con il gateway di Backup AWS.

2. TCP 80 in entrata
   - Fonte: l'host che usi per connetterti al AWS Management Console
   - Destinazione: Backup gateway
   - Utilizzo: da sistemi locali per ottenere la chiave di attivazione di Backup gateway. La porta 80 viene utilizzata solo durante l'attivazione del gateway di Backup. AWS Backup non richiede che la porta 80 sia accessibile al pubblico. Il livello di accesso richiesto alla porta 80 dipende dalla configurazione di rete. Se si attiva il gateway da AWS Management Console, l'host da cui ci si connette alla console deve avere accesso alla porta 80 del gateway.
3. UDP 53 in uscita
   - Origine: Backup gateway
   - Destinazione: server DNS (Domain Name Service)
   - Utilizzo: consente a Backup gateway di comunicare con il DNS.
4. TCP 22 in uscita
   - Origine: Backup gateway
   - Destinazione: AWS Support
   - Utilizzo: consente di accedere AWS Support al gateway per aiutarti a risolvere i problemi. Non è necessario aprire questa porta per il normale funzionamento del gateway, ma deve essere aperta per la risoluzione dei problemi.
5. UDP 123 in uscita
   - Origine: client NTP
   - Destinazione: server NTP
   - Utilizzo: utilizzato dai sistemi locali per sincronizzare l'ora della macchina virtuale con quella dell'host.
6. TCP 443 in uscita
   - Origine: Backup gateway
   - Destinazione: VMware vCenter
   - Utilizzo: consente a Backup gateway di comunicare con VMware vCenter.
7. TCP 443 in uscita

- Origine: Backup gateway
- Destinazione: host ESXi
- Utilizzo: consente a Backup gateway di comunicare con host ESXi.

8. TCP 902 in uscita
   - Origine: Backup gateway
   - Destinazione: host ESXi VMware
   - Utilizzo: utilizzato per il trasferimento di dati tramite Backup gateway.

Le porte di cui sopra sono necessarie per il gateway di Backup. Creazione di un AWS Backup endpoint VPCPer ulteriori informazioni su come configurare gli endpoint Amazon VPC per. AWS Backup

Configurazione del firewall

Il gateway di Backup richiede l'accesso ai seguenti endpoint di servizio con Amazon Web Services cui comunicare. Se si utilizza un firewall o un router per filtrare o limitare il traffico di rete, è necessario configurare il firewall e/o il router affinché consentano questi endpoint di servizio per le comunicazioni in uscita ad AWS. L'uso di un proxy HTTP tra il Backup gateway e i punti di servizio non è supportato.

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

Configurazione del gateway per più NIC in VMware

È possibile mantenere reti separate per il traffico interno ed esterno collegando più connessioni di interfaccia di rete virtuale (NIC) al gateway e quindi indirizzando il traffico interno (dal gateway all'hypervisor) e il traffico esterno (gateway to) separatamente. AWS

Per impostazione predefinita, le macchine virtuali connesse al AWS Backup gateway dispongono di una scheda di rete (). `eth0` Questa rete include l'hypervisor, le macchine virtuali e il gateway di rete (Backup gateway) che comunica con la più ampia rete Internet.

Di seguito è riportato un esempio di configurazione con più interfacce di rete virtuali:

```
            eth0:
            - IP: 10.0.3.83
            - routes: 10.0.3.0/24

            eth1:
            - IP: 10.0.0.241
            - routes: 10.0.0.0/24
            - default gateway: 10.0.0.1
```

- In questo esempio, la connessione è stabilita a un hypervisor con IP`10.0.3.123`, il gateway utilizzerà `eth0` poiché l'IP dell'hypervisor fa parte del blocco `10.0.3.0/24`
- Per connettersi a un hypervisor con IP `10.0.0.234`, il gateway utilizzerà `eth1`
- Per connettersi a un IP esterno alle reti locali (ad esempio, `34.193.121.211`), il gateway ripristinerà il gateway predefinito, `10.0.0.1`, che si trova nel blocco `10.0.0.0/24` e quindi attraverserà `eth1`.

La prima sequenza per aggiungere una scheda di rete avviene nel client vSphere:

1. Nel client VMware vSphere, apri il menu contestuale (con un clic del pulsante destro del mouse) per la macchina virtuale del gateway e scegli Modifica impostazioni.
2. Nella scheda Hardware virtuale della finestra di dialogo Proprietà macchina virtuale, apri il menu Aggiungi nuovo dispositivo e seleziona Scheda di rete per aggiungere una nuova scheda di rete.
3.
   a. Espandi i dettagli della nuova rete per configurare la nuova scheda.
   b. Assicurati che sia selezionata l'opzione Connetti all'accensione.
   c. Per Tipo di scheda, consulta Tipi di schede di rete nella documentazione di ESXi e vCenter Server.
4. Fai clic su OK per salvare le nuove impostazioni della scheda di rete.

La sequenza successiva di passaggi per configurare un adattatore aggiuntivo viene eseguita nella console del AWS Backup gateway (si noti che questa non è la stessa interfaccia della console di AWS gestione in cui vengono gestiti i backup e altri servizi).

Dopo che la nuova scheda di interfaccia di rete è stata aggiunta alla VM del gateway, procedi come descritto di seguito:

- Passa a `Command Prompt` e accendi i nuovo adattatori

- Configura gli IP statici per ogni nuova NIC
- Imposta la NIC preferita come predefinita

A tale scopo:

1. Nel client VMware vSphere, selezionare la macchina virtuale del gateway e avviare Web Console per accedere alla console locale del gateway di Backup.
    - Per ulteriori informazioni sull'accesso a una console locale, consulta Accesso alla console locale del gateway con VMware ESXi
2. Chiudi il prompt dei comandi e passa a Configurazione di rete > Configura IP statico, quindi segui le istruzioni di configurazione per aggiornare la tabella di routing.
    a. Assegna un IP statico all'interno della sottorete della scheda di rete.
    b. Configura una maschera di rete.
    c. Immetti l'indirizzo IP del gateway predefinito. Questo è il gateway di rete che si connette a tutto il traffico all'esterno alla rete locale.
3. Seleziona Imposta adattatore predefinito per designare l'adattatore che verrà connesso al cloud come dispositivo predefinito.
4. Tutti gli indirizzi IP per il gateway possono essere visualizzati nella console locale e nella pagina di riepilogo della VM in VMware vSphere.

Requisiti hardware

Devi poter dedicare le seguenti risorse minime su un host di macchina virtuale per il Backup gateway:

- 4 processori virtuali
- 8 GiB di RAM riservata

Autorizzazioni VMware

Questa sezione elenca le autorizzazioni VMware minime richieste per l'utilizzo. AWS Backup gateway Queste autorizzazioni sono necessarie per consentire a Backup gateway di rilevare, eseguire il backup e ripristinare le macchine virtuali.

Per utilizzare Backup gateway con VMware Cloud™ on AWS o VMware Cloud™ on AWS Outposts, è necessario utilizzare l'utente amministratore predefinito `cloudadmin@vmc.local` o assegnare il CloudAdmin ruolo al proprio utente dedicato.

Per utilizzare Backup gateway con macchine virtuali locali VMware, crea un utente dedicato con le autorizzazioni elencate di seguito.

Globale

- Disabilita metodi
- Abilita metodi
- Licenze
- Log eventi
- Gestisci attributi personalizzati
- Imposta attributi personalizzati

Assegnazione tag vSphere

- Assegna o annulla l'assegnazione di tag vSphere

DataStore

- Alloca spazio
- Sfoglia datastore
- Configura datastore (per datastore vSAN)
- Operazioni sui file di basso livello
- Aggiorna file della macchina virtuale

Host

- Configurazione
  - Impostazioni avanzate
  - Configurazione delle partizioni di storage

Cartella

- Crea cartella

Rete

- Assegna rete

Gruppo dvPort

- Crea
- Eliminazione

Risorsa

- Assegna macchina virtuale a pool di risorse

Macchina virtuale

- Modificare la configurazione
  - Acquisisci leasing del disco
  - Aggiungi disco esistente
  - Aggiungi nuovo disco
  - Configurazione avanzata
  - Modificare le impostazioni dell'
  - Configura dispositivo raw
  - Modifica impostazioni dispositivo
  - Rimuovi disco
  - Imposta annotazione
  - Attiva/disattiva rilevamento delle modifiche del disco
- Modifica inventario
  - Crea da esistente
  - Crea nuovo
  - Registrati

  - Rimuovi
  - Annulla registrazione
- Interazione
  - Spegnimento
  - Accensione
- Provisioning
  - Consenti accesso al disco
  - Consenti accesso del disco in sola lettura
  - Consenti download della macchina virtuale
- Gestione snapshot
  - Crea snapshot
  - Rimuovi snapshot
  - Ripristina snapshot

Utilizzo di gateway

Per eseguire il backup e il ripristino delle macchine virtuali (VM) utilizzando AWS Backup, è necessario prima installare un gateway di Backup. Un gateway è un software sotto forma di modello OVF (Open Virtualization Format) che collega Amazon Web Services Backup all'hypervisor, consentendogli di rilevare automaticamente le macchine virtuali e consentendoti di eseguirne il backup e il ripristino.

Un singolo gateway può eseguire fino a 4 processi di backup o ripristino contemporaneamente. Per eseguire più di 4 processi contemporaneamente, occorre creare più gateway e associali all'hypervisor.

Creazione di un gateway

Per creare un gateway:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, nella sezione Risorse esterne, scegli Gateway.
3. Selezionare Create gateway (Crea gateway).
4. Nella sezione Configura gateway, segui queste istruzioni per scaricare e distribuire il modello OVF.

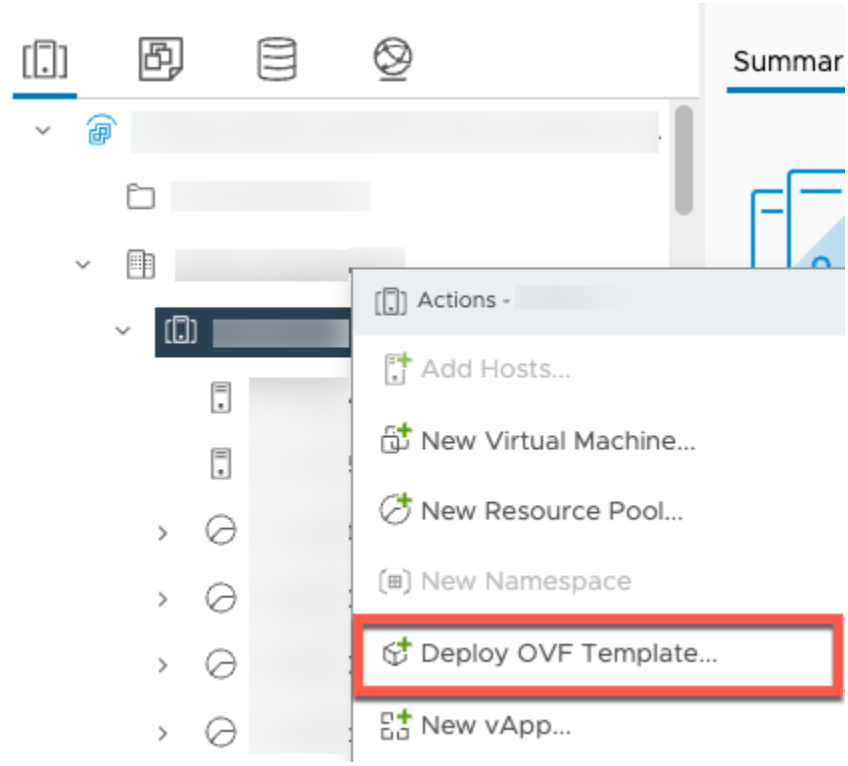
Download del software VMware

Connessione dell'hypervisor

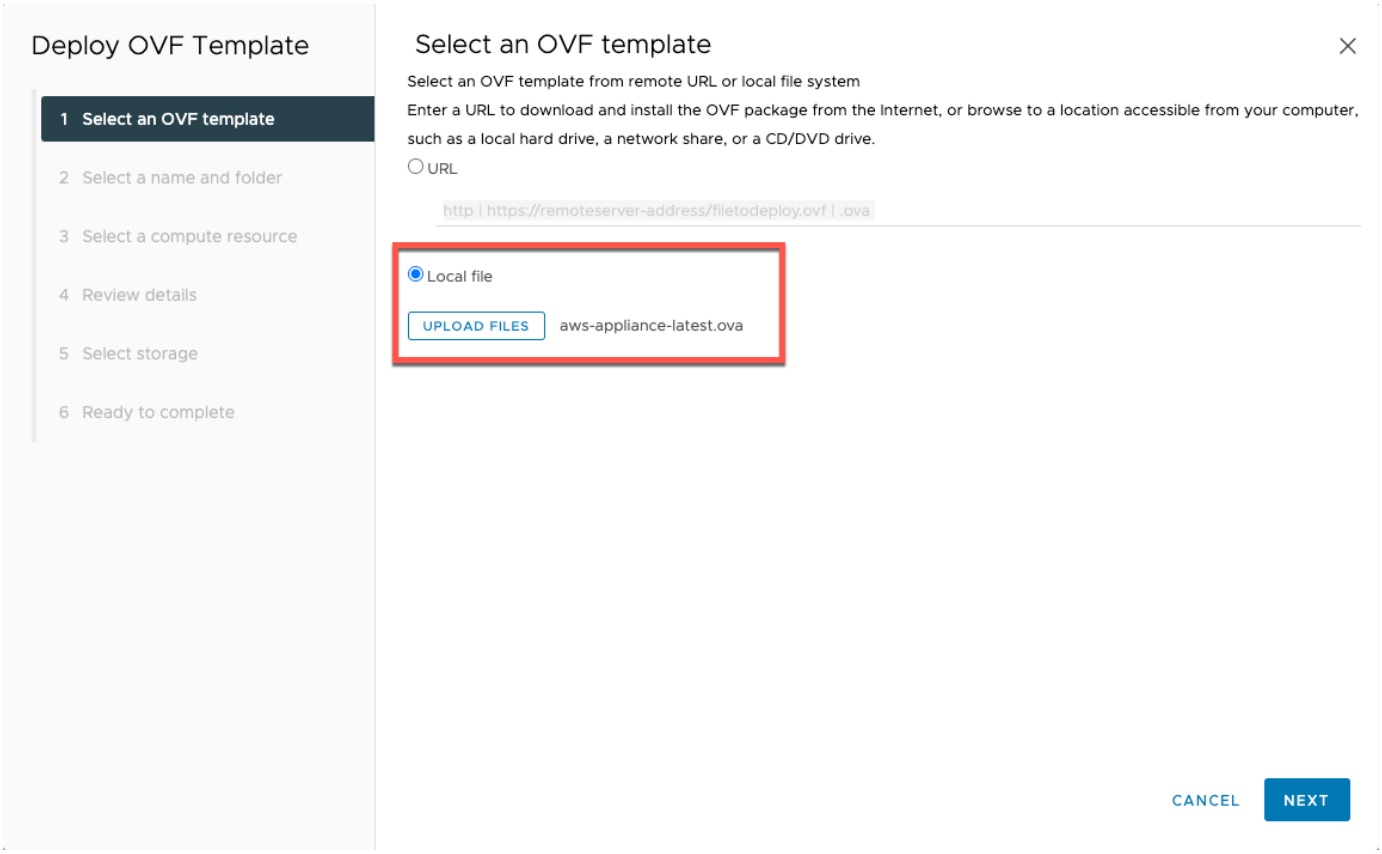
I gateway si connettono AWS Backup all'hypervisor in modo da poter creare e archiviare backup delle macchine virtuali. Per configurare il gateway su VMware ESXi, scarica il modello OVF. Il download può richiedere circa 10 minuti.

Al termine, procedi con i seguenti passaggi:

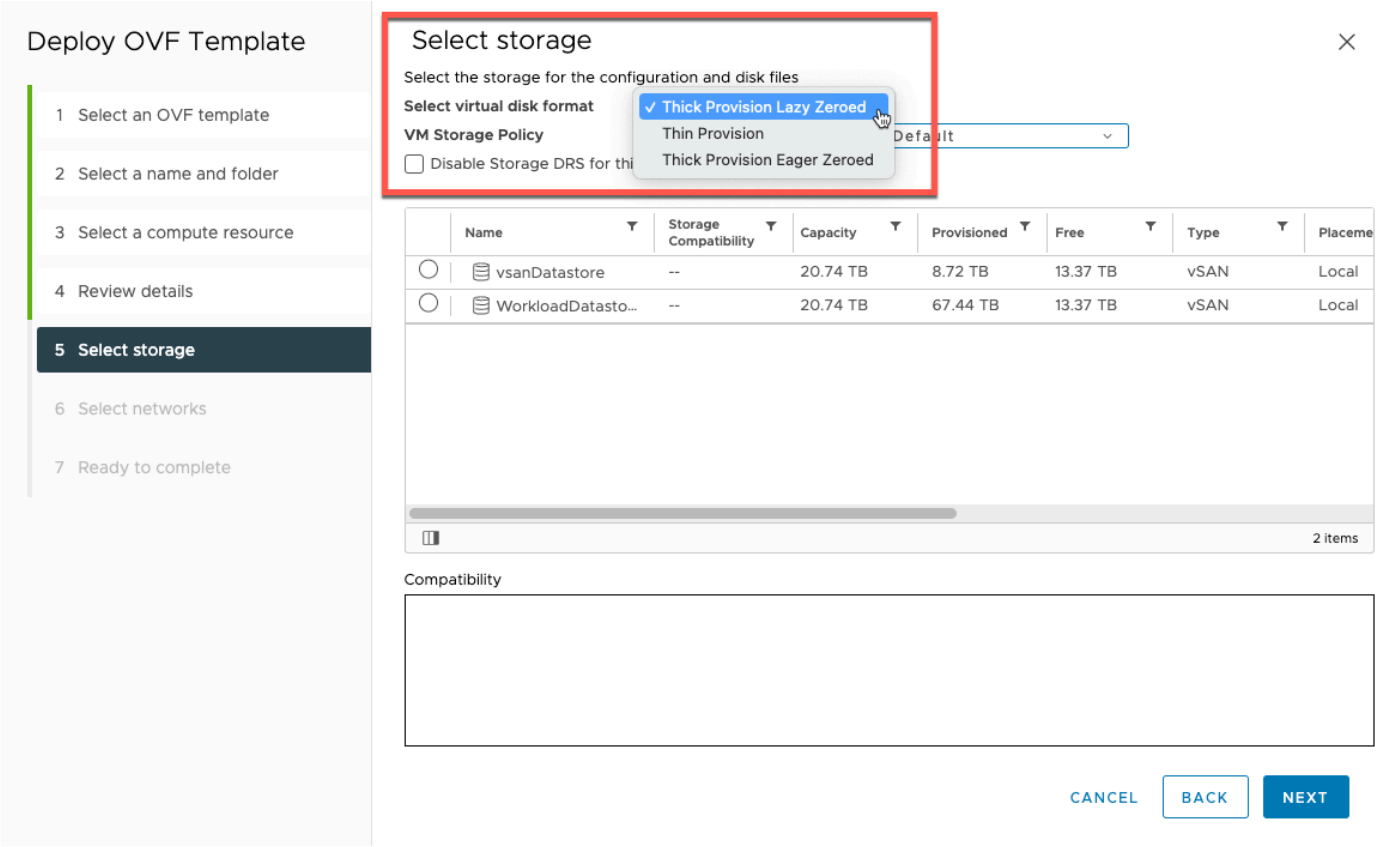
1. Esegui la connessione all'hypervisor della macchina virtuale utilizzando VMware vSphere.
2. Fai clic con il pulsante destro del mouse su un oggetto principale di una macchina virtuale e seleziona Implementa modello OVF.



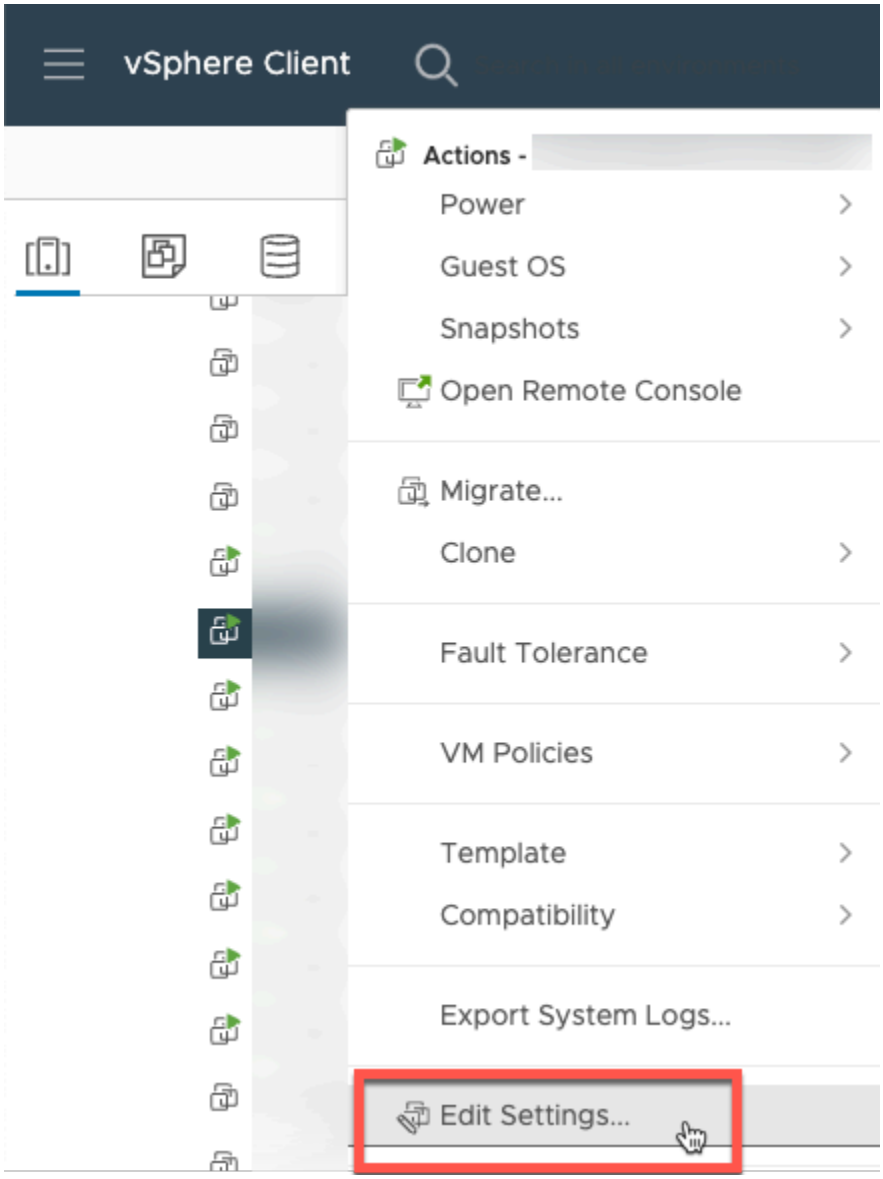
3. Scegli File locale e carica il aws-appliance-latestfile.ova che hai scaricato.



4. Segui i passaggi della procedura di implementazione guidata per distribuirlo. Nella pagina Seleziona uno storage, seleziona il formato del disco virtuale Thick Provision Lazy Zeroed.

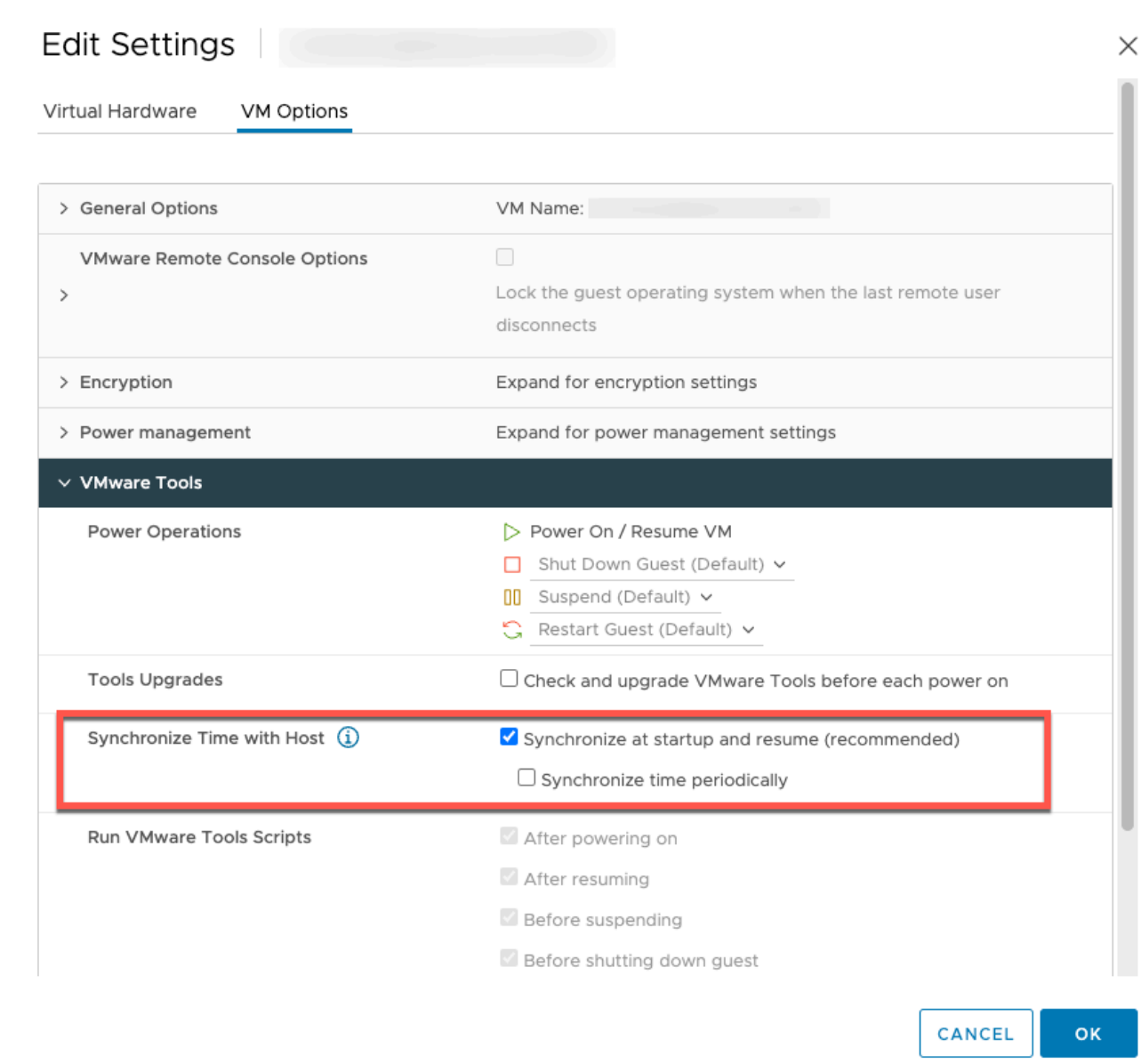


5. Dopo aver distribuito l'OVF, fai clic con il pulsante destro del mouse sul gateway e scegli Modifica impostazioni.

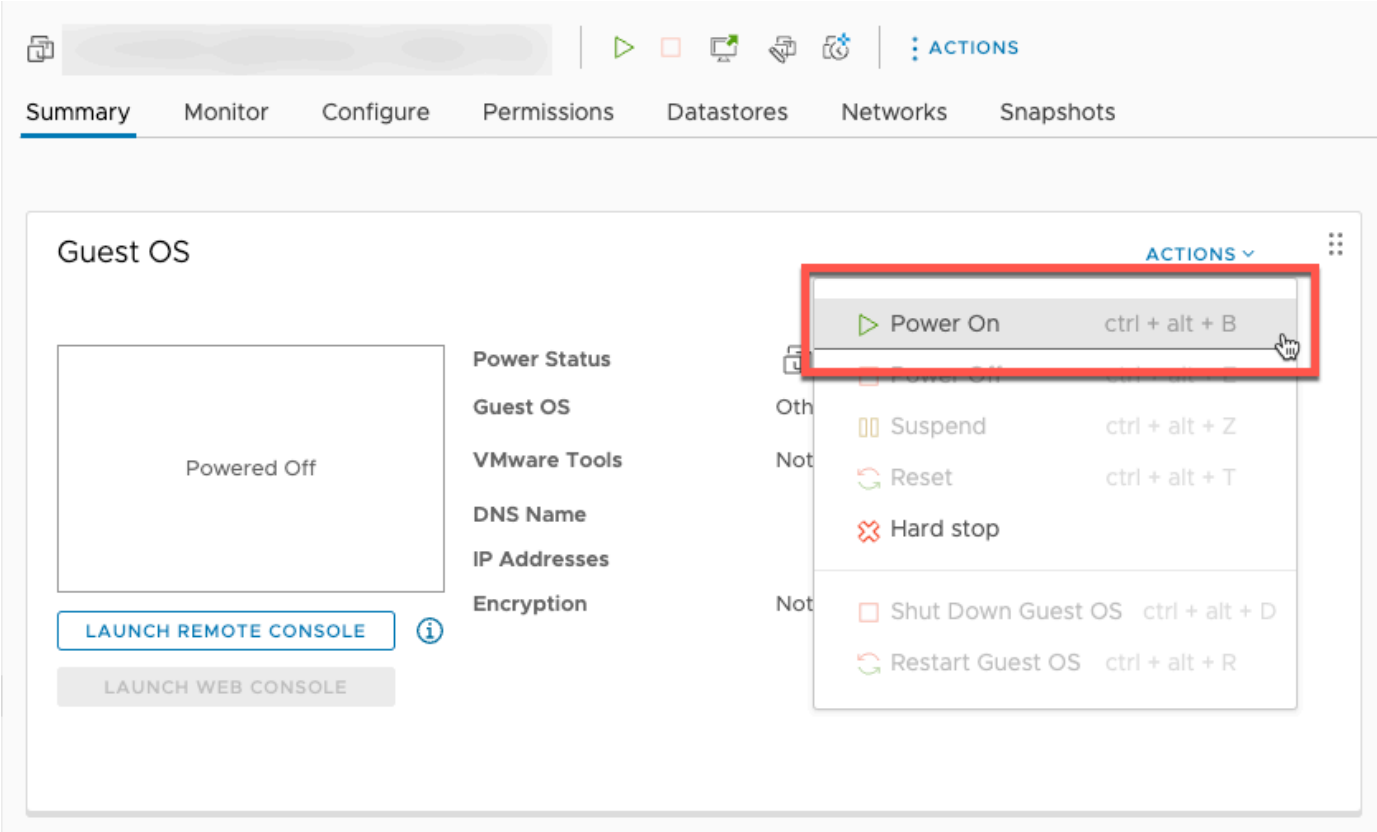


a. In Opzioni VM, passa a Strumenti VM.

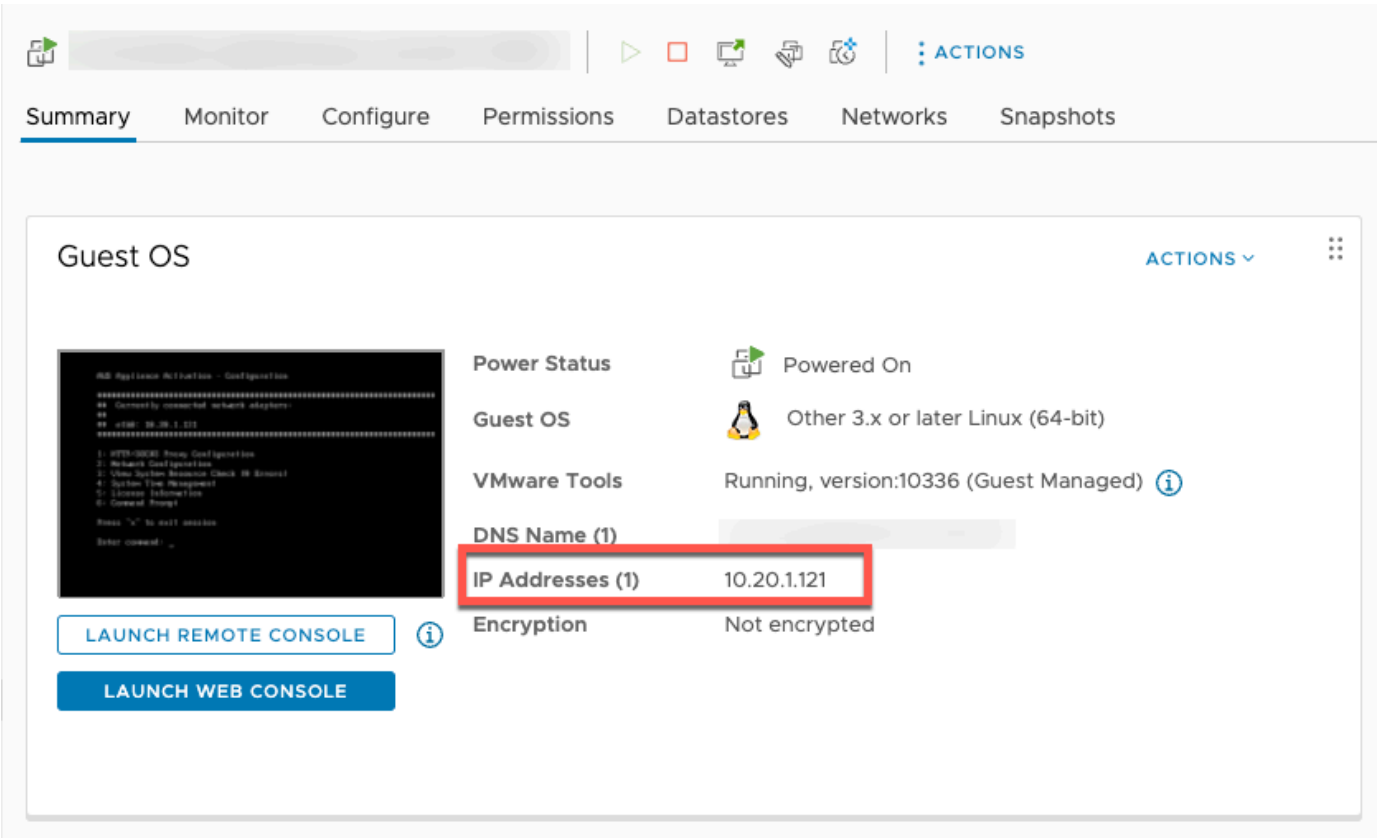
b. Assicurati che l'opzione Sincronizza ora con l'host sia impostata su Sincronizza all'avvio e riprendi.



6. Accendi la macchina virtuale selezionando “Accendere” dal menu Azioni.



7. Copia l'indirizzo IP dal riepilogo della VM e inseriscilo di seguito.



Dopo aver scaricato il software VMWare, completa la seguente procedura:

1. Nella sezione Connessione gateway, digita l'indirizzo IP del gateway.
   a. Per trovare questo indirizzo IP, passa a vSphere Client.
   b. Seleziona il gateway nella scheda Riepilogo.
   c. Copia l'indirizzo IP e incollalo nella barra di testo della AWS Backup console.
2. Nella sezione Impostazioni gateway
   a. Digita un nome gateway.
   b. Verifica la AWS regione.
   c. Scegli se l'endpoint è accessibile pubblicamente o è ospitato sul cloud privato virtuale (VPC).
   d. A seconda dell'endpoint scelto, inserisci il nome DNS dell'endpoint VPC.

      Per ulteriori informazioni, consulta Creazione di un endpoint VPC.
3. [Facoltativo] Nella sezione Tag gateway, puoi assegnare tag inserendo la chiave e il valore opzionale. Per aggiungere più tag, fai clic su Aggiungi un altro tag.
4. Per completare il processo, fai clic su Crea gateway. Viene visualizzata la pagina dei dettagli del gateway.

Modifica o eliminazione di un gateway

Per modificare o eliminare un gateway:

1. Nel riquadro di navigazione a sinistra, nella sezione Risorse esterne, scegli Gateway.
2. Nella sezione Gateway, scegli un gateway in base al suo Nome gateway.
3. Per modificare il nome del gateway, scegli Modifica.
4. Per eliminare il gateway, scegli Elimina, quindi seleziona Elimina gateway.

   Non è possibile riattivare un gateway eliminato. Se desideri connetterti nuovamente all'hypervisor, segui la procedura in Creazione di un gateway.
5. Per connetterti a un hypervisor, nella sezione Hypervisor connesso, scegli Connetti.

   Ogni gateway si connette a un singolo hypervisor. Tuttavia, puoi connettere più gateway allo stesso hypervisor per aumentare la larghezza di banda tra di essi oltre quella del primo gateway.

6. Per assegnare, modificare o gestire tag, nella sezione Tag, scegli Gestisci tag.

Limitazione della larghezza di banda del gateway di backup

> **Note**
>
> Questa funzionalità sarà disponibile sui nuovi gateway distribuiti dopo il 15 dicembre 2022. Per i gateway esistenti, questa nuova funzionalità sarà disponibile tramite un aggiornamento software automatico entro il 30 gennaio 2023. Per aggiornare manualmente il gateway alla versione più recente, utilizzare il comando. AWS CLI `UpdateGatewaySoftwareNow`

È possibile limitare la velocità di caricamento dal gateway AWS Backup al controllo della quantità di larghezza di banda di rete utilizzata dal gateway. Per impostazione predefinita, un gateway attivato non ha limiti di velocità.

È possibile configurare una pianificazione relativa al limite della velocità di larghezza di banda utilizzando la AWS Backup console o utilizzando l'API tramite (). AWS CLI `PutBandwidthRateLimitSchedule` Quando utilizzi una pianificazione del limite di velocità della larghezza di banda, puoi configurare i limiti in modo che cambino automaticamente durante il giorno o la settimana.

La limitazione di velocità della larghezza di banda funziona bilanciando la velocità di trasmissione effettiva di tutti i dati caricati, mediata su ogni secondo. Sebbene sia possibile che i caricamenti superino brevemente il limite di velocità della larghezza di banda per un microsecondo o millisecondo specifico, in genere ciò non comporta picchi elevati per periodi di tempo più lunghi.

Puoi aggiungere fino a un massimo di 20 intervalli. Il valore massimo per la velocità di caricamento è di 8.000.000 (milioni) di megabyte al secondo (Mbps).

Visualizza e modifica la pianificazione del limite di velocità di larghezza di banda per il gateway utilizzando la console. AWS Backup

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

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

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.

2. Nel riquadro di navigazione a sinistra, selezionare Gateways (Gateway). Nel riquadro Gateway, i gateway vengono visualizzati per nome. Fai clic sul pulsante di opzione accanto al nome del gateway che desideri gestire.
3. Dopo aver selezionato un pulsante di opzione, è possibile fare clic sul menu a discesa Azione. Fai clic su Azioni, quindi su Modifica della pianificazione del limite di velocità della larghezza di banda. Viene visualizzata la pianificazione corrente. Per impostazione predefinita, un gateway nuovo o non modificato non ha limiti di velocità della larghezza di banda definiti.

> **Note**
>
> Puoi anche fare clic su Gestione della pianificazione nella pagina dei dettagli del gateway per accedere alla pagina di modifica della larghezza di banda.

4. (Facoltativo) Scegli Aggiungi intervallo per aggiungere un nuovo intervallo configurabile alla pianificazione. Per ogni intervallo, inserisci le seguenti informazioni:

   a. Giorni della settimana: seleziona il giorno o i giorni ricorrenti in cui desideri applicare l'intervallo. Se questa opzione è selezionata, i giorni verranno visualizzati sotto il menu a discesa. Puoi rimuoverli facendo clic sulla X accanto al giorno.

   b. Ora di avvio: inserisci l'ora di inizio per l'intervallo di larghezza di banda, utilizzando il formato a 24 ore HH:MM. L'ora è espressa in UTC (Universal Coordinated Time.

      Nota: l' bandwidth-rate-limit intervallo inizia all'inizio del minuto specificato.

   c. Ora di fine: inserisci l'ora di fine per l'intervallo di larghezza di banda, utilizzando il formato a 24 ore HH:MM. L'ora è espressa in UTC (Universal Coordinated Time.

      > **Important**
      >
      > L' bandwidth-rate-limit intervallo termina alla fine del minuto specificato. Per pianificare un intervallo che termini alla fine di un'ora, immettere. `59` Per programmare intervalli continui consecutivi, con transizione all'inizio dell'ora, senza interruzioni tra gli intervalli, inserite `59` il minuto finale del primo intervallo. Inserisci `00` per il minuto di inizio dell'intervallo successivo.

   d. Velocità di caricamento: inserisci il limite di velocità di caricamento, in megabit al secondo (Mbps). Il valore minimo è 102 megabyte al secondo (Mbps).

5. (Facoltativo) Ripeti il passaggio precedente come desiderato fino al completamento della pianificazione del limite di velocità della larghezza di banda. Se occorre eliminare un intervallo dalla pianificazione, scegli Rimuovi.

> **Important**
>
> Gli intervalli del limite di velocità della larghezza di banda non possono sovrapporsi. L'ora di inizio di un intervallo deve essere successivo all'ora di fine di un intervallo precedente e precedente all'ora di inizio di un intervallo successivo; l'ora di fine deve essere precedente all'ora di inizio dell'intervallo successivo.

6. Al termine, fai clic sul pulsante Salva modifiche.

Visualizzare e modificare la pianificazione del limite di velocità della larghezza di banda per il gateway utilizzando AWS CLI.

L'azione `GetBandwidthRateLimitSchedule` può essere utilizzata per visualizzare la pianificazione della limitazione della larghezza di banda per un gateway specifico. Se non è stata impostata alcuna pianificazione, la pianificazione sarà un elenco vuoto di intervalli. Ecco un esempio di utilizzo di AWS CLI per recuperare la pianificazione della larghezza di banda di un gateway:

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

Per modificare la pianificazione della limitazione della larghezza di banda di un gateway, puoi utilizzare l'azione `PutBandwidthRateLimitSchedule`. Tieni presente che puoi aggiornare la pianificazione di un gateway solo nel suo insieme, anziché modificare, aggiungere o rimuovere singoli intervalli. La chiamata di questa azione sovrascriverà la pianificazione precedente della limitazione della larghezza di banda del gateway.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

Utilizzo degli hypervisor

Al terminCreazione di un gateway, è possibile collegarlo a un hypervisor per consentirne l'utilizzo con le macchine virtuali gestite AWS Backup da tale hypervisor. Ad esempio, l'hypervisor per le VM

VMware è VMware vCenter Server. Assicurati che l'hypervisor sia configurato con le autorizzazioni necessarie per AWS Backup.

Aggiunta di un hypervisor

Per aggiungere un hypervisor:

1. Nel riquadro di navigazione a sinistra, nella sezione Risorse esterne, scegli Hypervisor.
2. Scegli Aggiungi hypervisor.
3. Nella sezione Impostazioni dell'hypervisor, digita un Nome hypervisor.
4. Per Host del server vCenter, utilizza il menu a discesa per selezionare Indirizzo IP o Nome dominio completo. Digita il valore corrispondente.
5. AWS Backup Per consentire l'individuazione delle macchine virtuali sull'hypervisor, inserisci il nome utente e la password dell'hypervisor.
6. Esegui la crittografia della password. Puoi specificare questa crittografia selezionando una particolare chiave KMS gestita dal servizio o una chiave KMS gestita dal cliente utilizzando il menu a discesa o scegliendo Crea chiave KMS. Se non selezioni una chiave specifica, AWS Backup eseguirà la crittografia della password utilizzando una chiave di proprietà del servizio.
7. Nella sezione Gateway di connessione, utilizza l'elenco a discesa per specificare quale gateway connettere all'hypervisor.
8. Scegli Test della connessione gateway per verificare gli input precedenti.
9. Facoltativamente, nella sezione Tag dell'hypervisor, puoi assegnare tag all'hypervisor scegliendo Aggiungi nuovo tag.
10. Mappatura dei tag VMware opzionale: puoi aggiungere fino a 10 tag VMware attualmente utilizzati sulle macchine virtuali per generare tag. AWS
11. Nel pannello di impostazione del gruppo di log, puoi scegliere di integrarti con Amazon CloudWatch Logs per mantenere i log del tuo hypervisor (verranno applicati i prezzi standard di CloudWatch Logs in base all'utilizzo). Ogni hypervisor può appartenere a un gruppo di log.
    a. Se non hai ancora creato un gruppo di log, seleziona il pulsante di opzione Crea un nuovo gruppo di log. L'hypervisor che viene modificato verrà associato a questo gruppo di log.
    b. Se in precedenza hai creato un gruppo di log per un hypervisor diverso, puoi utilizzare tale gruppo di log per questo hypervisor. Seleziona Usa un gruppo di log esistente.
    c. Se non desideri effettuare la registrazione, seleziona Disattiva la CloudWatch registrazione.
12. Scegli Aggiungi hypervisor per accedere alla relativa pagina dei dettagli.

> **Tip**
>
> Puoi utilizzare Amazon CloudWatch Logs (vedi il passaggio 11 sopra) per ottenere informazioni sul tuo hypervisor, incluso il monitoraggio degli errori, la connessione di rete tra il gateway e l'hypervisor e le informazioni sulla configurazione della rete. Per informazioni sui gruppi di CloudWatch log, consulta Working with Log Groups and Log Streams nella Amazon CloudWatch User Guide.

Visualizzazione di macchine virtuali gestite da un hypervisor

Per visualizzare le macchine virtuali su un hypervisor:

1. Nel riquadro di navigazione a sinistra, nella sezione Risorse esterne, scegli Hypervisor.
2. Nella sezione Hypervisor, scegli un hypervisor in base al Nome hypervisor per accedere alla relativa pagina dei dettagli.
3. Nella sezione Riepilogo hypervisor, scegli la scheda Macchine virtuali.
4. Nella sezione Macchine virtuali connesse, viene compilato automaticamente un elenco di macchine virtuali.

Visualizzazione dei gateway connessi a un hypervisor

Per visualizzare i gateway connessi all'hypervisor:

1. Scegli la scheda Gateway.
2. Nella sezione Gateway connessi, viene compilato automaticamente un elenco di gateway.

Connessione di un hypervisor a gateway aggiuntivi

Le velocità di backup e ripristino potrebbero essere limitate dalla larghezza di banda della connessione tra il gateway e l'hypervisor. Puoi aumentare queste velocità collegando uno o più gateway aggiuntivi all'hypervisor. Per eseguire questa operazione nella sezione Gateway connessi, procedi come segue:

1. Scegli Connetti.
2. Seleziona un altro gateway utilizzando il menu a discesa. In alternativa, scegli Crea gateway per creare un nuovo gateway.

3. Scegli Connetti.

Modifica della configurazione di un hypervisor

Se non utilizzi la funzionalità Test della connessione gateway, puoi aggiungere un hypervisor con un nome utente o una password errati. In tal caso, lo stato di connessione dell'hypervisor è sempre `Pending`. In alternativa, puoi ruotare il nome utente o la password per accedere all'hypervisor. Aggiorna queste informazioni utilizzando la seguente procedura:

Per modificare un hypervisor già aggiunto:

1. Nel riquadro di navigazione a sinistra, nella sezione Risorse esterne, scegli Hypervisor.
2. Nella sezione Hypervisor, scegli un hypervisor in base al Nome hypervisor per accedere alla relativa pagina dei dettagli.
3. Scegli Modifica.
4. Il pannello superiore è denominato Impostazioni dell'hypervisor.
    a. In Host del server vCenter, puoi anche modificare il nome dominio completo o l'indirizzo IP.
    b. Facoltativamente, inserisci il nome utente e la password dell'hypervisor.
5. Nel pannello di impostazione del gruppo di log, puoi scegliere di integrarti con Amazon CloudWatch per mantenere i log del tuo hypervisor (verranno applicati i CloudWatch prezzi standard in base all'utilizzo). Ogni hypervisor può appartenere a un gruppo di log.
    a. Se non hai ancora creato un gruppo di log, seleziona il pulsante di opzione Crea un nuovo gruppo di log. L'hypervisor che viene modificato verrà associato a questo gruppo di log.
    b. Se in precedenza hai creato un gruppo di log per un hypervisor diverso, puoi utilizzare tale gruppo di log per questo hypervisor. Seleziona Usa un gruppo di log esistente.
    c. Se non desideri effettuare la registrazione, seleziona CloudWatch Disattiva registrazione.

> **Tip**
>
> Puoi utilizzare Amazon CloudWatch Logs (vedi il passaggio 5 sopra) per ottenere informazioni sul tuo hypervisor, incluso il monitoraggio degli errori, la connessione di rete tra il gateway e l'hypervisor e le informazioni sulla configurazione della rete. Per informazioni sui gruppi di CloudWatch log, consulta Working with Log Groups and Log Streams nella Amazon CloudWatch User Guide.

Per aggiornare un hypervisor a livello di codice, utilizza il comando CLI update-hypervisor e la chiamata API. UpdateHypervisor

Eliminazione della configurazione di un hypervisor

Se è necessario rimuovere un hypervisor già aggiunto, rimuovi la configurazione dell'hypervisor e aggiungine un'altra. Questa operazione di rimozione si applica alla configurazione per la connessione all'hypervisor. L'hypervisor non viene eliminato.

Per eliminare la configurazione per la connessione a un hypervisor già aggiunto:

1. Nel riquadro di navigazione a sinistra, nella sezione Risorse esterne, scegli Hypervisor.
2. Nella sezione Hypervisor, scegli un hypervisor in base al Nome hypervisor per accedere alla relativa pagina dei dettagli.
3. Scegli Rimuovi, quindi Rimuovi hypervisor.
4. Facoltativo: sostituisci la configurazione dell'hypervisor rimossa utilizzando la procedura per Aggiunta di un hypervisor.

Comprensione dello stato dell'hypervisor

Di seguito vengono descritti tutti i possibili stati dell'hypevisor e, se applicabile, i passaggi di correzione. Lo stato `ONLINE` è lo stato normale dell'hypervisor. L'hypervisor deve avere questo stato per tutto o la maggior parte del tempo in cui viene utilizzato per il backup e il ripristino delle VM gestite dall'hypervisor.

Stati dell'hypervisor

Stato	Significato e correzione
`ONLINE`	È stato aggiunto un hypervisor a AWS Backup cui è stato associato un gateway ed è possibile connettersi a tale gateway tramite la rete per eseguire il backup e il ripristino delle macchine virtuali gestite dall'hypervisor. Puoi eseguire backup on demand e pianificati di tali macchine virtuali in qualsiasi momento.
`PENDING`	Hai aggiunto un hypervisor a ma: AWS Backup

Stato	Significato e correzione
	• Non è associato ad alcun gateway oppure • È associato a uno o più gateway, ma tutti questi gateway sono stati eliminati o non sono altrimenti attivi. Per modificare lo stato di un hypervisor da `PENDING` a `ONLINE`, crea un gateway e connetti l'hypervisor a tale gateway.
`OFFLINE`	Hai aggiunto un hypervisor AWS Backup e lo hai associato a un gateway, ma il gateway non può connettersi all'hypervisor tramite la rete. Per modificare lo stato di un hypervisor da `OFFLINE` a `ONLINE`, verifica la correttezza della configurazione di rete. Se il problema persiste, verifica che l'indirizzo IP o il nome dominio completo dell'hypervisor siano corretti. Se sono errati, aggiungi nuovamente l'hypervisor utilizzando le informazioni corrette e verifica la connessione gateway.
`ERROR`	Hai aggiunto un hypervisor AWS Backup e lo hai associato a un gateway, ma il gateway non può comunicare con l'hypervisor. Per modificare lo stato di un hypervisor da `ERROR` a `ONLINE`, verifica che il nome utente e la password dell'hypervisor siano corretti. Se sono errati, modifica la configurazione dell'hypervisor.

Fasi successive

Per eseguire il backup delle macchine virtuali sull'hypervisor, consulta Backup di macchine virtuali.

Backup di macchine virtuali

Al termine di Aggiunta di un hypervisor, Backup gateway elenca automaticamente le macchine virtuali. Puoi visualizzare le tue macchine virtuali scegliendo Hypervisor o Macchine virtuali nel riquadro di navigazione a sinistra.

- Scegli Hypervisor per visualizzare solo le macchine virtuali gestite da un hypervisor specifico. Con questa vista, puoi utilizzare una macchina virtuale alla volta.
- Scegli Macchine virtuali per visualizzare tutte le macchine virtuali su tutti gli hypervisor che hai aggiunto al tuo. Account AWS Con questa vista, puoi utilizzare alcune o tutte le tue macchine virtuali su più hypervisor.

A prescindere dalla vista scelta, per eseguire un'operazione di backup su una macchina virtuale specifica, scegli il Nome macchina virtuale per aprire la relativa pagina dei dettagli. La pagina dei dettagli della macchina virtuale è il punto di partenza per le procedure riportate di seguito.

Creazione di un backup on demand di una macchina virtuale

Un backup on demand è un backup completo una tantum avviato manualmente. Puoi utilizzare i backup su richiesta per testare le funzionalità AWS Backup di backup e ripristino.

Per creare un backup on demand di una macchina virtuale:

1. Scegliere Create on-demand backup (Crea backup on demand).
2. Configura un backup on demand.
3. Scegliere Create on-demand backup (Crea backup on demand).
4. Verifica quando lo stato del processo di backup è `Completed`. Nel riquadro di navigazione a sinistra, scegli Processi.
5. Scegli l'ID del processi di backup per visualizzare le informazioni sul processo di backup, come le Dimensioni del backup e il tempo trascorso tra la Data di creazione e la Data di completamento.

Backup VM incrementali

Le versioni più recenti di VMware contengono una funzionalità chiamata Changed Block Tracking, che tiene traccia dei blocchi di storage delle macchine virtuali mentre cambiano nel tempo. Quando si esegue AWS Backup il backup di una macchina virtuale, AWS Backup tenta di utilizzare i dati

CBT, se disponibili. AWS Backup utilizza i dati CBT per accelerare il processo di backup; senza dati CBT, i processi di backup sono spesso più lenti e utilizzano più risorse dell'hypervisor. Il backup può comunque essere completato con successo anche quando i dati CBT non sono validi o disponibili. Ad esempio, è possibile che i dati CBT non siano validi o disponibili se si verifica un arresto forzato della macchina virtuale o dell'host ESXi.

Nei casi in cui i dati CBT non siano validi o disponibili, lo stato del backup sarà `Successful` con un messaggio. In questi casi, il messaggio indicherà che, in assenza di dati CBT, ha AWS Backup utilizzato il proprio meccanismo proprietario di rilevamento delle modifiche per completare il backup anziché i dati CBT di VMware. I backup successivi tenteranno nuovamente di utilizzare i dati CBT e nella maggior parte dei casi i dati CBT saranno correttamente validi e disponibili. Se il problema persiste, consultare Risoluzione dei problemi di VMware per la procedura di correzione.

Affinché CBT funzioni correttamente, devono essere soddisfatte le seguenti condizioni:

- L'host deve essere ESXi 4.0 o versione successiva
- La macchina virtuale proprietaria dei dischi deve disporre della versione hardware 7 o successiva
- CBT deve essere abilitato per la macchina virtuale (è abilitato per impostazione predefinita)

Per verificare se CBT è abilitato su un disco virtuale:

1. Apri vSphere Client e seleziona una macchina virtuale spenta.
2. Fai clic con il pulsante destro del mouse sulla macchina virtuale e passa a Modifica impostazioni > Opzioni > Avanzate/Generali > Parametri di configurazione.
3. L'opzione `ctkEnabled` deve essere uguale a `True`.

Automatizzazione del backup delle macchine virtuali assegnando risorse a un piano di backup

Un piano di backup è una policy di protezione dei dati definita dall'utente che automatizza la protezione dei dati tra vari servizi AWS e applicazioni di terze parti. Crea innanzitutto il piano di backup specificando la relativa frequenza di backup, il periodo di conservazione, la policy del ciclo di vita e molte altre opzioni. Per creare un piano di backup, consulta il Tutorial sulle nozioni di base.

Dopo aver creato il piano di backup, si assegnano le risorse AWS Backup supportate, incluse le macchine virtuali, a tale piano di backup. AWS Backup offre molti modi per assegnare risorse, tra cui l'assegnazione di tutte le risorse dell'account, incluse o escluse singole risorse specifiche o l'aggiunta di risorse con determinati tag.

Oltre alle funzionalità di assegnazione delle risorse esistenti, il AWS Backup supporto per le macchine virtuali introduce diverse nuove funzionalità che consentono di assegnare rapidamente le macchine virtuali ai piani di backup. Dalla pagina Macchine virtuali, puoi assegnare tag a più macchine virtuali o utilizzare la nuova funzionalità Assegna risorse da pianificare. Utilizza queste funzionalità per assegnare le macchine virtuali già rilevate dal gateway. AWS Backup

Se prevedi di individuare e assegnare altre macchine virtuali in futuro e desideri automatizzare la fase di assegnazione delle risorse per includere tali macchine virtuali future, utilizza la nuova funzionalità Crea assegnazione del gruppo.

Tag VMware

I tag sono coppie chiave-valore che puoi utilizzare per gestire, filtrare e cercare le risorse.

Un tag VMware è costituito da una categoria e da un nome tag. I tag VMware vengono utilizzati per raggruppare le macchine virtuali. Un nome tag è un'etichetta assegnata a una macchina virtuale. Una categoria è una raccolta di nomi tag.

Nei AWS tag, è possibile utilizzare caratteri compresi tra lettere UTF-8, numeri, spazi e caratteri speciali. `+ - = . _ : /`

Se utilizzi tag sulle macchine virtuali, puoi aggiungere fino a 10 tag corrispondenti in AWS Backup per semplificare l'organizzazione. È possibile mappare fino a 10 tag VMware ai tag. AWS Nella AWS Backup console, questi possono essere trovati in La mia organizzazione > Macchine virtuali > AWS tag o tag VMware.

Mappatura dei tag VMware

Se utilizzi tag sulle macchine virtuali, puoi aggiungere fino a 10 tag corrispondenti in AWS Backup per chiarezza e organizzazione aggiuntive. Le mappature si applicano a qualsiasi macchina virtuale sull'hypervisor.

1. Aprire la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nella console, passa a Modifica hypervisor (fai clic su Risorse esterne, Hypervisor, quindi fai clic sul nome dell'hypervisor e seleziona Gestione delle mappature).
3. L'ultimo riquadro, VMware tag mapping, contiene quattro campi di testo in cui è possibile inserire le informazioni dei tag VMware esistenti nei tag corrispondenti. AWS I quattro campi sono VMware tag category, tag name VMware, tag key e tag value (esempio: Category = OS;AWS tag name = Windows; tag key = OS-Windows e tag value = Windows).AWS AWS AWS

4. Dopo aver inserito i valori preferiti, fai clic su Aggiungi mappatura. In caso di errore, puoi fare clic su Rimuovi per eliminare le informazioni inserite.
5. Dopo aver aggiunto una o più mappature, specifica il ruolo IAM che intendi utilizzare per applicare questi tag AWS alle macchine virtuali VMware.

   La policy `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` contiene le autorizzazioni necessarie. Puoi collegare questa policy al ruolo che stai utilizzando (o chiedere a un amministratore di eseguire questa operazione) oppure puoi creare una policy personalizzata per il ruolo in uso.
6. Infine, fai clic su Aggiungi hypervisor o Salva.

La relazione di fiducia dei ruoli IAM deve essere modificata per aggiungere i servizi backup-gateway.amazonaws.com e backup.amazonaws.com. Senza questo servizio, è probabile che si verifichi un errore durante la mappatura dei tag. Per modificare la relazione di fiducia per un ruolo esistente:

1. Accedi alla console IAM.
2. Nel riquadro di navigazione della console, scegli Ruoli.
3. Scegli il nome del ruolo che desideri modificare, quindi seleziona la scheda Relazioni di fiducia nella pagina dei dettagli.
4. In Documento policy, incolla quanto segue:

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

5. Scegli Update Trust Policy (Aggiorna policy di trust).

Per ulteriori dettagli, consulta Modifica della relazione di attendibilità per un ruolo esistente nella Guida di amministrazione di Servizio di directory AWS .

Visualizzazione delle mappature di tag VMware

Nella console di AWS Backup, fai clic su Risorse esterne, Hypervisor, quindi seleziona il collegamento del nome dell'hypervisor per visualizzare le proprietà dell'hypervisor selezionato. Nel riquadro di riepilogo sono presenti quattro schede, l'ultima delle quali è Mappature di tag VMware. Tiene presente che, se non disponi ancora di mappature, verrà visualizzato il messaggio "Nessuna mappatura di tag VMware".

Da qui, è possibile sincronizzare i metadati delle macchine virtuali scoperte dall'hypervisor, copiare le mappature sui propri hypervisor, aggiungere AWS tag mappati ai tag VMware alla selezione di backup di un piano di backup oppure gestire le mappature.

Nella console, per vedere quali tag vengono applicati a una macchina virtuale selezionata, fai clic su Macchine virtuali, nome della macchina virtuale, quindi su Tag AWS o Tag VMware. Puoi visualizzare i tag associati a questa macchina virtuale, nonché gestire i tag.

Assegnazione di macchine virtuali per pianificare l'utilizzo di mappature di tag VMware

Per assegnare le macchine virtuali a un piano di backup utilizzando tag mappati, esegui le operazioni seguenti:

1. Apri la console all'indirizzo https://console.aws.amazon.com/backup. AWS Backup
2. Nella console, passa a Mappature di tag VMware nella pagina dei dettagli dell'hypervisor (fai clic su Risorse esterne, quindi su Hypervisor e seleziona il nome dell'hypervisor).
3. Seleziona la casella di controllo accanto a più tag mappati per assegnarli allo stesso piano di backup.
4. Fai clic su Aggiungi all'assegnazione delle risorse.
5. Scegli un piano di backup esistente dall'elenco a discesa. In alternativa, puoi scegliere Crea un piano di backup per creare un nuovo piano di backup.
6. Fai clic su Conferma. Viene visualizzata la pagina Assegna risorse con campi Migliora la selezione utilizzando i tag con valori precompilati.

Tag VMware che utilizzano il AWS CLI

AWS Backup utilizza la chiamata API `PutHypervisorPropertyMappings`per mappare le proprietà dell'entità dell'hypervisor in locale alle proprietà in. AWS

In, usa l' AWS CLI operazione: `put-hypervisor-property-mappings`

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId \
--vmware-to-aws-tag-mappings list of VMware to AWS tag mappings \
--iam-role-arn arn:aws:iam::account:role/roleName \
--region AWSRegion
--endpoint-url URL
```

Ecco un esempio:

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--vmware-to-aws-tag-mappings VmwareCategory=OS,VmwareTagName=Windows,AwsTagKey=OS-
Windows,AwsTagValue=Windows \
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole \
--region us-east-1
```

Inoltre, puoi utilizzare `GetHypervisorPropertyMappings` per fornire assistenza con le informazioni sulla mappatura delle proprietà. In AWS CLI, utilizzare l'operazione`get-hypervisor-property-mappings`. Di seguito è riportato un modello di esempio:

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

Ecco un esempio:

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Sincronizza i metadati delle macchine virtuali scoperte dall'hypervisor AWS utilizzando API, CLI o SDK

Puoi sincronizzare i metadati delle macchine virtuali. Quando esegui questa operazione, i tag VMware presenti sulla macchina virtuale che fanno parte delle mappature verranno sincronizzati. Inoltre, i tag AWS mappati ai tag VMware presenti sulla macchina virtuale verranno applicati alla risorsa macchina virtuale AWS .

AWS Backup utilizza la chiamata API `StartVirtualMachinesMetadataSync`per sincronizzare i metadati delle macchine virtuali scoperte dall'hypervisor. Per sincronizzare i metadati delle macchine

virtuali individuate dall'hypervisor mediante AWS CLI, utilizza l'operazione `start-virtual-machines-metadata-sync`.

Modello di esempio:

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Esempio:

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Puoi anche utilizzare `GetHypervisor` per fornire informazioni sull'hypervisor, ad esempio host, stato, stato dell'ultima sincronizzazione dei metadati, nonché recuperare l'ultima ora di sincronizzazione dei metadati andata a buon fine. In AWS CLI, utilizzare l'operazione. `get-hypervisor`

Modello di esempio:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Esempio:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Per ulteriori informazioni, consulta la documentazione dell'API VmwareTage VmwareToAwsTagMapping.

Questa funzionalità sarà disponibile sui nuovi gateway distribuiti dopo il 15 dicembre 2022. Per i gateway esistenti, questa nuova funzionalità sarà disponibile tramite un aggiornamento software automatico entro il 30 gennaio 2023. Per aggiornare manualmente il gateway alla versione più recente, usa AWS CLI il comando UpdateGatewaySoftwareNow.

Esempio:

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

Assegnazione di macchine virtuali mediante tag

È possibile assegnare le macchine virtuali attualmente scoperte da AWS Backup, insieme ad altre AWS Backup risorse, assegnando loro un tag che è già stato assegnato a uno dei piani di backup esistenti. Puoi anche creare un nuovo piano di backup e una nuova assegnazione di risorse basata su tag. I piani di backup verificano la presenza di nuove risorse assegnate ogni volta che eseguono un processo di backup.

Per assegnare tag a più macchine virtuali con lo stesso tag:

1. Nel riquadro di navigazione a sinistra, scegli Macchine virtuali.
2. Seleziona la casella di controllo accanto a Nome VM per scegliere tutte le tue macchine virtuali. In alternativa, seleziona la casella di controllo accanto ai nomi VM a cui desideri assegnare tag.
3. Scegli Aggiungi tag.
4. Digita una Chiave tag.
5. Consigliato: digita un valore tag.
6. Scegli Conferma.

Assegnazione di macchine virtuali mediante la funzionalità Assegna risorse da pianificare

È possibile assegnare le macchine virtuali attualmente scoperte da AWS Backup a un piano di backup nuovo o esistente utilizzando la funzionalità Assegna risorse al piano.

Per assegnare macchine virtuali mediante la funzionalità Assegna risorse da pianificare:

1. Nel riquadro di navigazione a sinistra, scegli Macchine virtuali.
2. Seleziona la casella di controllo accanto a Nome VM per scegliere tutte le tue macchine virtuali. In alternativa, seleziona la casella di controllo accanto a più nomi VM per assegnarli allo stesso piano di backup.
3. Scegli Assegnazioni, quindi seleziona Assegna risorse da pianificare.
4. Digita un Nome assegnazione di risorsa.

5. Scegli un ruolo IAM di assegnazione delle risorse per creare backup e gestire punti di ripristino. Se non disponi di un ruolo IAM specifico da utilizzare, ti consigliamo il ruolo predefinito con le autorizzazioni corrette.
6. Nella sezione Piano di backup, scegli un Piano di backup esistente dall'elenco a discesa. In alternativa, puoi scegliere Crea un piano di backup per creare un nuovo piano di backup.
7. Scegli Assegna risorse.
8. Facoltativo: verifica che le macchine virtuali siano assegnate a un piano di backup scegliendo Visualizza piano di backup. Quindi, nella sezione Assegnazioni delle risorse, scegli il Nome dell'assegnazione di risorsa.

Assegnazione di macchine virtuali mediante la funzionalità Crea assegnazione del gruppo

A differenza delle due funzioni di assegnazione delle risorse precedenti per le macchine virtuali, la funzionalità Crea assegnazione di gruppo non solo assegna le macchine virtuali attualmente scoperte da AWS Backup, ma anche le macchine virtuali scoperte in futuro in una cartella o in un hypervisor definito dall'utente.

Inoltre, per utilizzare la funzionalità Crea assegnazione del gruppo, non è necessario selezionare alcuna casella di controllo.

Per assegnare macchine virtuali mediante la funzionalità Assegna risorse da pianificare:

1. Nel riquadro di navigazione a sinistra, scegli Macchine virtuali.
2. Scegli Assegnazioni, quindi seleziona Crea assegnazione del gruppo.
3. Digita un Nome assegnazione di risorsa.
4. Scegli un ruolo IAM di assegnazione delle risorse per creare backup e gestire punti di ripristino. Se non disponi di un ruolo IAM specifico da utilizzare, ti consigliamo il ruolo predefinito con le autorizzazioni corrette.
5. Nella sezione Gruppo di risorse, seleziona il menu a discesa Tipo di gruppo. Le opzioni disponibili sono Cartella o Hypervisor.

    a. Scegli Cartella per assegnare tutte le macchine virtuali in una cartella su un hypervisor. Utilizzando il menu a discesa, seleziona un Nome gruppo della cartella, ad esempio `datacenter/vm`. Puoi anche scegliere di includere Cartelle secondarie.

> **Note**
>
> Per eseguire assegnazioni basate su cartelle, durante il processo di scoperta, contrassegna le macchine virtuali con la cartella AWS Backup in cui le trovano durante il processo di scoperta. Se successivamente sposti una macchina virtuale in un'altra cartella, AWS Backup non puoi aggiornare il tag automaticamente a causa delle migliori pratiche di AWS etichettatura. Questo metodo di assegnazione potrebbe causare il backup continuo delle macchine virtuali che sono state spostate fuori dalla cartella assegnata.

   b. Scegli Hypervisor per assegnare tutte le macchine virtuali gestite da un hypervisor. Seleziona un Nome gruppo dell'ID hypervisor utilizzando il menu a discesa.

6. Nella sezione Piano di backup, scegli un Piano di backup esistente dall'elenco a discesa. In alternativa, puoi scegliere Crea un piano di backup per creare un nuovo piano di backup.
7. Scegli Crea assegnazione del gruppo.
8. Facoltativo: verifica che le macchine virtuali siano assegnate a un piano di backup scegliendo Visualizza piano di backup. Nella sezione Assegnazioni delle risorse, scegli il Nome dell'assegnazione di risorsa.

Fasi successive

Per ripristinare una macchina virtuale, consulta Ripristino di una macchina virtuale utilizzando AWS Backup.

Informazioni sui componenti di origine di terze parti per il Backup gateway

In questa sezione, è possibile trovare informazioni sugli strumenti e le licenze di terze parti da cui dipendiamo per offrire funzionalità Backup gateway.

Il codice sorgente per determinati componenti software open source di terze parti inclusi con il software Backup gateway è disponibile per il download agli indirizzi seguenti:

- Per i gateway implementati su VMware ESXi, scarica sources.tzg.

Questo prodotto include software sviluppato dal progetto OpenSSL per l'uso in OpenSSL Toolkit (https://www.openssl.org/).

Questo prodotto include software sviluppato dal Software Development Kit VMware® vSphere (https://www.vmware.com).

Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consulta Licenze di terze parti.

Componenti open source per AWS Appliance

Diversi strumenti e licenze di terze parti vengono utilizzati per fornire funzionalità per Backup gateway.

Utilizzate i seguenti collegamenti per scaricare il codice sorgente di alcuni componenti software open source inclusi nel software Appliance: AWS

- Per i gateway distribuiti su VMware ESXi, scarica sources.tar

Questo prodotto include software sviluppato dal progetto OpenSSL per l'uso in OpenSSL Toolkit (https://www.openssl.org/). Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consulta Licenze di terze parti.

Risoluzione dei problemi delle macchine virtuali

Problemi e messaggi di backup incrementali / CBT

Messaggio di errore: **"The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."**

Se il messaggio persiste, ripristina CBT come indicato da VMware.

Note sul messaggio CBT non è stata attivato o non era disponibile: "VMware Change Block Tracking (CBT) non era disponibile per questa macchina virtuale, ma il backup incrementale è stato completato con il meccanismo di modifica proprietario."

Verifica che il CBT sia acceso. Per verificare se CBT è abilitato su un disco virtuale:

1. Apri vSphere Client e seleziona una macchina virtuale spenta.
2. Fai clic con il pulsante destro del mouse sulla macchina virtuale e passa a Modifica impostazioni > Opzioni > Avanzate/Generali > Parametri di configurazione.
3. L'opzione `ctkEnabled` deve essere uguale a `True`.

Se è acceso, assicurati di utilizzare le funzionalità di VMware. up-to-date L'host deve essere ESXi 4.0 o versione successiva e la macchina virtuale proprietaria dei dischi da tracciare deve disporre di una versione hardware 7 o successiva.

Se CBT è acceso (abilitato) e il software e l'hardware sono aggiornati, spegni la macchina virtuale e riaccendila. Assicurati che CBT sia acceso. Quindi, esegui nuovamente il backup.

Backup di DynamoDB avanzato

AWS Backup supporta funzionalità aggiuntive e avanzate per le tue esigenze di protezione dei dati di Amazon DynamoDB. Dopo aver abilitato le funzionalità avanzate AWS Backup di DynamoDB Regione AWS, sbloccherai le seguenti funzionalità per tutti i nuovi backup di tabelle DynamoDB che crei:

- Risparmio e ottimizzazione dei costi:
  - Suddivisione in livelli dei backup su storage a freddo per ridurre i costi di storage
  - Tag di allocazione dei costi per l'utilizzo con Esploratore dei costi
- Continuità aziendale:
  - Copia tra regioni
  - Copia tra account
- Sicurezza:
  - Archivia i backup in vault di AWS Backup crittografati, che puoi proteggere con Vault Lock di AWS Backup, Policy di AWS Backup e chiavi di crittografia.
  - I backup ereditano i tag dalle tabelle DynamoDB di origine, consentendo di utilizzare tali tag per impostare autorizzazioni e policy di controllo dei servizi.

I nuovi clienti che effettuano l'onboarding AWS Backup dopo novembre 2021 hanno le funzionalità di backup avanzate di DynamoDB abilitate di default. In particolare, le funzionalità di backup avanzate di DynamoDB sono abilitate per impostazione predefinita per i clienti che non hanno creato un vault di backup prima del 21 novembre 2021.

Consigliamo a tutti i AWS Backup clienti esistenti di abilitare le funzionalità avanzate per DynamoDB. Non vi è differenza di prezzo nello storage di backup a caldo dopo aver abilitato le funzionalità avanzate. Puoi risparmiare denaro suddividendo in livelli i backup su storage a freddo e ottimizzare i costi utilizzando i tag di allocazione dei costi. Puoi anche iniziare a sfruttare le funzionalità AWS Backup di continuità aziendale e di sicurezza.

> **Note**
>
> Se utilizzi un ruolo o una politica personalizzata anziché il ruolo AWS Backup di servizio predefinito, devi aggiungere o utilizzare le seguenti politiche di autorizzazione (o aggiungere le relative autorizzazioni equivalenti) al tuo ruolo personalizzato:
>
> - `AWSBackupServiceRolePolicyForBackup` per eseguire il backup avanzato di DynamoDB.
> - `AWSBackupServiceRolePolicyForRestores` per ripristinare i backup avanzati di DynamoDB.
>
> Per ulteriori informazioni sulle politiche AWS gestite dai clienti e visualizzare esempi di politiche gestite dai clienti, consulta. Politiche gestite per AWS Backup

Argomenti

Abilitazione del backup avanzato di DynamoDB mediante la console

È possibile abilitare funzionalità AWS Backup avanzate per i backup di DynamoDB utilizzando la console DynamoDB o la AWS Backup console DynamoDB.

Per abilitare le funzionalità di backup avanzate di DynamoDB dalla console: AWS Backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, scegli Impostazioni.
3. Nella sezione Servizi supportati, verifica che DynamoDB sia abilitato.

   In caso contrario, scegli Opt-in e abilita DynamoDB come servizio supportato da AWS Backup .

4. Nella sezione Funzionalità avanzate per i backup DynamoDB, scegli Abilita.
5. Scegli Enable features (Abilita caratteristiche).

Per come abilitare le funzionalità AWS Backup avanzate utilizzando la console DynamoDB, consulta AWS Backup Enabling features nella Amazon DynamoDB User Guide.

Abilitazione del backup avanzato di DynamoDB a livello di codice

È inoltre possibile abilitare funzionalità AWS Backup avanzate per i backup DynamoDB utilizzando la (CLI AWS Command Line Interface). I backup DynamoDB avanzati vengono abilitati quando si impostano entrambi i valori seguenti su `true`:

Per abilitare a livello di codice funzionalità AWS Backup avanzate per i backup DynamoDB:

1. Verifica se hai già abilitato le funzionalità AWS Backup avanzate per DynamoDB utilizzando il seguente comando:

   ```
   $ aws backup describe-region-settings
   ```

   Se `"DynamoDB":true` in `"ResourceTypeManagementPreference"` e `"ResourceTypeOptInPreference"`, hai già abilitato il backup DynamoDB avanzato.

   Se, come nell'output seguente, disponi di almeno un'istanza di `"DynamoDB":false`, significa che non hai ancora abilitato il backup DynamoDB avanzato e puoi andare al passaggio successivo.

   ```
   {
     "ResourceTypeManagementPreference":{
       "DynamoDB":false,
       "EFS":true
     }
     "ResourceTypeOptInPreference":{
       "Aurora":true,
       "DocumentDB":false,
       "DynamoDB":false,
       "EBS":true,
       "EC2":true,
       "EFS":true,
       "FSx":true,
       "Neptune":false,
   ```

```
    "RDS":true,
    "Storage Gateway":true
  }
}
```

2. Utilizza la seguente operazione `UpdateRegionSettings` per impostare `"ResourceTypeManagementPreference"` e `"ResourceTypeOptInPreference"` su `"DynamoDB":true`:

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

Modifica di un backup DynamoDB avanzato

Quando si crea un backup DynamoDB dopo aver AWS Backup abilitato le funzionalità avanzate, è possibile utilizzare per: AWS Backup

- Copiare un backup tra regioni
- Copiare un backup tra account
- Modifica la modalità di AWS Backup trasferimento di un backup alla conservazione a freddo
- Assegnare tag al backup

Per utilizzare queste funzionalità avanzate su un backup esistente, consulta Modifica di un backup.

Se in seguito disabiliti le funzionalità AWS Backup avanzate per DynamoDB, puoi continuare a eseguire tali operazioni sui backup DynamoDB che hai creato durante il periodo in cui hai abilitato le funzionalità avanzate.

Ripristino di un backup DynamoDB avanzato

È possibile ripristinare i backup di DynamoDB eseguiti AWS Backup con funzionalità avanzate abilitate nello stesso modo in cui si ripristinano i backup di DynamoDB eseguiti prima di abilitare le funzionalità avanzate. AWS Backup È possibile eseguire un ripristino utilizzando uno AWS Backup o DynamoDB.

Puoi specificare come crittografare la tabella appena ripristinata con le seguenti opzioni:

- Quando esegui il ripristino nella stessa regione della tabella originale, puoi facoltativamente specificare una chiave di crittografia per la tabella ripristinata. Se non si specifica una chiave di crittografia, AWS Backup crittograferà automaticamente la tabella ripristinata utilizzando la stessa chiave che ha crittografato la tabella originale.
- Quando esegui il ripristino in una regione diversa dalla tabella originale, devi specificare una chiave di crittografia.

Per ripristinare l'utilizzo AWS Backup, vedereRipristino di una tabella Amazon DynamoDB.

Per eseguire il ripristino mediante DynamoDB, consulta Ripristino di una tabella DynamoDB da un backup nella Guida per l'utente di Amazon DynamoDB.

Eliminazione di un backup DynamoDB avanzato

Non è possibile eliminare i backup creati utilizzando queste funzionalità avanzate in DynamoDB. È necessario utilizzare AWS Backup per eliminare i backup per mantenere la coerenza globale in tutto l'ambiente AWS .

Per eliminare un backup DynamoDB, consulta Eliminazione di backup.

Altri vantaggi della gestione completa AWS Backup quando si abilita il backup DynamoDB avanzato

Quando abiliti le funzionalità AWS Backup avanzate per DynamoDB, offri la gestione completa dei tuoi backup DynamoDB a. AWS Backup In questo modo si ottengono i seguenti vantaggi aggiuntivi:

Encryption (Crittografia)

AWS Backup cripta automaticamente i backup con la chiave KMS del vault di destinazione. AWS Backup In precedenza, venivano crittografati utilizzando lo stesso metodo di crittografia della tabella DynamoDB di origine. Ciò aumenta il numero di difese che puoi utilizzare per proteggere i dati. Per ulteriori informazioni, consulta Crittografia per i backup in AWS Backup.

Nome della risorsa Amazon (ARN)

Lo spazio dei nomi del servizio di ciascun ARN di backup è `awsbackup`. In precedenza, lo spazio dei nomi del servizio era `dynamodb`. In altre parole, l'inizio di ogni ARN cambierà da `arn:aws:dynamodb` a `arn:aws:backup`. Consulta ARNs for AWS Backup in Service Authorization Reference.

Con questa modifica, l'utente o l'amministratore di backup può creare policy di accesso per i backup utilizzando lo spazio dei nomi del servizio `awsbackup` che ora si applica ai backup DynamoDB creati dopo aver abilitato le funzionalità avanzate. Utilizzando lo spazio dei nomi del servizio `awsbackup`, è anche possibile applicare le policy ad altri backup eseguiti da AWS Backup. Per ulteriori informazioni, consulta Controllo accessi.

Ubicazione degli addebiti sull'estratto conto

Gli addebiti per i backup (inclusi archiviazione, trasferimento di dati, ripristino ed eliminazione anticipata) vengono visualizzati alla voce «Backup» della fattura. AWS In precedenza, gli addebiti erano visualizzati sotto "DynamoDB" nella fattura.

Questa modifica consente di utilizzare la AWS Backup fatturazione per monitorare centralmente i costi di backup. Per ulteriori informazioni, consulta Misurazione, costi e fatturazione.

Backup Amazon Timestream

Amazon Timestream è un database di serie temporali scalabile che consente lo storage e l'analisi di trilioni di punti dati di serie temporali al giorno. Timestream è ottimizzato per risparmiare tempo e costi conservando i dati recenti in memoria e archiviando i dati storici in un livello di storage ottimizzato in termini di costi in conformità con le policy dell'utente.

Un database Timestream dispone di tabelle. Queste tabelle contengono record e ogni record è un singolo punto dati in una serie temporale. Una serie temporale è una sequenza di record registrati in un intervallo di tempo, ad esempio il prezzo delle azioni, il livello di utilizzo della memoria di un'istanza Amazon EC2 o una lettura della temperatura. AWS Backup può eseguire il backup e il ripristino centralizzati delle tabelle Timestream. È possibile copiare questi backup delle tabelle su altri account e diversi altri all' Regioni AWS interno della stessa organizzazione.

Attualmente Timestream non offre servizi di backup e ripristino nativi, quindi utilizzarli AWS Backup per creare copie sicure delle tabelle Timestream può aggiungere un ulteriore livello di sicurezza e resilienza alle risorse.

Backup delle tabelle Timestream

È possibile eseguire il backup delle tabelle Timestream tramite la console o utilizzando il. AWS Backup AWS CLI

Esistono due modi per utilizzare la AWS Backup console per eseguire il backup di una tabella Timestream: su richiesta o come parte di un piano di backup.

Creazione di backup Timestream on demand

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Utilizzando il riquadro di navigazione, scegli Risorse protette, quindi Crea backup on demand.
3. Nella pagina Crea backup on demand, scegli Amazon Timestream.
4. Scegli Tipo di risorsa Timestream, quindi seleziona il nome della tabella di cui desideri eseguire il backup.
5. Nella finestra di backup, assicurati che l'opzione Crea backup adesso sia selezionata. Questo consente di avviare un backup immediatamente e di visualizzare il cluster più rapidamente nella pagina Risorse protette.
6. Nel menu a discesa Transizione allo storage a freddo, puoi configurare le impostazioni di transizione.
7. In Periodo di conservazione, puoi scegliere per quanto tempo mantenere il backup.
8. Scegli un vault di backup esistente o crea un nuovo vault di backup. Scegliendo Create new backup vault (Crea nuovo vault di backup), si apre una nuova pagina in cui è possibile creare un vault e al termine viene visualizzata nuovamente la pagina Create on-demand backup.
9. In Ruolo IAM, scegli Ruolo AWS Backup predefinito (se il ruolo predefinito non è presente nel tuo account, verrà creato per te con le autorizzazioni corrette).
10. Facoltativamente, puoi aggiungere tag al punto di ripristino. Se si desidera assegnare uno o più tag al proprio backup on demand, immettere una chiave e, facoltativamente, un valore, quindi scegliere Aggiungi tag.
11. Scegliere Create on-demand backup (Crea backup on demand). In questo modo si accede alla pagina Processi, in cui è visualizzato un elenco di processi.
12. Scegli l'ID del processo di backup per il cluster per visualizzare i dettagli di tale processo. Verrà visualizzato lo stato `Completed`, `In Progress` o `Failed`. Puoi fare clic sul pulsante Aggiorna per aggiornare lo stato visualizzato.

Creazione di backup Timestream pianificati in un piano di backup

I backup pianificati possono includere tabelle Timestream se sono una risorsa protetta. Per attivare la protezione delle tabelle Amazon Timestream:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette.

3. Imposta Amazon Timestream su Attivo.
4. Per includere tabelle Timestream in un piano nuovo o esistente, consulta Assegnazione di risorse tramite la console.

In Gestisci i piani di backup, puoi scegliere di creare un piano di backup e includere tabelle Timestream oppure puoi aggiornare uno esistente per includere tabelle Timestream. Quando aggiungi il tipo di risorsa Timestream, puoi scegliere di aggiungere Tutte le tabelle Timestream o selezionare le caselle accanto alle tabelle che desideri aggiungere in Seleziona tipi di risorse specifici.

Il primo backup effettuato delle tabelle Timestream sarà un backup completo. I backup successivi saranno backup incrementali.

Dopo aver creato o modificato il piano di backup, passa a Piani di backup nella barra di navigazione a sinistra. Il piano di backup specificato deve visualizzare i cluster in Assegnazioni delle risorse.

Esecuzione di backup in modo programmatico

Puoi utilizzare il nome operazione `start-backup-job`. Includere i seguenti parametri:

```
aws backup start-backup-job \
--backup-vault-name backup-vault-name \
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-name \
--iam-role-arn arn:aws:iam::account:role/role-name \
--region Regione AWS \
--endpoint-url URL
```

Visualizzazione dei backup delle tabelle Timestream

Per visualizzare e modificare i backup delle tabelle Timestream all'interno della console:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Scegliere Vault di Backup. Quindi, fai clic sul nome del vault di backup contenente le tabelle Timestream.
3. Nel vault di backup verrà visualizzato un riepilogo e un elenco di backup.
    a. Puoi fare clic sul collegamento nella colonna ID punto di ripristino, oppure

b. Puoi selezionare la casella a sinistra dell'ID del punto di ripristino e fare clic su Azioni per eliminare i punti di ripristino che non sono più necessari.

Ripristino di una tabella Timestream

Vedi come ripristinare una tabella Timestream

Database SAP HANA su backup di istanze Amazon EC2

> **Note**
>
> Servizi supportati da Regione AWScontiene le regioni attualmente supportate in cui sono disponibili i backup del database SAP HANA su istanze Amazon EC2.

AWS Backup supporta backup e ripristini di database SAP HANA su istanze Amazon EC2.

Argomenti

- Panoramica dei database SAP HANA con AWS Backup
- Prerequisiti per il backup dei database SAP HANA tramite AWS Backup
- Operazioni di backup SAP HANA nella console AWS Backup
- Visualizza i backup del database SAP HANA
- Utilizzalo AWS CLI per i database SAP HANA con AWS Backup
- Risoluzione dei problemi relativi ai backup dei database SAP HANA
- Glossario dei termini di SAP HANA durante l'utilizzo AWS Backup
- AWS Backup supporto dei database SAP HANA sulle istanze EC2 (note di rilascio).

Panoramica dei database SAP HANA con AWS Backup

Oltre alla possibilità di creare backup e ripristinare database, l'integrazione AWS Backup con Amazon EC2 Systems Manager for SAP consente ai clienti di identificare e assegnare tag ai database SAP HANA.

AWS Backup è integrato con AWS Backint Agent per eseguire backup e ripristini SAP HANA. Per ulteriori informazioni, consulta Backint AWS.

Prerequisiti per il backup dei database SAP HANA tramite AWS Backup

È necessario completare diversi prerequisiti prima di poter eseguire attività di backup e ripristino. Tieni presente che avrai bisogno dell'accesso amministrativo al tuo database SAP HANA e delle autorizzazioni per creare nuovi ruoli e policy IAM nel tuo account per eseguire questi passaggi. AWS

Completa questi prerequisiti presso Amazon EC2 Systems Manager.

1. Configurazione delle autorizzazioni richieste per l'istanza Amazon EC2 che esegue il database SAP HANA
2. Registra le credenziali in AWS Secrets Manager
3. Installa AWS Backint and AWS Systems Manager for SAP Agents
4. Verifica dell'agente SSM
5. Verifica dei parametri
6. Registrazione del database SAP HANA

È consigliabile registrare ogni istanza HANA una sola volta. Registrazioni multiple possono generare più ARN per lo stesso database. Il mantenimento di un unico ARN e della registrazione semplifica la creazione e la manutenzione del piano di backup e può anche aiutare a ridurre la duplicazione non pianificata dei backup.

Operazioni di backup SAP HANA nella console AWS Backup

Dopo che i prerequisiti e le configurazioni SSM per SAP sono stati completati, puoi eseguire il backup e il ripristino di SAP HANA su database EC2.

Adesione alla protezione delle risorse SAP HANA

AWS Backup Per proteggere i database SAP HANA, è necessario attivare SAP HANA come una delle risorse protette. Per acconsentire:

1. Apri la console all'indirizzo https://console.aws.amazon.com/backup. AWS Backup
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. In Attivazione del servizio, seleziona Configura risorse.
4. Fornisci il consenso per SAP HANA su Amazon EC2.
5. Fai clic su Conferma.

Attivazione del servizio per SAP HANA su Amazon EC2 verrà ora abilitato.

Crea un backup pianificato dei database SAP HANA

Puoi modificare un piano di backup esistente e aggiungervi risorse SAP HANA oppure puoi creare un nuovo piano di backup solo per le risorse SAP HANA.

Se scegli di creare un nuovo piano di backup, sono disponibili tre opzioni:

1. Opzione 1: Inizia con un modello
    1. Scegli un modello del piano di backup.
    2. Specifica un nome del piano di backup.
    3. Fai clic su Crea piano.
2. Opzione 2: Crea un nuovo piano
    1. Specifica un nome del piano di backup.
    2. Specifica facoltativamente i tag da aggiungere al piano di backup.
    3. Specifica la configurazione della regola di backup.
        a. Specifica un nome della regola di backup.
        b. Seleziona un vault esistente o crea un nuovo vault di backup. I backup vengono archiviati qui.
        c. Specifica una frequenza di backup.
        d. Specifica una finestra di backup.

            Nota: la transizione allo storage a freddo non è attualmente supportata.
        e. Specifica il periodo di conservazione.

            Copia nella destinazione non è attualmente supportata
        f. (Facoltativo) Specifica i tag da aggiungere ai punti di ripristino.
    4. Fai clic su Crea piano.
3. Opzione 3: Definisci un piano utilizzando JSON
    1. Specifica il JSON per il piano di backup modificando l'espressione JSON di un piano di backup esistente o creando una nuova espressione.
    2. Specifica un nome del piano di backup.

3. Fai clic su Convalida JSON.

Dopo che è stato creato, puoi assegnare risorse al piano di backup nel passaggio successivo.

Qualunque sia il piano utilizzato, assicurati di assegnare risorse. Puoi scegliere quali database SAP HANA assegnare, inclusi i database di sistema e tenant. Hai anche la possibilità di escludere ID risorsa specifici.

Crea un backup su richiesta dei database SAP HANA

Puoi creare un backup on demand completo che viene eseguito subito dopo la creazione. Tieni presente che i backup on demand di database SAP HANA su istanze Amazon EC2 sono backup completi; i backup incrementali non sono supportati.

Il backup on demand è stato creato. Verrà avviato il backup delle risorse specificate. La console eseguirà la transizione alla pagina Processi di backup in cui è possibile visualizzare lo stato di avanzamento del processo. Prendi nota dell'ID del processo di backup dal banner blu nella parte superiore dello schermo, poiché sarà necessario per trovare facilmente lo stato del processo di backup. Al termine del backup, lo stato passerà a `Completed`. I backup possono richiedere anche diverse ore.

Aggiorna l'elenco dei processi di backup per visualizzare la modifica dello stato. Puoi anche cercare e fare clic sull'ID del processo di backup per visualizzare lo stato dettagliato del processo.

Backup continui di database SAP HANA

È possibile eseguire backup continui, utilizzabili con point-in-time restore (PITR) (si noti che i backup su richiesta preservano le risorse nello stato in cui vengono acquisite; mentre PITR utilizza backup continui che registrano le modifiche nel corso di un periodo di tempo).

Con i backup continui, puoi ripristinare il database SAP HANA su un'istanza EC2 riportandola a un momento specifico scelto, entro 1 secondo di precisione (tornando indietro fino a un massimo di 35 giorni). Il backup continuo funziona creando innanzitutto un backup completo della risorsa e quindi eseguendo costantemente il backup dei log delle transazioni della risorsa. Il ripristino PITR funziona accedendo al backup completo e riproducendo il registro delle transazioni fino all'ora indicata per il ripristino. AWS Backup

Puoi attivare i backup continui quando crei un piano di backup AWS Backup utilizzando la AWS Backup console o l'API.

Per abilitare i backup continui tramite la console

1. Accedi a e AWS Management Console apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Piani di backup e seleziona Crea un piano di backup.
3. In Regole di backup, scegli Aggiungi regola di backup.
4. Nella sezione Configurazione regola di backup, seleziona Abilita backup continui per le risorse supportate.

Dopo aver disabilitato PITR (point-in-timeripristino) per i backup del database SAP HANA, i log continueranno a essere inviati AWS Backup fino alla scadenza del punto di ripristino (stato uguale). `EXPIRED`) Puoi passare a una posizione di backup dei log alternativa in SAP HANA per interrompere la trasmissione dei log ad AWS Backup.

Un punto di ripristino continuo con uno stato pari a `STOPPED` indica che un punto di ripristino continuo è stato interrotto; ovvero, i log trasmessi da SAP HANA a che mostrano le modifiche incrementali a AWS Backup un database presentano una lacuna. I punti di ripristino che si verificano entro questo gap di intervallo di tempo presentano uno stato `STOPPED`..

Per i problemi che si possono verificare durante i processi di ripristino dei backup continui (punti di ripristino), consulta la sezione Risoluzione dei problemi relativi al ripristino di SAP HANA di questa guida.

Visualizza i backup del database SAP HANA

Visualizzare lo stato dei processi di backup e di ripristino:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Jobs (Processi).
3. Scegli i processi di backup, i processi di ripristino o i processi di copia per visualizzare l'elenco dei processi.
4. Cerca e fai clic sull'ID processo per visualizzare gli stati dettagliati dei processi.

Visualizzare tutti i punti di ripristino in un vault:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).

3. Cerca e fai clic su un vault di backup per visualizzare tutti i punti di ripristino all'interno del vault.

Visualizzare i dettagli delle risorse protette:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione selezionare Protected resources (Risorse protette).
3. Puoi anche filtrare per tipo di risorsa per visualizzare tutti i backup di tale tipo di risorsa.

Utilizzalo AWS CLI per i database SAP HANA con AWS Backup

Ogni azione all'interno della console di backup dispone di una chiamata API corrispondente.

Per configurare e gestire a livello di codice AWS Backup e le relative risorse, utilizza la chiamata API `StartBackupJob`per eseguire il backup di un database SAP HANA su un'istanza EC2.

Utilizza `start-backup-job` come il comando CLI.

Risoluzione dei problemi relativi ai backup dei database SAP HANA

Se riscontri errori durante il flusso di lavoro, consulta i seguenti errori di esempio e le risoluzioni suggerite:

Prerequisiti Python

- Errore: errore di Zypper relativo alla versione di Python a partire da SSM per SAP e richiede Python 3.6 ma SUSE 12 SP5 di default supporta AWS Backup Python 3.4.

  Risoluzione: installa più versioni di Python su SUSE12 SP5 effettuando le seguenti operazioni:

  1. Esegui un comando update-alternatives per creare un collegamento simbolico per Python 3 in '/usr/local/bin/' invece di usare direttamente '/usr/bin/python3'. Questo comando imposterà Python 3.4 come versione predefinita. Il comando è: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.4 5`
  2. Aggiungi Python 3.6 alla configurazione delle alternative eseguendo il seguente comando: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
  3. Cambia la configurazione alternativa a Python 3.6 eseguendo il seguente comando: `# sudo update-alternatives –config python3`

     Dovrebbe essere visualizzato il seguente output:

```
There are 2 choices for the alternative python3 (providing /usr/local/bin/python3).
 Selection Path Priority Status
* 0 /usr/bin/python3.4 5 auto mode
 1 /usr/bin/python3.4 5 manual mode
 2 /usr/bin/python3.6 2 manual mode
Press enter to keep the current choice[*], or type selection number:
```

4. Immettete il numero corrispondente a Python 3.6.
5. Controlla la versione di Python e conferma che Python 3.6 sia in uso.
6. (Facoltativo, ma consigliato) Verifica che i comandi Zypper funzionino come previsto.

Amazon EC2 Systems Manager per il rilevamento e la registrazione di SAP

- Errore: SSM per SAP non è riuscito a rilevare il carico di lavoro a causa del blocco dell'accesso all'endpoint pubblico per SSM. AWS Secrets Manager

  Risoluzione: verifica se gli endpoint sono raggiungibili dal database SAP HANA. Se non possono essere raggiunti, puoi creare endpoint Amazon VPC per AWS Secrets Manager e SSM per SAP.

  1. Verifica l'accesso a Secrets Manager dall'host Amazon EC2 per HANA DB eseguendo il seguente comando:. `aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp` Se il comando non riesce a restituire un valore, il firewall blocca l'accesso all'endpoint del servizio Secrets Manager. Il registro si interromperà alla fase «Recupero di segreti da Secrets Manager».
  2. Verifica la connettività a SSM per l'endpoint SAP eseguendo il comando. `aws ssm-sap list-registration` Se il comando non riesce a restituire un valore, il firewall blocca l'accesso all'endpoint SSM per SAP.

     Esempio di errore:. `Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application"`

  Esistono due opzioni per procedere se gli endpoint non sono raggiungibili.

  - Aprire le porte firewall per consentire l'accesso agli endpoint di servizio pubblico per Secrets Manager e SSM per SAP; oppure
  - Crea endpoint VPC per Secrets Manager e SSM per SAP, quindi:
    - Assicurati che Amazon VPC sia abilitato per DNSSupport e DNSHostName.

    - Assicurati che il tuo endpoint VPC abbia abilitato l'opzione Allow Private DNS Name.
    - Se il rilevamento SSM per SAP è stato completato correttamente, il registro mostrerà che l'host è stato scoperto.

- Errore: AWS Backup e la connessione Backint fallisce a causa del blocco dell'accesso agli endpoint pubblici AWS Backup del servizio. `aws-backint-agent.log`può mostrare errori simili a questo: `time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id"` o. `level=fatal msg="Error performing backup missing backup data plane Id` Inoltre, la AWS Backup console può mostrare `Fatal Error: An internal error occured.`

  Risoluzione: ci sono due opzioni per procedere se gli endpoint non sono raggiungibili:

    - Aprire le porte del firewall per consentire l'accesso agli endpoint del servizio pubblico (HTTPS). Dopo aver utilizzato questa opzione, il DNS risolverà le richieste ai AWS servizi tramite indirizzi IP pubblici.
    - Crea endpoint VPC per indirizzare privatamente il traffico da AWS e verso i servizi richiesti. AWS Backup Dopo aver utilizzato questa opzione, il DNS risolverà le richieste per tali servizi tramite indirizzi IP privati. Questa opzione potrebbe richiedere aggiornamenti al server DNS per aggiungere regole per inoltrare le richieste agli endpoint privati.

- Errore: la registrazione SSM per SAP non riesce a causa della password HANA contenente caratteri speciali. Gli errori di esempio possono includere `Error connecting to database HBX/HBX when validating its credentials.` o `Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.` dopo aver testato una connessione utilizzando `hdbsql` for `systemdb` e `tenantdb` che è stata testata dall'istanza Amazon EC2 del database HANA.

  Nella AWS Backup console, nella pagina Processi, i dettagli del processo di backup possono mostrare lo stato corrispondente `FAILED` all'errore. `Miscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’`

  Risoluzione: assicurati che la tua password non contenga caratteri speciali, come $.

- Errore: **`b’* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  Risoluzione: l'installazione di AWS BackInt Agent for SAP HANA potrebbe non essere stata completata correttamente. Riprova il processo per distribuire l'AWS agente Backint e l'agente Amazon EC2 Systems Manager sul tuo server di applicazioni SAP.

- Errore: la console non corrisponde ai file di registro dopo la registrazione.

  Il registro di rilevamento mostra che la registrazione non è riuscita quando si tenta di connettersi a HANA DB a causa della password contenente caratteri speciali, sebbene l'SSM per SAP Application Manager per la console SAP indichi che la registrazione è avvenuta correttamente. Non conferma che la registrazione sia avvenuta con successo. Se la registrazione è avvenuta correttamente sulla console ma non nei log, i backup avranno esito negativo.

  Conferma lo stato della registrazione:

  1. Accedi alla console SSM
  2. Seleziona Esegui comando dalla barra di navigazione a sinistra.
  3. Nel campo di testo Cronologia dei comandi`Instance ID:Equal:`, inserisci il valore uguale all'istanza utilizzata per la registrazione. Questo filtrerà la cronologia dei comandi.
  4. Usa la colonna command id per trovare i comandi con stato`Failed`. Quindi, trova il nome del documento di AWSSystemsManagerSAP-Discovery.
  5. Nel AWS CLI, esegui il comando`aws ssm-sap register-application status`. Se il valore restituito viene visualizzato`Error`, la registrazione non è riuscita.

  Risoluzione: assicurati che la tua password HANA non contenga caratteri speciali (come '$').

Creazione di un backup di un database SAP HANA

- Errore: la AWS Backup console visualizza il messaggio «Errore irreversibile» quando viene creato un backup su richiesta per SystemDB o TenantDB. Ciò si verifica perché non è possibile accedere all'endpoint pubblico cell-1.prod.us-west-2.storage.cryo.aws.a2z.com. Ciò è causato da un firewall lato client che blocca l'accesso a questo endpoint.

  `aws-backint-agent.log`può mostrare errori come o `level=error msg="Storage configuration validation failed: missing backup data plane Id" level=fatal msg="Error performing backup missing backup data plane Id."`

  Risoluzione: aprire l'accesso tramite firewall all'endpoint pubblico cell-1.prod.us-west-2.storage.cryo.aws.a2z.com.

- **`Database cannot be backed up while it is stopped`**Errore:.

  Risoluzione: assicurati che il database di cui eseguire il backup sia attivo. È possibile eseguire il backup dei dati e dei log del database solo mentre il database è online.

- Errore: `Getting backup metadata failed. Check the SSM document execution for more details.`

  Risoluzione: assicurati che il database di cui eseguire il backup sia attivo. È possibile eseguire il backup dei dati e dei log del database solo mentre il database è online.

Monitoraggio dei registri di backup

- Errore: `Encountered an issue with log backups, please check SAP HANA for details.`

  Risoluzione: controlla SAP HANA per assicurarti che i backup dei log vengano inviati AWS Backup da SAP HANA.
- Errore: `One or more log backup attempts failed for recovery point.`

  Risoluzione: consulta SAP HANA per i dettagli. Assicurati che i backup dei log vengano inviati AWS Backup da SAP HANA.
- Errore: `Unable to determine the status of log backups for recovery point.`

  Risoluzione: consulta SAP HANA per i dettagli. Assicurati che i backup dei log vengano inviati AWS Backup da SAP HANA.
- Errore: `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

  Risoluzione: attendi il completamento del processo di ripristino. I backup dei log verranno ripristinati.

Glossario dei termini di SAP HANA durante l'utilizzo AWS Backup

Tipi di backup dei dati: SAP HANA supporta due tipi di backup dei dati: completo e INC (incrementale). AWS Backup ottimizza il tipo utilizzato durante ogni operazione di backup.

Backup del catalogo: SAP HANA mantiene il proprio manifesto chiamato catalogo. AWS Backup interagisce con questo catalogo. Ogni nuovo backup creerà una voce nel catalogo.

Backup dei log continuo (log delle transazioni): per le funzioni ripristino point-in-time (PITR), SAP HANA tiene traccia di tutte le transazioni dal backup più recente.

Copia di sistema: un processo di ripristino in cui il database di destinazione del ripristino è diverso dal database di origine da cui è stato creato il punto di ripristino.

Ripristino distruttivo: un ripristino distruttivo è un tipo di processo di ripristino durante il quale un database ripristinato elimina o sovrascrive il database di origine o esistente.

FULL: un backup completo è il backup di un database completo.

INC: un backup incrementale è un backup di tutte le modifiche apportate a un database SAP HANA dal backup precedente.

Per ulteriori dettagli, consulta il Glossario AWS.

AWS Backup supporto dei database SAP HANA sulle istanze EC2 (note di rilascio).

Alcune funzionalità non sono al momento supportate:

- La copia tra account e tra regioni non è attualmente supportata.
- Backup Audit Manager e creazione di report non sono attualmente supportati.
- Servizi supportati da Regione AWScontiene le regioni attualmente supportate per i backup del database SAP HANA su istanze Amazon EC2.

Backup Amazon Redshift

Amazon Redshift è un data warehouse cloud completamente gestito e scalabile che accelera i tempi di acquisizione delle informazioni con analisi rapide, semplici e sicure. Puoi utilizzarli AWS Backup per proteggere i tuoi data warehouse con backup immutabili, politiche di accesso separate e governance organizzativa centralizzata dei processi di backup e ripristino.

Un data warehouse Amazon Redshift è una raccolta di risorse di calcolo chiamate nodi, che sono organizzate in un gruppo chiamato cluster. AWS Backup può eseguire il backup di questi cluster.

Per informazioni su Amazon Redshift, consulta la Guida alle operazioni di base di Amazon Redshift, la Guia per sviluppatori di database di Amazon Redshift e la Guida alla gestione del cluster Amazon Redshift.

Backup di cluster con provisioning di Amazon Redshift

Puoi proteggere i tuoi cluster Amazon Redshift utilizzando la AWS Backup console o programmaticamente utilizzando API o CLI. È possibile eseguire il backup di questi cluster a intervalli regolari come parte di un piano di backup oppure, se necessario, tramite backup on demand.

Puoi ripristinare una singola tabella (noto anche come ripristino a livello di elemento) o un intero cluster. Tieni presente che non è possibile eseguire il backup delle tabelle da sole; il backup delle tabelle viene eseguito come parte di un cluster quando si esegue il backup del cluster.

L'utilizzo ti AWS Backup consente di visualizzare le tue risorse in modo centralizzato; tuttavia, se Amazon Redshift è l'unica risorsa che utilizzi, puoi continuare a utilizzare lo scheduler automatizzato di snapshot in Amazon Redshift. Tieni presente che non puoi continuare a gestire le impostazioni manuali degli snapshot utilizzando Amazon Redshift se scegli di gestirle tramite. AWS Backup

Puoi eseguire il backup dei cluster Amazon Redshift tramite la AWS Backup console o utilizzando il. AWS CLI

Esistono due modi per utilizzare la AWS Backup console per eseguire il backup di un cluster Amazon Redshift: su richiesta o come parte di un piano di backup.

Creazione di backup on demand di Amazon Redshift

Per ulteriori informazioni, consulta Creazione di un backup on demand.

Per creare uno snapshot manuale, lascia deselezionata la casella di controllo del backup continuo quando crei un piano di backup che include risorse Amazon Redshift.

Creazione di backup Amazon Redshift pianificati in un piano di backup

I backup pianificati possono includere cluster Amazon Redshift se sono una risorsa protetta. Per attivare la protezione delle tabelle Amazon Redshift:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette.
3. Imposta Amazon Redshift su Attivo.
4. Per includere cluster Amazon Redshift in un piano nuovo o esistente, consulta Assegnazione di risorse tramite la console.

In Gestisci i piani di backup, puoi scegliere di creare un piano di backup e includere cluster Amazon Redshift oppure puoi aggiornare uno esistente per includere cluster Amazon Redshift. Quando aggiungi il tipo di risorsa Amazon Redshift, puoi scegliere di aggiungere Tutti i cluster Amazon Redshift o selezionare le caselle accanto ai cluster.

Esecuzione di backup in modo programmatico

Puoi anche definire il tuo piano di backup in un documento JSON e fornirlo utilizzando la AWS Backup console o AWS CLI. Vedi Creazione di piani di backup utilizzando un documento JSON e la AWS Backup CLI per informazioni su come creare un piano di backup in modo programmatico.

Utilizzando API puoi effettuare le seguenti operazioni:

- Avviare un processo di backup
- Descrivere un processo di backup
- Ottenere i metadati dei punti di ripristino
- Elencare i punti di ripristino in base alle risorse
- Elencare i tag per il punto di ripristino

Visualizzazione dei backup dei cluster Amazon Redshift

Per visualizzare e modificare i backup delle tabelle Amazon Redshift all'interno della console:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Scegliere Vault di Backup. Quindi, fai clic sul nome del vault di backup contenente i cluster Amazon Redshift.
3. Nel vault di backup verrà visualizzato un riepilogo e un elenco di backup. Puoi fare clic sul collegamento nella colonna ID punto di ripristino.
4. Per eliminare uno o più punti di ripristino, seleziona le caselle che desideri eliminare. Sotto il pulsante Azioni, puoi selezionare Elimina.

Ripristino di un cluster Amazon Redshift

Per ulteriori informazioni, consulta Ripristino di un cluster Amazon Redshift.

Backup di Amazon Relational Database Service

Amazon RDS e AWS Backup

Quando si considerano le opzioni per il backup delle istanze e dei cluster Amazon RDS, è importante chiarire quale tipo di backup si desidera creare e utilizzare. Diverse AWS risorse, tra cui Amazon RDS, offrono le proprie soluzioni di backup native.

Amazon RDS offre la possibilità di effettuare backup automatici e backup manuali. Nella terminologia di Amazon RDS, tutti i punti di ripristino creati da AWS Backup, compresi quelli inclusi in un piano di backup, prendono in considerazione i backup manuali.

Quando lo utilizzi AWS Backup per creare un backup (punto di ripristino) di un'istanza Amazon RDS, AWS Backup verifica se in precedenza hai utilizzato Amazon RDS per creare un backup automatico. Se esiste un backup automatico, AWS Backup crea una copia di questa istantanea (`copy-db-snapshot`operazione). Se non esiste alcun backup esistente, AWS Backup crea un'istantanea dell'istanza indicata, anziché una copia (`create-db-snapshot`operazione).

La prima istantanea creata da AWS Backup, creata da una delle due operazioni, risulterà in 1 istantanea completa. Tutte le copie successive saranno backup incrementali, purché esista il backup completo.

> **Important**
>
> Quando è pianificato un piano di AWS Backup backup per creare più snapshot giornalieri di un'istanza Amazon RDS e quando una di queste finestre di avvio di AWS Backup backup pianificate coincide con la finestra di backup di Amazon RDS, la derivazione dei dati dei backup può suddividersi in backup non identici, creando backup non pianificati e in conflitto. Per evitare che ciò accada, assicurati che il piano di AWS Backup backup o la finestra di Amazon RDS non coincidano nei rispettivi orari.

Backup continui e ripristino point-in-time di Amazon RDS

I backup continui prevedono l'utilizzo AWS Backup per creare un backup completo della risorsa Amazon RDS, quindi l'acquisizione di tutte le modifiche tramite un registro delle transazioni. È possibile ottenere una maggiore granularità riavvolgendo fino al punto in cui si desidera eseguire il ripristino anziché scegliere un'istantanea precedente scattata a intervalli di tempo prestabiliti.

Per ulteriori informazioni, consulta i backup continui e i servizi supportati da PITR e la gestione delle impostazioni di backup continuo.

Backup di più zone di disponibilità Amazon RDS

AWS Backup esegue il backup e supporta le opzioni di distribuzione di Amazon RDS for MySQL e PostgreSQL Multi-AZ (Availability Zone) con un'istanza di database in standby principale e due istanze di database in standby leggibili.

I backup di più zone di disponibilità sono disponibili nelle regioni seguenti: Asia Pacifico (Sydney), Asia Pacifico (Tokyo), Europa (Irlanda), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Europa (Stoccolma), Asia Pacifico (Singapore), Stati Uniti orientali (Virginia settentrionale) ed Europa (Francoforte).

L'opzione di implementazione Multi-AZ ottimizza le transazioni di scrittura ed è ideale quando i carichi di lavoro richiedono capacità di lettura aggiuntiva, latenza delle transazioni di scrittura più bassa, maggiore resilienza dal jitter di rete (che influisce sulla coerenza della latenza delle transazioni di scrittura) e disponibilità e durabilità elevate.

Per creare un cluster Multi-AZ, puoi scegliere MySQL o PostgreSQL come tipo di motore.

Nella console sono disponibili tre opzioni di distribuzione: AWS Backup

- Cluster DB Multi-AZ: crea un cluster database con un'istanza database principale e due istanze database standby leggibili, ciascuna delle quali si trova in una zona di disponibilità diversa. Fornisce elevata disponibilità, ridondanza dei dati e aumenta la capacità dei carichi di lavoro pronti per il server.
- Istanza database Multi-AZ: crea un'istanza database principale e un'istanza database standby in una zona di disponibilità differente. Ciò garantisce elevata disponibilità e ridondanza dei dati, ma l'istanza database in standby non supporta connessioni per carichi di lavoro di lettura.
- Istanza database singola: crea una singola istanza database senza istanze database in standby.

Per creare un backup per Amazon RDS, consulta Creazione di un backup per la pianificazione di un backup come parte dei piani di backup o la creazione di un backup on demand.

> **Note**
>
> Ripristino point-in-time (PITR) può supportare istanze, ma non cluster.
> La copia di uno snapshot di cluster DB Multi-AZ non è supportata.

Differenze tra un cluster Multi-AZ e un'istanza RDS

Un backup in una singola zona di disponibilità o in due zone di disponibilità è un'istanza RDS; un'implementazione e un backup con tre o più istanze è un cluster, simile ai cluster Amazon Aurora, Amazon Neptune e Amazon DocumentDB.

Il nome della risorsa Amazon (ARN) viene riprodotto in modo diverso a seconda che venga utilizzata l'istanza o il cluster:

Un ARN dell'istanza RDS: `arn:aws:rds:region: account:db:name`

Un cluster in più zone di disponibilità RDS: `arn:aws:rds:region:account :cluster:name`

Per ulteriori informazioni, consulta Implementazioni cluster di database multi-AZ nella Guida per l'utente di Amazon RDS.

Per ulteriori informazioni sulla Creazione di uno snapshot di un cluster di database Multi-AZ, consulta la Guida per l'utente di Amazon RDS.

AWS CloudFormation backup in pila

Uno CloudFormation stack è costituito da più risorse stateful e stateless di cui è possibile eseguire il backup come singola unità. In altre parole, è possibile eseguire il backup e il ripristino di un'applicazione contenente più risorse eseguendo il backup di uno stack e ripristinando le risorse al suo interno. Tutte le risorse di uno stack sono definite dal modello AWS CloudFormation dello stack.

Quando viene eseguito il backup di uno CloudFormation stack, vengono creati punti di ripristino per il CloudFormation modello e per ogni risorsa aggiuntiva supportata dallo stack. AWS Backup Questi punti di ripristino sono raggruppati all'interno di un punto di ripristino complessivo chiamato composito.

Questo punto di ripristino composito non può essere ripristinato, ma è possibile ripristinare punti di ripristino nidificati. È possibile ripristinare ovunque da uno a tutti i backup nidificati all'interno di un backup composito utilizzando la console o AWS CLI.

CloudFormation terminologia dello stack di applicazioni

- Punto di ripristino composito: un punto di ripristino utilizzato per raggruppare punti di ripristino nidificati, nonché altri metadati.
- Punto di ripristino annidato: punto di ripristino di una risorsa che fa parte di uno CloudFormation stack e di cui viene eseguito il backup come parte del punto di ripristino composito. Ogni punto di ripristino nidificato appartiene allo stack di un punto di ripristino composito.
- Job composito: un processo di backup, copia o ripristino per uno CloudFormation stack che può attivare altri processi di backup per singole risorse all'interno dello stack.

- Job annidato: un processo di backup, copia o ripristino per una risorsa all'interno di uno stack. AWS CloudFormation

CloudFormation lavori di backup dello stack

Il processo di creazione di un backup è chiamato processo di backup. Un processo CloudFormation di stack backup ha uno stato. Quando un processo di backup è terminato, lo stato è `Completed`. Ciò significa che è stato creato un AWS CloudFormation punto di ripristino (un backup).

CloudFormation È possibile eseguire il backup degli stack utilizzando la console o eseguirne il backup in modo programmatico. Per eseguire il backup di qualsiasi risorsa, incluso uno CloudFormation stack, consulta Creazione di un backup altrove in questa AWS Backup Guida per gli sviluppatori.

CloudFormation è possibile eseguire il backup degli stack utilizzando il comando API. `StartBackupJob` Tieni presente che la documentazione e la console fanno riferimento a punti di ripristino compositi e nidificati; il linguaggio API utilizza la terminologia "punti di ripristino padre e figlio" nella stessa relazione contestuale.

CloudFormation gli stack contengono tutte AWS le risorse indicate dal modello. CloudFormation Tieni presente che il modello può contenere risorse non ancora supportate da AWS Backup. Se il modello contiene una combinazione di risorse AWS supportate e risorse non supportate, AWS Backup eseguirà comunque il backup del modello in uno stack composito, ma Backup creerà solo punti di ripristino dei servizi supportati da Backup. Tutti i tipi di risorse contenuti nel CloudFormation modello verranno inclusi in un backup, anche se non hai aderito a un servizio particolare (impostando un servizio su «Abilitato» nelle Impostazioni della console). I backup nidificati (punti di ripristino) supportati da AWS Backup possono essere ripristinati, ma non è possibile eseguire il backup o il ripristino degli stack nidificati.

AWS CloudFormation punto di ripristino

Stato del punto di ripristino

Quando il processo di backup di uno stack è terminato (lo stato del processo è `Completed`), viene creato un backup dello stack. Questo backup è anche noto come punto di ripristino composito. Lo stato di un punto di ripristino composito può essere uno dei seguenti: `Completed`, `Failed` o `Partial`. Tieni presente che un processo di backup presenta uno stato e che un punto di ripristino (chiamato anche backup) presenta uno stato separato.

Un processo di backup completato significa che l'intero stack e le risorse in esso contenute sono protetti da AWS Backup. Uno stato non riuscito indica che il processo di backup non è andato a buon fine; è necessario creare nuovamente il backup dopo che il problema che ha causato l'errore è stato risolto.

Uno stato `Partial` indica che non è stato eseguito il backup di tutte le risorse nello stack. Ciò può accadere se il CloudFormation modello contiene risorse che attualmente non sono supportate da AWS Backup, oppure può accadere se uno o più job di backup appartenenti alle risorse all'interno dello stack (risorse annidate) hanno uno stato diverso da. `Completed` Puoi creare manualmente un backup on demand per eseguire nuovamente le eventuali risorse il cui stato è diverso da `Completed`. Se prevedevi che lo stato dello stack fosse `Completed` ma invece è contrassegnato come `Partial`, verifica quale delle condizioni precedenti potrebbe essere vera per lo stack.

Ogni risorsa nidificata all'interno del punto di ripristino composito dispone del proprio punto di ripristino individuale, ciascuno con il proprio stato (`Completed` o `Failed`). I punti di ripristino nidificati con uno stato `Completed` possono essere ripristinati.

Gestione dei punti di ripristino

I punti di ripristino compositi (backup) possono essere copiati; i punti di ripristino nidificati possono essere copiati, eliminati, dissociati o ripristinati. Un punto di ripristino composito che contiene backup nidificati non può essere eliminato. Dopo che i punti di ripristino nidificati all'interno di un punto di ripristino composito sono stati eliminati o dissociati, è possibile eliminare manualmente il punto di ripristino composito o lasciarlo finché non viene eliminato dal ciclo di vita del piano di backup.

Eliminazione di un punto di ripristino

È possibile eliminare un punto di ripristino utilizzando la AWS Backup console o utilizzando. AWS CLI

Per eliminare i punti di ripristino utilizzando la AWS Backup console,

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Fai clic su Risorse protette nella barra di navigazione a sinistra. Nella casella di testo, digita `CloudFormation` per visualizzare solo i tuoi CloudFormation stack.
3. I punti di ripristino compositi verranno visualizzati nel riquadro Punti di ripristino. Puoi fare clic sul segno più (+) a sinistra di ciascun ID del punto di ripristino per espandere ciascun punto di ripristino composito, visualizzando tutti i punti di ripristino nidificati contenuti al suo interno. Puoi selezionare la casella a sinistra di qualsiasi punto di ripristino per includerlo nella selezione dei punti di ripristino che desideri eliminare.

4. Fai clic sul pulsante Elimina bucket.

Quando utilizzi la console per eliminare uno o più punti di ripristino compositi, viene visualizzata una finestra di avviso. Questa finestra di avviso richiede la conferma dell'intenzione di eliminare i punti di ripristino compositi, inclusi i punti di ripristino nidificati all'interno di stack compositi.

Per eliminare i punti di ripristino tramite l'API, utilizza il comando `DeleteRecoveryPoint`.

Quando si utilizza l'API con, AWS Command Line Interface è necessario eliminare tutti i punti di ripristino annidati prima di eliminare un punto composito. Se invii una richiesta API per eliminare un backup dello stack composito (punto di ripristino) che contiene ancora punti di ripristino nidificati, la richiesta restituirà un errore.

Annullare l'associazione di un punto di ripristino nidificato dal punto di ripristino composito

Puoi annullare l'associazione di un punto di ripristino nidificato da un punto di ripristino composito (ad esempio, desideri mantenere il punto di ripristino nidificato ma eliminare il punto di ripristino composito). Entrambi i punti di ripristino verranno mantenuti, ma non saranno più connessi; ovvero, le azioni che si verificano sul punto di ripristino composito non verranno più applicate al punto di ripristino nidificato dopo che l'associazione è stata annullata.

Puoi annullare l'associazione del punto di ripristino utilizzando la console oppure chiamare l'API `DisassociateRecoveryPointFromParent`. [Tieni presente che le chiamate API utilizzano il termine "padre" per fare riferimento a punti di ripristino compositi.]

Copia di un punto di ripristino

È possibile copiare un punto di ripristino composito oppure copiare un punto di ripristino annidato se la risorsa supporta la copia tra account e più regioni.

Per copiare i punti di ripristino utilizzando la console: AWS Backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Fai clic su Risorse protette nella barra di navigazione a sinistra. Nella casella di testo, digita `CloudFormation` per visualizzare solo i tuoi CloudFormation stack.
3. I punti di ripristino compositi verranno visualizzati nel riquadro Punti di ripristino. Puoi fare clic sul segno più (+) a sinistra di ciascun ID del punto di ripristino per espandere ciascun punto di ripristino composito, visualizzando tutti i punti di ripristino nidificati contenuti al suo interno. Puoi fare clic sul pulsante circolare radiale a sinistra di qualsiasi punto di ripristino per copiarlo.

4. Dopo che è stato selezionato, fai clic sul pulsante Copia nell'angolo in alto a destra del riquadro.

Quando copi un punto di ripristino composito, i punti di ripristino nidificati che non supportano la funzionalità di copia non finiranno nello stack copiato. Lo stato del punto di ripristino composito sarà `Partial`.

Domande frequenti

1. "Cosa è incluso come parte del backup dell'applicazione?"

   Come parte di ogni backup di un'applicazione definita utilizzando CloudFormation, viene eseguito il backup del modello, del valore elaborato di ogni parametro nel modello e delle risorse annidate AWS Backup supportate da. Il backup di una risorsa annidata viene eseguito nello stesso modo in cui viene eseguito il backup di una singola risorsa che non fa parte di uno CloudFormation stack. Tieni presente che i valori dei parametri contrassegnati come `no-echo` non vengono sottoposti a backup.

2. «Posso eseguire il backup del mio AWS CloudFormation stack con stack annidati?»

   Sì. I tuoi CloudFormation stack che contengono stack annidati possono essere nel tuo backup.

3. "Uno stato *`Partial`* significa che la creazione del backup non è andata buon fine?"

   No. Uno stato parziale indica che è stato eseguito il backup solo di alcuni punti di ripristino. Esistono tre condizioni per verificare se il risultato di backup atteso era `Completed`:

   a. Il tuo CloudFormation stack contiene risorse attualmente non supportate da? AWS Backup Per un elenco delle risorse supportate, consulta AWS Risorse supportate e applicazioni di terze parti nella nostra Guida per gli sviluppatori.

   b. Uno o più processi di backup appartenenti a risorse all'interno dello stack non sono andati a buon fine ed è necessario eseguire nuovamente il processo.

   c. Un punto di ripristino nidificato è stato eliminato o dissociato dal punto di ripristino composito.

4. «Come posso escludere le risorse dal mio CloudFormation stack backup?»

   Quando esegui il backup CloudFormation dello stack, puoi escludere le risorse dal backup. Nella console, durante i processi di creazione di un piano di backup e aggiornamento di un piano di backup, è previsto un passaggio di assegnazione delle risorse. In questo passaggio, esiste una sezione Selezione delle risorse. Se scegli di includere tipi di risorse specifici e di averle incluse

CloudFormation come risorsa di backup, puoi escludere ID di risorse specifici dai tipi di risorse selezionati. Puoi anche utilizzare i tag per escludere risorse all'interno dello stack.

Utilizzando CLI, puoi utilizzare

- `NotResources`nel piano di backup per escludere una risorsa specifica dagli CloudFormation stack.
- `StringNotLike` per escludere elementi tramite tag.

5. "Quali tipi di backup sono supportati per le risorse nidificate?"

   I backup delle risorse annidate possono essere backup completi o incrementali, a seconda del tipo di backup supportato per tali risorse. AWS Backup Per ulteriori informazioni, consulta Come funzionano i backup incrementali. Tuttavia, tieni presente che PITR (point-in-time ripristino) non è supportato per le risorse annidate di Amazon S3 e Amazon RDS.

6. «I set di modifiche che fanno parte dello CloudFormation stack sono sottoposti a backup?»

   No. Il backup dei set di modifiche non viene eseguito come parte del backup CloudFormation dello stack.

7. «In che modo lo stato dello AWS CloudFormation stack influisce sul backup?»

   Lo stato dello CloudFormation stack può influire sul backup. È possibile eseguire il backup di uno stack con uno stato che include `COMPLETE`, ad esempio gli stati `CREATE_COMPLETE`, `ROLLBACK_COMPLETE`, `UPDATE_COMPLETE`, `UPDATE_ROLLBACK_COMPLETE`, `IMPORT_COMPLETE` o `IMPORT_ROLLBACK_COMPLETE`.

   Se si verifica un problema durante il caricamento di un nuovo modello e lo stack passa nello stato `ROLLBACK_COMPLETE`, verrà eseguito il backup del nuovo modello, ma i backup delle risorse nidificate si baseranno sulle risorse sottoposte al roolback.

8. "In che modo i cicli di vita dello stack delle applicazioni differiscono dagli altri cicli di vita dei punti di ripristino?"

   I cicli di vita dei punti di ripristino nidificati sono determinati dal piano di backup a cui appartengono. Il punto di ripristino composito è determinato dal ciclo di vita più lungo di tutti i punti di ripristino nidificati. Quando l'ultimo punto di ripristino nidificato rimasto all'interno di un punto di ripristino composito viene eliminato o dissociato, viene eliminato anche il punto di ripristino composito.

9. «Come vengono CloudFormation copiati i tag di un file nei punti di ripristino?»

   Sì. Questi tag verranno copiati in ogni rispettivo punto di ripristino nidificato.

10. "Esiste un ordine per l'eliminazione dei punti di ripristino compositi e nidificati (backup)?"

    Sì. Alcuni backup devono essere eliminati prima che sia possibile eliminare altri. I backup compositi contenenti punti di ripristino nidificati non possono essere eliminati finché tutti i punti di ripristino all'interno del backup composito non sono stati eliminati. Una volta che un punto di ripristino composito non contiene più punti di ripristino nidificati, è possibile eliminarlo manualmente. In caso contrario, verrà eliminato in base al relativo ciclo di vita del piano di backup.

Ripristino delle applicazioni all'interno di uno stack

Per informazioni sul ripristino di punti di ripristino nidificati, consulta Come ripristinare i backup degli stack di applicazioni.

Creazione di backup Windows VSS

Con AWS Backup, puoi eseguire il backup e il ripristino di applicazioni Windows abilitate per VSS (Volume Shadow Copy Service) in esecuzione su istanze Amazon EC2. Se l'applicazione ha VSS writer registrato con Windows VSS, AWS Backup crea un'istantanea che sarà coerente per quell'applicazione.

È possibile eseguire ripristini coerenti, utilizzando lo stesso servizio di backup gestito utilizzato per proteggere altre risorse. AWS Con i backup Windows coerenti con le applicazioni su EC2, ottieni le stesse impostazioni di coerenza e la stessa consapevolezza delle applicazioni degli strumenti di backup tradizionali.

> **Note**
>
> AWS Backup attualmente supporta solo backup coerenti con le applicazioni delle risorse in esecuzione su Amazon EC2, in particolare scenari di backup in cui i dati delle applicazioni possono essere ripristinati sostituendo un'istanza esistente con una nuova istanza creata dal backup. Non tutti i tipi di istanze o applicazioni sono supportati per i backup di Windows VSS.

Per ulteriori informazioni, consulta Creating a Application-Consistent Snapshot VSS nella Guida per l'utente di Amazon EC2.

Per eseguire il backup e il ripristino delle risorse Windows con tecnologia VSS che eseguono Amazon EC2, segui questi passaggi per completare le attività preliminari richieste. Per istruzioni, consulta Prerequisiti nella Guida per l'utente delle istanze Windows di Amazon EC2.

1. Scarica, installa e configura l'agente SSM in. AWS Systems Manager Questo passaggio è obbligatorio. Per istruzioni, consulta Working with SSM agent on Amazon EC2 for Windows Server nella Systems AWS Manager User Guide.
2. Aggiungi una policy IAM al ruolo IAM e associa il ruolo all'istanza Amazon EC2 prima di eseguire il backup di Windows VSS (Volume Shadow Copy Service). Per istruzioni, consulta Create an IAM Role for Snapshot abilitati per VSS nella Guida per l'utente di Amazon EC2. Per un esempio della policy IAM, consulta Politiche gestite per AWS Backup.
3. Download e installazione di componenti VSS nell'istanza Windows su Amazon EC2
4. Abilita AWS Backup VSS in:

    1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
    2. Nel pannello di controllo, scegli il tipo di backup che desideri creare, Crea un backup on demand o Gestisci i piani di backup. Fornisci le informazioni necessarie per il tipo di backup.
    3. Quando assegni risorse, scegli EC2. Il backup Windows VSS è attualmente supportato solo per istanze EC2.
    4. Nella sezione Impostazioni avanzate, scegli Windows VSS. Ciò consente di eseguire backup di Windows VSS coerenti con le applicazioni.
    5. Crea il backup.

Un processo di backup con uno stato `Completed` non garantisce che la parte VSS vada a buon fine; l'inclusione di VSS viene effettuata nel miglior modo possibile. Procedi con i seguenti passaggi per determinare se un backup è coerente con le applicazioni, crash-consistent o non riuscito:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. In Il mio account, nella barra di navigazione a sinistra, fai clic su Processi.
3. Uno stato `Completed` indica un processo riuscito coerente con le applicazioni (VSS).

    Uno stato `Completed with issues` indica che l'operazione VSS non è andata buon fine, pertanto solo un backup crash-consistent è stato completato. A questo stato è associato anche

un messaggio popover "`Windows VSS Backup Job Error encountered, trying for regular backup`".

Se il backup non è andato a buon fine, lo stato sarà `Failed`.

4. Per visualizzare ulteriori dettagli del processo di backup, fai clic sul singolo processo. Ad esempio, i dettagli potrebbero riportare `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`.

I backup abilitati per VSS con una destinazione diversa da Windows o un componente non VSS Windows che ha esito positivo saranno coerenti con gli arresti anomali senza VSS.

Istanze Amazon EC2 non supportate

I seguenti tipi di istanze Amazon EC2 non sono supportati per i backup Windows con tecnologia VSS perché sono istanze di piccole dimensioni e potrebbero non eseguire il backup correttamente.

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

Amazon EBS e AWS Backup

Il processo di backup per le risorse Amazon EBS è simile ai passaggi utilizzati per eseguire il backup di altri tipi di risorse:

- Creazione di un backup on demand
- Creazione di un backup pianificato

Le informazioni specifiche delle risorse sono riportate nelle sezioni seguenti.

Livello di archiviazione di Amazon EBS per l'archiviazione a freddo

EBS supporta la transizione dei backup all'archiviazione a freddo. Per ulteriori informazioni, consulta Ciclo di vita e livelli di archiviazione.

> **Note**
>
> Questa funzionalità non è disponibile nelle regioni Cina (Pechino), Cina (Ningxia), (Stati Uniti orientali) e AWS GovCloud AWS GovCloud (Stati Uniti occidentali).

Backup multi-volume crash-consistent Amazon EBS

Per impostazione predefinita, AWS Backup crea backup coerenti in caso di crash dei volumi Amazon EBS collegati a un'istanza Amazon EC2. Crash-consistent significa che gli snapshot per ogni volume Amazon EBS collegato alla stessa istanza Amazon EC2 vengono acquisiti esattamente nello stesso momento. Non è più necessario interrompere le istanze o coordinarsi tra più volumi Amazon EBS per garantire che lo stato dell'applicazione sia crash-consistent.

Poiché le istantanee multivolume e resistenti agli arresti anomali sono una AWS Backup funzionalità predefinita, non è necessario fare nulla di diverso per utilizzare questa funzionalità. Puoi eseguire il backup di volumi Amazon EBS utilizzando una delle procedure seguenti:

Il ruolo utilizzato per creare un punto di ripristino delle istantanee EBS verrà associato a tale istantanea. Lo stesso ruolo deve essere utilizzato per eliminare i punti di ripristino da esso creati o per trasferire i punti di ripristino a un livello di archiviazione.

Amazon EBS Snapshot Lock e AWS Backup

AWS Backup gli snapshot gestiti di Amazon EBS e gli snapshot associati a un'AMI AWS Backup Amazon EC2 gestita a cui è applicato Amazon EBS Snapshot Lock non possono essere eliminati come parte del ciclo di vita del punto di ripristino se la durata del blocco degli snapshot supera il ciclo di vita del backup. Questi punti di ripristino avranno lo stato `EXPIRED`. Possono essere eliminati manualmente se scegli di rimuovere prima lo Snapshot Lock di Amazon EBS.

Ripristino delle risorse Amazon EBS

Per ripristinare i volumi Amazon EBS, segui i passaggi riportati in Ripristino di un volume Amazon EBS.

Copia di tag nei backup

In generale, copia i tag dalle risorse che protegge ai punti di ripristino AWS Backup . Per ulteriori informazioni su come copiare i tag durante un ripristino, consulta Copia i tag durante un ripristino.

Ad esempio, quando esegui il backup di un volume Amazon EC2, ne AWS Backup copia i tag di risorsa di gruppo e individuali nello snapshot risultante, in base a quanto segue:

- Per un elenco delle autorizzazioni specifiche della risorsa che sono richieste per salvare i tag dei metadati nei backup, consulta Autorizzazioni necessarie per assegnare tag ai backup.
- I tag originariamente associati a una risorsa e i tag assegnati durante il backup vengono assegnati ai punti di ripristino archiviati in un archivio di backup, fino a un massimo di 50 (questa è una AWS limitazione). I tag assegnati durante il backup hanno la priorità ed entrambi i set di tag vengono copiati in ordine alfabetico.
- DynamoDB non supporta l'assegnazione di tag ai backup a meno che non venga prima abilitato Backup di DynamoDB avanzato.
- I volumi Amazon EBS collegati alle istanze Amazon EC2 sono risorse nidificate. I tag sui volumi Amazon EBS collegati alle istanze Amazon EC2 sono tag annidati. AWS Backup fa del suo meglio per copiare i tag annidati, ma se non riesce, crea un backup senza di essi e riporta lo stato di completamento.
- Quando un backup Amazon EC2 crea un punto di ripristino dell'immagine e un set di istantanee, AWS Backup copia i tag nell'AMI risultante. AWS Backup fa inoltre del suo meglio per copiare i tag dai volumi associati all'istanza Amazon EC2 negli snapshot risultanti.

Se copi il backup su un altro Regione AWS, AWS Backup copia tutti i tag del backup originale nella destinazione. Regione AWS

Arresto di un processo di backup

È possibile interrompere un processo di backup AWS Backup dopo che è stato avviato. In questo modo il backup non viene creato e il record del processo di backup viene conservato con lo stato di aborted (interrotto).

Per interrompere un processo di backup utilizzando la console AWS Backup

1. Accedere a e aprire la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup. AWS Management Console
2. Nel riquadro di navigazione sinistro scegliere Processi.
3. Scegliere il processo di backup che si desidera arrestare.
4. Nel riquadro dei dettagli del processo di backup scegliere Stop (Arresta).

Copia di un backup

È possibile copiare i backup su più backup Account AWS o Regioni AWS su richiesta o automaticamente come parte di un piano di backup pianificato per la maggior parte dei tipi di risorse. Per informazioni specifiche, vedere. the section called “Disponibilità delle funzionalità per risorsa”

Puoi anche automatizzare una sequenza di copie in più account e più regioni per la maggior parte delle risorse supportate, ad eccezione di Amazon RDS e Aurora. Per le istantanee di Amazon RDS e Aurora AWS Backup , supporta solo l'automazione delle copie tra account o più regioni, a causa del modo in cui tali servizi creano le proprie chiavi di crittografia (la copia di uno snapshot del cluster DB Multi-AZ non è supportata).

Alcuni tipi di risorse dispongono della funzionalità di backup continuo e di quella di copia in più regioni e in più account. Quando si esegue una copia in più regioni o in più account di un backup continuo, il punto di ripristino copiato (backup) diventa un backup (periodico) snapshot. A seconda del tipo di risorsa, le istantanee possono essere una copia incrementale o una copia completa. PITR (ripristino point-in-time) non è disponibile per queste copie.

Le copie mantengono la configurazione di origine, incluse le date di creazione e il periodo di conservazione. La data di creazione si riferisce a quando è stata creata la fonte, non a quando è stata creata la copia.

NOTA: la configurazione di origine sostituisce l'impostazione di scadenza della copia, anche se la copia è impostata per non scadere mai; una copia impostata per non scadere mai manterrà comunque la data di scadenza dell'origine.

Se le copie di backup non devono mai scadere, imposta i backup di origine in modo che non scadano mai o specifica che la copia scada 100 anni dopo la sua creazione.

Indice

Creazione di copie di backup in tutto Regioni AWS

Utilizzando AWS Backup, è possibile copiare i backup Regioni AWS su più backup su richiesta o automaticamente come parte di un piano di backup pianificato. La replica tra regioni è particolarmente utile se si hanno requisiti di continuità aziendale o di conformità per archiviare i

backup a una distanza minima dai dati di produzione. Per un tutorial video, consulta Managing cross-Region copies of backups.

Quando si copia un backup su uno nuovo Regione AWS per la prima volta, AWS Backup copia il backup per intero. In generale, se un servizio supporta backup incrementali, le copie successive di quel backup nello stesso Regione AWS saranno incrementali. AWS Backup crittograferà nuovamente la copia utilizzando la chiave gestita dal cliente del vault di destinazione.

Un'eccezione è Amazon EBS, che afferma che, la modifica dello stato di crittografia di uno snapshot durante un'operazione di copia comporta una copia completa (non incrementale).

Requisiti

- La maggior parte delle risorse AWS Backup supportate supporta il backup interregionale. Per le specifiche, consulta Disponibilità delle funzionalità per risorsa.
- La maggior parte delle AWS regioni supporta il backup interregionale. Per le specifiche, consulta Disponibilità delle funzionalità tramite Regione AWS.
- AWS Backup non supporta copie interregionali per l'archiviazione su livelli freddi.

Considerazioni sulla copia in più regioni con risorse specifiche

Amazon RDS

Non è possibile copiare un gruppo di opzioni in un altro. Regione AWS Se si tenta di farlo, è possibile che venga visualizzato un errore, ad esempio «L'istantanea richiede un gruppo di opzioni di destinazione con le seguenti opzioni:...»

È necessario inserire gli stessi gruppi di opzioni nella destinazione Regione AWS quando si crea una nuova copia interregionale di uno snapshot Amazon RDS.

Esecuzione di backup tra regioni on demand

Per copiare on demand un backup esistente

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Scegliere Vault di Backup.
3. Scegli il vault contenente il punto di ripristino che desideri copiare.
4. Nella sezione Backup, seleziona un punto di ripristino da copiare.

5. Utilizzando il pulsante a discesa Azioni, scegli Copia.
6. Immetti uno dei seguenti valori:

   Copia nella destinazione

   Scegliete la destinazione Regione AWS per la copia. È possibile aggiungere una nuova regola di copia per ciascuna copia in una nuova destinazione.

   Vault di back di destinazione

   Scegliere il vault di backup di destinazione per la copia.

   Transizione allo storage a freddo

   Scegli quando eseguire la transizione della copia di backup allo storage a freddo. I backup trasferiti allo storage dei dati inattivi devono essere archiviati per un minimo di 90 giorni. Questo valore non può essere modificato dopo il trasferimento di una copia allo storage a freddo.

   Per visualizzare l'elenco di risorse che è possibile trasferire nell'archiviazione a freddo, consulta la sezione "Dal ciclo di vita all'archiviazione a freddo" della tabella Disponibilità delle funzionalità per risorsa. L'espressione archiviazione a freddo viene ignorata per le altre risorse.

   Periodo di conservazione

   Scegli specifica il numero di giorni dopo la creazione prima che la copia venga eliminata. Questo valore deve essere maggiore di 90 giorni rispetto al valore di Transizione allo storage a freddo. Il periodo di conservazione Sempre mantiene la copia a tempo indeterminato.

   Ruolo IAM

   Scegli il ruolo IAM da utilizzare durante la creazione della copia. AWS Backup Il ruolo deve inoltre essere AWS Backup elencato come entità attendibile, che consente AWS Backup di assumere il ruolo. Se scegli Predefinito e il ruolo AWS Backup predefinito non è presente nel tuo account, ne verrà creato uno con le autorizzazioni corrette.
7. Scegli Copia.

Pianificazione del backup tra regioni

Puoi utilizzare un piano di backup pianificato per copiare i backup in più Regioni AWS.

Per copiare un backup utilizzando un piano di backup pianificato

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. In Il mio account, scegli Piani di backup, quindi scegli Crea un piano di backup.
3. Nella pagina Crea un piano di backup, scegli Crea un nuovo piano.
4. In Nome del piano di backup, inserisci il nome del piano di backup.
5. Nella sezione Configurazione regola di backup, aggiungi una regola di backup che definisce una pianificazione di backup, una finestra di backup e regole del ciclo di vita. Puoi aggiungere altre regole di backup in un secondo momento.

   a. In Nome, inserisci un nome per la regola.

   b. In Vault di backup, scegli un vault dall'elenco. I punti di ripristino per questo backup verranno salvati in questo vault. Puoi creare un nuovo vault di backup.

   c. Per Frequenza di backup, scegli la frequenza con cui desideri eseguire i backup.

   d. Per i servizi che supportano PITR, se desideri questa funzionalità, scegli Abilita backup continui per il point-in-time ripristino (PITR). Per un elenco dei servizi che supportano PITR, consulta la sezione corrispondente della tabella Disponibilità delle funzionalità per risorsa.

   e. In Finestra di backup, scegli Utilizza le impostazioni predefinite della finestra di backup - scelta consigliata. Puoi personalizzare la finestra di backup.

   f. In Copia nella destinazione, scegli la destinazione Regione AWS per la copia di backup. Il backup verrà copiato in questa regione. È possibile aggiungere una nuova regola di copia per ciascuna copia in una nuova destinazione. Quindi, inserisci uno dei seguenti valori:

      Copia nel vault di un altro account

      Non attivare questa opzione. Per ulteriori informazioni sulla copia tra account, consulta Creazione di copie di backup su più account Account AWS

      Vault di back di destinazione

      Scegli l'archivio di backup nella regione di destinazione in cui copiare AWS Backup il backup.

      Se desideri creare un nuovo vault di backup per la copia in più regioni, scegli Crea nuovo vault di backup. Inserisci le informazioni nella procedura guidata. Quindi scegli Crea vault di backup.

6. Seleziona Crea piano.

Creazione di copie di backup in tutto Account AWS

Utilizzando AWS Backup, è possibile eseguire il backup di più copie Account AWS su richiesta o automaticamente come parte di un piano di backup pianificato. Utilizza un backup su più account se desideri copiare in modo sicuro i backup su uno o più Account AWS account dell'organizzazione per motivi operativi o di sicurezza. Se il backup originale viene eliminato inavvertitamente, puoi copiare il backup dall'account di destinazione all'account di origine e quindi avviare il ripristino. Prima di farlo, devi disporre di due account appartenenti alla stessa organizzazione nel servizio AWS Organizations . Per ulteriori informazioni, consulta Tutorial: creazione e configurazione di un'organizzazione nella Guida per l'utente di .

Un vault di backup deve essere creato nell'account di destinazione. Quindi, assegni una chiave gestita dal cliente per crittografare i backup nell'account di destinazione e una politica di accesso basata sulle risorse per consentire AWS Backup l'accesso alle risorse che desideri copiare. Nell'account di origine, se le risorse sono crittografate con una chiave gestita dal cliente, questa deve essere condivisa con l'account di destinazione. Puoi quindi creare un piano di backup e scegliere un account di destinazione che fa parte dell'unità organizzativa in AWS Organizations.

Quando copi un backup su più account per la prima volta, copia il backup per intero. AWS Backup In generale, se un servizio supporta i backup incrementali, le copie successive di quel backup nello stesso account sono incrementali. AWS Backup cripta nuovamente la copia utilizzando la chiave gestita dal cliente del vault di destinazione.

Requisiti

- Prima di gestire le risorse su più Account AWS account AWS Backup, gli account devono appartenere alla stessa organizzazione del servizio. AWS Organizations
- La maggior parte delle risorse supportate da AWS Backup supporta il backup su più account. Per le specifiche, consulta Disponibilità delle funzionalità per risorsa.
- La maggior parte AWS delle regioni supporta il backup su più account. Per le specifiche, consulta Disponibilità delle funzionalità tramite Regione AWS.
- AWS Backup non supporta copie su più account per l'archiviazione su livelli freddi.

Configurazione del backup tra account

Che cosa occorre per creare backup tra account?

- Un account di origine

L'account di origine è l'account in cui risiedono le AWS risorse di produzione e i backup principali.

L'utente dell'account di origine avvia l'operazione di backup tra account. L'utente o il ruolo dell'account di origine deve disporre delle autorizzazioni API appropriate per avviare l'operazione. Le autorizzazioni appropriate possono essere la politica AWS gestita`AWSBackupFullAccess`, che consente l'accesso completo alle AWS Backup operazioni, o una politica gestita dal cliente che consente azioni come. `ec2:ModifySnapshotAttribute` Per ulteriori informazioni sui tipi di policy, consulta Policy gestite da AWS Backup.

- Un account di destinazione

  L'account di destinazione è quello in cui desideri mantenere una copia del backup. Puoi scegliere più di un account di destinazione. L'account di destinazione deve trovarsi nella stessa organizzazione dell'account di origine in AWS Organizations.

  È necessario "Consentire" la policy di accesso `backup:CopyIntoBackupVault` per il vault di backup di destinazione. L'assenza di questa policy impedirà i tentativi di copia nell'account di destinazione.

- Un account di gestione in AWS Organizations

  L'account di gestione è l'account principale dell'organizzazione, come definito da AWS Organizations, utilizzato per gestire il backup tra account in più Account AWS. Per utilizzare il backup tra account, occorre inoltre abilitare l'affidabilità del servizio. Dopo aver abilitato l'affidabilità del servizio, puoi utilizzare qualsiasi account dell'organizzazione come un account di destinazione. Dall'account di destinazione, puoi scegliere quali vault utilizzare per il backup tra account.

- Abilitare il backup tra account nella console AWS Backup

Per ulteriori informazioni sulla sicurezza, consulta Considerazioni di sicurezza per il backup tra account.

Per utilizzare il backup tra account, è necessario abilitare la funzionalità di backup tra account. Quindi, è necessario "Consentire" la policy di accesso `backup:CopyIntoBackupVault` nel vault di backup di destinazione.

Abilita il backup su più account

1. Accedi utilizzando le credenziali AWS Organizations del tuo account di gestione. Il backup tra account può essere abilitato o disabilitato solo utilizzando queste credenziali.

2. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
3. In Il mio account, scegli Impostazioni.
4. In Backup tra account, scegli Abilita.
5. In Vault di backup, scegli il vault di destinazione.

   Per la copia su più account, il vault di origine e il vault di destinazione si trovano in account diversi. Passa all'account proprietario dell'account di destinazione, se necessario.
6. Nella sezione Policy di accesso, "Consentire" `backup:CopyIntoBackupVault`.
   Ad esempio, scegli Aggiungi autorizzazioni e quindi Consenti l'accesso a un vault di backup dall'organizzazione. Qualsiasi azione tra account diversa da quella effettuata `backup:CopyIntoBackupVault` verrà rifiutata.
7. Ora, qualsiasi account dell'organizzazione può condividere i contenuti del vault di backup con qualsiasi altro account dell'organizzazione. Per ulteriori informazioni, consulta Condivisione di un vault di backup con un account AWS diverso. Per limitare gli account che possono ricevere il contenuto dai vault di backup di altri account, consulta Configurazione dell'account come un account di destinazione.

Pianificazione del backup tra account

Puoi utilizzare un piano di backup pianificato per copiare i backup in più Account AWS.

Per copiare un backup utilizzando un piano di backup pianificato

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. In Il mio account, scegli Piani di backup, quindi scegli Crea un piano di backup.
3. Nella pagina Crea un piano di backup, scegli Crea un nuovo piano.
4. In Nome del piano di backup, inserisci il nome del piano di backup.
5. Nella sezione Configurazione regola di backup, aggiungi una regola di backup che definisce una pianificazione di backup, una finestra di backup e regole del ciclo di vita. Puoi aggiungere altre regole di backup in un secondo momento.

   In Nome regola, inserisci un nome per la regola.
6. Nella sezione Pianificazione, in Frequenza, scegli la frequenza desiderata di esecuzione del backup.
7. In Finestra di backup, scegli Utilizza le impostazioni predefinite della finestra di backup (scelta consigliata). Puoi personalizzare la finestra di backup.

8. In Vault di backup, scegli un vault dall'elenco. I punti di ripristino per questo backup verranno salvati in questo vault. Puoi creare un nuovo vault di backup.
9. Nella sezione Genera copia - facoltativa, inserisci i seguenti valori:

   Regione di destinazione

   Scegli la destinazione Regione AWS per la tua copia di backup. Il backup verrà copiato in questa regione. È possibile aggiungere una nuova regola di copia per ciascuna copia in una nuova destinazione.

   Copia nel vault di un altro account

   Attiva per scegliere questa opzione. L'opzione diventa blu quando è selezionata. Verrà visualizzata l'opzione ARN di vault esterno.

   ARN di vault esterno

   Inserisci il nome della risorsa Amazon (ARN) dell'account di destinazione. L'ARN è una stringa che contiene l'ID dell'account e il relativo. Regione AWS AWS Backup copierà il backup nel vault dell'account di destinazione. L'elenco delle regioni di destinazione viene aggiornato automaticamente alla regione nell'ARN del vault esterno.

   In Consenti l'accesso al vault di backup, scegli Consenti. Quindi scegli Consenti nella procedura guidata visualizzata.

   AWS Backup necessita delle autorizzazioni per accedere all'account esterno per copiare il backup sul valore specificato. La procedura guidata mostra il seguente esempio di policy che fornisce questo accesso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow account to copy into backup vault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      }
    }
  ]
```

```
}
```

Transizione allo storage a freddo

Scegliere quando trasferire la copia di backup allo storage a freddo e la scadenza (eliminazione) della copia. I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Questo valore non può essere modificato dopo il trasferimento di una copia allo storage a freddo.

Per visualizzare l'elenco di risorse che è possibile trasferire nell'archiviazione a freddo, consulta la sezione "Dal ciclo di vita all'archiviazione a freddo" della tabella Disponibilità delle funzionalità per risorsa. L'espressione archiviazione a freddo viene ignorata per le altre risorse.

Scadenza specifica il numero di giorni dopo la creazione prima che la copia venga eliminata. Questo valore deve essere maggiore di 90 giorni rispetto al valore di Transizione allo storage a freddo.

> **Note**
>
> Quando i backup scadono e sono contrassegnati per l'eliminazione come parte della politica del ciclo di vita, AWS Backup elimina i backup in un momento scelto casualmente nelle 8 ore successive. Questa finestra aiuta a garantire prestazioni costanti.

10. Scegli Tag aggiunti ai punti di ripristino per aggiungere tag ai punti di ripristino.
11. Per Modifica le impostazioni di backup avanzate, scegli Windows VSS per abilitare snapshot coerenti con l'applicazione per il software di terze parti selezionato in esecuzione su EC2.
12. Seleziona Crea piano.

Esecuzione di backup tra account on demand

È possibile copiare un backup su un altro su richiesta. Account AWS

Per copiare un backup on demand

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.

2. In Il mio account, scegli Vault di backup per visualizzare tutti i vault di backup elencati. Puoi filtrare in base al nome o al tag del vault di backup.
3. Scegli l'ID punto di ripristino del backup che desideri copiare.
4. Scegli Copia.
5. Espandi Dettagli del backup per visualizzare le informazioni sul punto di ripristino che stai copiando.
6. Nella sezione Copia configurazione, scegli un'opzione dall'elenco Regione di destinazione.
7. Scegli Copia nel vault di un altro account. L'opzione diventa blu quando è selezionata.
8. Inserisci il nome della risorsa Amazon (ARN) dell'account di destinazione. L'ARN è una stringa che contiene l'ID dell'account e il relativo. Regione AWS AWS Backup copierà il backup nel vault dell'account di destinazione. L'elenco delle regioni di destinazione viene aggiornato automaticamente alla regione nell'ARN del vault esterno.
9. In Consenti l'accesso al vault di backup, scegli Consenti. Quindi scegli Consenti nella procedura guidata visualizzata.

   Per creare la copia, sono AWS Backup necessarie le autorizzazioni per accedere all'account di origine. La procedura guidata mostra una policy di esempio che fornisce questo accesso. Questa policy viene mostrata di seguito.

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "Allow account to copy into backup vault",
         "Effect": "Allow",
         "Action": "backup:CopyIntoBackupVault",
         "Resource": "*",
         "Principal": {
           "AWS": "arn:aws:iam::account-id:root"
         }
       }
     ]
   }
   ```

10. In Transizione allo storage a freddo, scegli quando trasferire la copia di backup allo storage a freddo e la scadenza (eliminazione) della copia. I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Questo valore non può essere modificato dopo il trasferimento di una copia allo storage a freddo.

Per visualizzare l'elenco di risorse che è possibile trasferire nell'archiviazione a freddo, consulta la sezione "Dal ciclo di vita all'archiviazione a freddo" della tabella Disponibilità delle funzionalità per risorsa. L'espressione archiviazione a freddo viene ignorata per le altre risorse.

Scadenza specifica il numero di giorni dopo la creazione prima che la copia venga eliminata. Questo valore deve essere maggiore di 90 giorni rispetto al valore di Transizione allo storage a freddo.

11. Per Ruolo IAM, specifica il ruolo IAM (ad esempio il ruolo predefinito) che dispone delle autorizzazioni per rendere il backup disponibile per la copia. L'operazione di copia viene eseguita dal ruolo collegato al servizio dell'account di destinazione.
12. Scegli Copia. A seconda delle dimensioni della risorsa da copiare, il completamento di questo processo potrebbe richiedere diverse ore. Al termine del processo di copia, la copia verrà visualizzata nella scheda Copia processi del menu Processi.

Chiavi di crittografia e copie tra account

La chiave di crittografia delle copie tra account dipende dal tipo di risorsa. Risorse che hanno Gestione completa AWS Backup utilizzato la chiave di crittografia dell'archivio di backup di origine. Le chiavi KMS gestite dal cliente possono essere utilizzate per la crittografia delle copie tra account diversi di questi tipi di risorse.

I tipi di risorse che non sono completamente gestiti da AWS Backup hanno la stessa chiave KMS di origine e la stessa chiave KMS di risorsa. La copia su più account con chiavi KMS AWS gestite non è supportata per questi tipi di risorse che non sono completamente gestite da. AWS Backup

Per ulteriore assistenza nella risoluzione degli errori di copia su più account, consulta il Knowledge Center.AWS

Durante una copia su più account, la politica delle chiavi KMS dell'account di origine deve consentire l'accesso all'account di destinazione sulla politica delle chiavi KMS.

Ripristino di un backup da uno all'altro Account AWS

AWS Backup non supporta il ripristino delle risorse da una Account AWS all'altra. Tuttavia, puoi copiare un backup da un account a un account differente e ripristinarlo in tale account. Ad esempio, non è possibile ripristinare un backup dall'account A all'account B, ma è possibile copiare un backup dall'account A all'account B e quindi ripristinarlo nell'account B.

Il ripristino di un backup da un account a un altro è un processo in due fasi.

Per ripristinare un backup da un account a un altro

1. Copia il backup dall'origine Account AWS all'account su cui desideri eseguire il ripristino. Per istruzioni, consulta Configurazione del backup tra account.
2. Utilizza le istruzioni appropriate per la risorsa per ripristinare il backup.

Condivisione di un vault di backup con un account AWS diverso

AWS Backup consente di condividere un vault di backup con uno o più account o con l'intera organizzazione. AWS Organizations Puoi condividere un vault di backup di destinazione con un account AWS di origine, un utente o un ruolo IAM.

Per condividere un vault di backup di destinazione

1. Scegli AWS Backup, quindi seleziona Vault di backup.
2. Scegli il nome del vault di backup che desideri condividere.
3. Nel riquadro Policy di accesso, scegli il menu a discesa Aggiungi autorizzazioni.
4. Scegli Consenti l'accesso a livello di account a un vault di backup. In alternativa, puoi scegliere di consentire l'accesso a livello di organizzazione o a livello di ruolo.
5. Inserisci l'AccountID dell'account che desideri condividere con questo vault di backup di destinazione.
6. Scegli Salva policy.

Puoi utilizzare le policy IAM per condividere il vault di backup.

Condivisione di un vault di backup di destinazione con un Account AWS o un ruolo IAM

La seguente policy condivide un vault di backup con numero di account `444455566666` e il ruolo IAM `SomeRole` nel numero di account `111122223333`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
```

```
      "Principal":{
        "AWS":[
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
        ]
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*"
    }
  ]
}
```

Condividi un archivio di backup di destinazione in cui risiede un'unità organizzativa. AWS Organizations

La seguente policy condivide un vault di backup con le unità organizzative utilizzando `PrincipalOrgPaths`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAnyValue:StringLike":{
          "aws:PrincipalOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

Condividi un archivio di backup di destinazione con un'organizzazione in AWS Organizations

La seguente policy condivide un vault di backup con l'organizzazione con `PrincipalOrgID` "o-a1b2c3d4e5".

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

Configurazione dell'account come un account di destinazione

Quando abiliti per la prima volta i backup tra account utilizzando il tuo account di AWS Organizations gestione, qualsiasi utente di un account membro può configurare il proprio account come account di destinazione. Ti consigliamo di impostare una o più delle seguenti policy di controllo dei servizi in AWS Organizations per limitare gli account di destinazione. Per ulteriori informazioni su come allegare le politiche di controllo del servizio ai AWS Organizations nodi, consulta Allegare e scollegare le politiche di controllo del servizio.

Limitazione degli account di destinazione utilizzando tag

Se collegata a un account AWS Organizations principale, a un'unità organizzativa o a un account individuale, questa politica limita le destinazioni delle copie da quell'unità organizzativa principale, unità organizzativa o account solo agli account con archivi di backup a cui hai assegnato i tag. `DestinationBackupVault` L'autorizzazione `"backup:CopyIntoBackupVault"` controlla il funzionamento di un vault di backup e, in questo caso, quali vault di backup di destinazione sono validi. Utilizza questa policy, insieme al tag corrispondente applicato ai vault di destinazione approvati, per controllare le destinazioni delle copie tra account ai soli account e vault di backup approvati.

```
{
```

```
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

Limitazione degli account di destinazione utilizzando numeri di account e nomi dei vault

Se collegata a un account AWS Organizations principale, a un'unità organizzativa o a un account individuale, questa policy limita le copie provenienti da tale unità organizzativa, unità organizzativa o account a soli due account di destinazione. L'autorizzazione `"backup:CopyFromBackupVault"` controlla il funzionamento di un punto di ripristino nel vault di backup e, in questo caso, le destinazioni in cui è possibile copiare tale punto di ripristino. Il vault di origine consentirà copie nel primo account di destinazione (112233445566) solo se i nomi di uno o più vault di backup di destinazione iniziano con `cab-`. Il vault di origine consentirà copie nel secondo account di destinazione (123456789012) se la destinazione è un singolo vault di backup denominato `fort-knox`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"arn:aws:ec2:*:snapshot/*",
      "Condition":{
        "ForAllValues:ArnNotLike":{
          "backup:CopyTargets":[
            "arn:aws:backup:*:112233445566:backup-vault:cab-*",
            "arn:aws:backup:us-west-1:123456789012:backup-vault:fort-knox"
          ]
        }
      }
    }
```

```
  ]
}
```

Limita gli account di destinazione utilizzando unità organizzative in AWS Organizations

Se collegati a un'unità organizzativa o AWS Organizations root che contiene l'account di origine o quando sono collegati all'account di origine, la seguente politica limita gli account di destinazione a quegli account all'interno delle due unità organizzative specificate.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringNotLike":{
          "backup:CopyTargetOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

Considerazioni di sicurezza per il backup tra account

Quando esegui i backup tra account in AWS Backup, tieni presente quando segue:

- Il vault di destinazione non può essere il vault predefinito. Questo perché il vault predefinito è crittografato con una chiave che non può essere condivisa con altri account.
- I backup tra account possono continuare a funzionare per un massimo di 15 minuti dopo che hai disabilitato il backup tra account. Ciò a causa della consistenza finale che potrebbe causare l'avvio o il completamento di alcuni processi tra account anche dopo che il backup tra account è stato disabilitato.
- Se l'account di destinazione lascia l'organizzazione in un secondo momento, tale account manterrà i backup. Per evitare una potenziale perdita di dati, inserisci un'autorizzazione di rifiuto

sull'autorizzazione `organizations:LeaveOrganization` in una policy di controllo dei servizi collegata all'account di destinazione. Per informazioni dettagliate sugli SCP, consulta Rimozione di un account membro dall'organizzazione nella Guida per l'utente di Organizations.

- Se si elimina un ruolo di copia durante una copia su più account, non è AWS Backup possibile annullare la condivisione delle istantanee dall'account di origine al termine del processo di copia. In questo caso, il processo di backup termina, ma lo stato del processo di copia viene visualizzato come Failed to unshare snapshot.

Eliminazione di backup

Ti consigliamo di utilizzare l'opzione AWS Backup per eliminare automaticamente i backup che non ti servono più configurando il ciclo di vita al momento della creazione del piano di backup. Ad esempio, se imposti il ciclo di vita del piano di backup in modo da conservare i punti di ripristino per un anno, AWS Backup verranno eliminati automaticamente il 1° gennaio 2022 i punti di ripristino creati il 1° gennaio 2021 o entro diverse ore. (AWS Backup semplifica le eliminazioni in modo casuale entro 8 ore dalla scadenza del punto di ripristino per mantenere le prestazioni.) Per ulteriori informazioni sulla configurazione della policy di conservazione del ciclo di vita, consulta Creazione di un piano di backup.

Tuttavia, potrebbe essere necessario eliminare manualmente uno o più punti di ripristino. Per esempio:

- Sono disponibili punti di ripristino `EXPIRED`. Non AWS Backup è stato possibile eliminare automaticamente questi punti di ripristino perché hai eliminato o modificato la policy IAM originale utilizzata per creare il piano di backup. Quando AWS Backup ha tentato di eliminarli, non aveva il permesso di farlo.

  È inoltre possibile creare punti di ripristino scaduti se AWS a un punto di ripristino Amazon EBS o Amazon EC2 gestito è applicato un Amazon EBS Snapshot Lock AWS Backup e non è in grado di completare il processo del ciclo di vita che normalmente comporterebbe l'eliminazione del punto di ripristino. Tieni presente che questi punti di ripristino scaduti possono essere ripristinati dalla console e dall'API Amazon EC2 o dalla console e dall'API Amazon EBS.

  > **Warning**
  >
  > I punti di ripristino scaduti continueranno ad essere archiviati nell'account. Ciò potrebbe aumentare i costi di storage.

Dopo il 6 agosto 2021, AWS Backup mostrerà il punto di ripristino di destinazione come Scaduto nel relativo archivio di backup. È possibile passare il mouse sullo stato Scaduto rosso per visualizzare un messaggio di stato popover in cui viene descritto perché non è stato possibile eliminare il backup. È anche possibile scegliere Aggiorna per ricevere le informazioni più recenti.

- Non è più necessario che un piano di backup funzioni nel modo configurato. L'aggiornamento del piano di backup influisce sui punti di ripristino futuri che verranno creati, ma non sul punto di ripristino già creato. Per ulteriori informazioni, consulta Aggiornamento di un piano di backup.
- È necessario eseguire la pulizia dopo aver terminato un test o un tutorial.

Eliminazione manuale dei backup

Per eliminare manualmente i punti di ripristino

1. Nella AWS Backup console, nel riquadro di navigazione, scegli Backup vault.
2. Nella pagina Backup vaults (Vault di backup) scegliere il vault di backup in cui sono archiviati i backup.
3. Scegli un punto di ripristino, seleziona il menu a discesa Azioni, quindi scegli Elimina.
4. 1. Se l'elenco contiene un backup continuo, scegli una delle seguenti opzioni. Ogni backup continuo dispone di un singolo punto di ripristino.
   - Elimina definitivamente i miei dati di backup o Elimina punto di ripristino. Selezionando una di queste opzioni, i backup continui futuri vengono interrotti e i dati di backup continuo esistenti vengono eliminati.

     > **Note**
     >
     > Vedi Backup e point-in-time ripristino continui (PITR) per considerazioni sul backup continuo di Amazon S3, Amazon RDS e Aurora.

   - Conserva i miei dati di backup continui o il punto di ripristino Disassociate. Selezionando una di queste opzioni, i backup continui futuri vengono interrotti ma i dati di backup continuo esistenti vengono mantenuti fino alla scadenza come definito dal periodo di conservazione.

     Un punto di ripristino continuo (backup) di Amazon S3 dissociato rimarrà nel suo archivio di backup, ma il suo stato passerà a. `STOPPED`

2. Per eliminare tutti i punti di ripristino elencati, digita delete, quindi scegli Elimina punti di ripristino.
3. AWS Backup inizia a inviare i punti di ripristino per l'eliminazione e visualizza una barra di avanzamento. Mantieni aperta la scheda del browser e non chiudere questa pagina durante il processo di invio.
4. Al termine del processo di invio, ti AWS Backup presenta uno stato nel banner. Lo stato può essere:
   - Inviato correttamente. Puoi scegliere l'opzione Visualizza l'avanzamento per lo stato di eliminazione di ciascun punto di ripristino.
   - Impossibile inviare. Puoi scegliere l'opzione Visualizza l'avanzamento per lo stato di eliminazione di ciascun punto di ripristino o Riprova per eseguire un nuovo invio.
   - Un risultato misto in cui alcuni punti di ripristino sono stati inviati correttamente mentre altri non sono stati inviati.
5. Se scegli Visualizza l'avanzamento, puoi rivedere lo Stato di eliminazione di ciascun backup. Se lo stato di eliminazione è Non riuscito o Scaduto, puoi fare clic su tale stato per visualizzare il motivo. Puoi anche scegliere Riprova a eseguire le eliminazioni non riuscite.

Risoluzione dei problemi relativi alle eliminazioni manuali

In rare situazioni, AWS Backup potrebbe non completare la richiesta di eliminazione. AWS Backup utilizza il ruolo collegato al servizio `AWSServiceRoleForBackup` per eseguire le eliminazioni.

Se la richiesta di eliminazione non va a buon fine, verifica che il ruolo IAM disponga dell'autorizzazione per creare ruoli collegati ai servizi. In particolare, verifica che il ruolo IAM disponga dell'azione `iam:CreateServiceLinkedRole`. In caso contrario, aggiungi questa autorizzazione al ruolo utilizzato per creare un backup. L'aggiunta di questa autorizzazione consente di AWS Backup eseguire eliminazioni manuali.

Se, dopo aver confermato che il ruolo IAM dispone dell'azione `iam:CreateServiceLinkedRole`, i punti di ripristino sono ancora bloccati nello stato `DELETING`, è probabile che il problema sia sotto indagine. Completa l'eliminazione manuale con i seguenti passaggi:

1. Imposta un promemoria per tornare tra 2-3 giorni.
2. Dopo 2-3 giorni, controlla i punti di eliminazione con stato `EXPIRED` recente che sono il risultato della prima operazione di eliminazione manuale.
3. Elimina manualmente questi punti di ripristino `EXPIRED`.

Per ulteriori informazioni sui ruoli, consulta Utilizzo dei ruoli collegati a servizi e Aggiunta e rimozione di autorizzazioni per identità IAM.

Modifica di un backup

Dopo aver creato un backup utilizzando AWS Backup, è possibile modificare il ciclo di vita o i tag del backup. Il ciclo di vita definisce quando un backup viene trasferito in uno storage di dati inattivi e quando scade. AWS Backup trasferisce e fa scadere i backup automaticamente in base al ciclo di vita definito dall'utente.

Per visualizzare l'elenco di risorse che è possibile trasferire nell'archiviazione a freddo, consulta la sezione "Dal ciclo di vita all'archiviazione a freddo" della tabella Disponibilità delle funzionalità per risorsa. L'espressione archiviazione a freddo viene ignorata per le altre risorse.

> **Note**
>
> La modifica dei tag di un backup tramite la AWS Backup console è supportata solo per i backup dei file system Amazon Elastic File System (Amazon EFS) e Advanced Amazon DynamoDB.
> I tag che sono stati aggiunti al punto di ripristino al momento della creazione di altre risorse continueranno a essere visualizzati, ma saranno non selezionabili e non modificabili. Anche se questi tag non sono modificabili nella AWS Backup console, puoi modificare i tag dei backup di questi altri servizi utilizzando la console o l'API del servizio.

I backup che vengono trasferiti allo storage dei dati inattivi devono essere archiviati nello storage per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". Quando si aggiorna l'impostazione che specifica dopo quanti giorni deve essere eseguito il trasferimento allo storage inattivo, il valore deve corrispondere almeno all'età del backup più un giorno. L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

L'esempio seguente spiega come aggiornare il ciclo di vita di un backup.

Per modificare il ciclo di vita di un backup

1. Accedi a e apri AWS Management Console la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.

2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Scegliere un backup nella sezione Backup.
4. Nella pagina dei dettagli del backup scegliere Modifica.
5. Configurare le impostazioni del ciclo di vita, quindi scegliere Salva.

Ripristino di un backup

Come ripristinare

Per le istruzioni di ripristino della console e i collegamenti alla documentazione per ogni tipo di risorsa AWS Backup supportato, consulta i collegamenti in fondo a questa pagina.

Per ripristinare un backup in modo programmatico, utilizza l'operazione API StartRestoreJob.

I valori di configurazione ("metadati di ripristino") necessari per ripristinare la risorsa variano a seconda della risorsa che si desidera ripristinare. Per ottenere i metadati di configurazione con cui è stato creato il backup, puoi chiamare GetRecoveryPointRestoreMetadata. Esempi di metadati di ripristino sono disponibili anche nei collegamenti nella parte inferiore di questa pagina.

Il ripristino dallo storage a freddo richiede in genere 4 ore in più rispetto al ripristino dallo storage a caldo.

Per ciascun ripristino, viene creato un processo di ripristino con un ID processo univoco, ad esempio, `1323657E-2AA4-1D94-2C48-5D7A423E7394`.

> **Note**
>
> AWS Backup non fornisce alcun accordo sul livello di servizio (SLA) per i tempi di ripristino. I tempi di ripristino possono variare in base al carico e alla capacità del sistema, anche per ripristini contenenti le stesse risorse.

Ripristini non distruttivi

Quando si utilizza AWS Backup per ripristinare un backup, viene creata una nuova risorsa con il backup che si sta ripristinando. Questo serve a evitare che le risorse esistenti vengano distrutte dall'attività di ripristino.

Test di ripristino

È possibile eseguire i test sulle risorse per simulare un'esperienza di ripristino. In tal modo è possibile determinare se si soddisfa l'obiettivo del tempo di ripristino (RTO) dell'organizzazione e prepararsi per le future esigenze di ripristino.

Per ulteriori informazioni, consulta Test di ripristino.

Copia dei tag durante un ripristino

> **Note**
>
> Attualmente, i ripristini di Amazon DynamoDB, Amazon S3, SAP HANA su istanze Amazon EC2, macchine virtuali e risorse Amazon Timestream non dispongono di questa funzionalità.

Introduzione

Puoi copiare i tag durante il ripristino di una risorsa se i tag appartenevano alla risorsa protetta al momento del backup. I tag, che sono etichette contenenti una coppia chiave-valore, possono semplificare l'identificazione e la ricerca delle risorse. Quando si avvia un processo di ripristino, i tag che appartenevano alle risorse di backup originali possono essere aggiunti alla risorsa da ripristinare.

Quando si sceglie di includere i tag durante un processo di ripristino, questo passaggio può sostituire i costi operativi e la manodopera associati all'applicazione manuale dei tag alle risorse dopo il completamento di un processo di ripristino. Tieni presente che ciò è diverso dall'aggiunta di nuovi tag alle risorse ripristinate.

Quando ripristini un backup nel flusso della console, i tag di origine verranno copiati per impostazione predefinita. Nella console, deseleziona la casella se desideri escludere la copia dei tag in una risorsa ripristinata

Nell'operazione API `StartRestoreJob`, il parametro `CopySourceTagsToRestoredResource` è impostato su `false` per impostazione predefinita. Ciò escluderà i tag di origine originali dalla risorsa che stai ripristinando. Se desideri includere tag dalla sorgente originale, imposta questo valore su `True`.

Considerazioni

- Una risorsa può contenere un massimo di 50 tag, incluse le risorse ripristinate. Per ulteriori informazioni sui limiti dei tag, consulta Taggare le AWS risorse.
- Assicurati che il ruolo utilizzato per i ripristini dei tag di copia, disponga delle autorizzazioni corrette. Il ruolo predefinito per i ripristini contiene le autorizzazioni necessarie. Un ruolo personalizzato deve includere autorizzazioni aggiuntive per assegnare tag alle risorse.
- Le seguenti risorse non sono attualmente supportate per l'inclusione dei tag di ripristino: VMware Cloud™ on AWS, VMware Cloud™ on, sistemi locali, SAP HANA su AWS Outposts istanze Amazon EC2, Timestream, DynamoDB, Advanced DynamoDB e Amazon S3.
- Per i backup continui, i tag sulla risorsa originale a partire dal backup più recente verranno copiati nella risorsa ripristinata.
- I tag non verranno copiati per ripristini a livello di elemento.
- I tag che sono stati aggiunti a un backup dopo il completamento del processo di backup ma che non erano presenti nella risorsa originale prima del backup non verranno copiati nella risorsa ripristinata. Solo i backup creati dopo il 22 maggio 2023 sono idonei per la copia dei tag al momento del ripristino.

Interazione dei tag con risorse specifiche

- Amazon EC2
  - I tag applicati alle istanze Amazon EC2 ripristinate vengono applicati anche ai volumi Amazon EBS ripristinati collegati.
  - I tag applicati ai volumi EBS collegati alle istanze di origine non vengono copiati sui volumi collegati alle istanze ripristinate. Se disponi di policy IAM che consentono o negano agli utenti l'accesso ai volumi EBS in base ai loro tag, devi riassegnare manualmente i tag richiesti ai volumi ripristinati per garantire che le policy rimangano in vigore.
- Quando ripristini una risorsa Amazon EFS, questa deve essere copiata in un nuovo file system. Nei ripristini eseguiti in un file system esistente non è possibile copiare i tag su di essi.
- Amazon RDS
  - Se il cluster RDS di cui è stato eseguito il backup è ancora attivo, i tag di questo cluster verranno copiati.
  - Se il cluster originale non è più attivo, verranno invece copiati i tag dello snapshot del cluster.

- I tag presenti sulla risorsa al momento del backup, verranno copiati durante il ripristino a prescindere che il parametro booleano per `CopySourceTagsToRestoredResource` sia impostato su `True` o `False`. Tuttavia, se lo snapshot non contiene tag, verrà utilizzata l'impostazione booleana precedente.

- Per impostazione predefinita, i cluster Amazon Redshift includono sempre i tag durante un processo di ripristino.

Copia dei tag tramite la console

1. Apri la console AWS Backup
2. Nel riquadro di navigazione, scegli Risorse protette e seleziona l'ID della risorsa Amazon S3 che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionato. Per ripristinare una risorsa:
   a. Nel riquadro Backup, scegli l'ID del punto di ripristino della risorsa.
   b. Nell'angolo in alto a destra del riquadro, scegli Ripristina (in alternativa, puoi passare al vault di backup, trovare il punto di ripristino, quindi fare clic su Azioni e su Ripristina).
4. Nella pagina Ripristina backup, individua il pannello denominato Ripristina con tag. Per includere tutti i tag della risorsa originale, mantieni la casella di selezionata (nota che nella console questa casella è selezionata per impostazione predefinita).
5. Fai clic su Ripristina backup dopo aver selezionato tutte le impostazioni e i ruoli preferiti.

Per includere tag in modo programmatico

Usa l'operazione API `StartRestoreJob`. Assicurati che il seguente parametro booleano sia impostato su `True`:

```
CopySourceTagsToRestoredResource = true
```

Se il parametro booleano `CopySourceTagsToRestoredResource` = `True`, il processo di ripristino copierà i tag dalle risorse originali nel materiale ripristinato.

> **Important**
>
> Il processo di ripristino avrà esito negativo se questo parametro viene incluso per una risorsa non supportata (VMware, sistemi locali, AWS Outposts SAP HANA su istanze EC2, Timestream, DynamoDB, Advanced DynamoDB e Amazon S3).

```
{
    "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
    "Metadata": {
        "InstanceInitiatedShutdownBehavior": "stop",
        "DisableApiTermination": "false",
        "EbsOptimized": "false",
        "InstanceType": "t1.micro",
        "SubnetId": "subnet-123ab456cd7efgh89",
        "SecurityGroupIds": "[\"sg-0a1bc2d345ef67890\"]",
        "Placement": "{\"GroupName\":null,\"Tenancy\":\"default\"}",
        "HibernationOptions": "{\"Configured\":false}",
        "IamInstanceProfileName": "UseBackedUpValue",
        "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
    },
    "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
    "ResourceType": "EC2",
    "IdempotencyToken": "34ab5678-9012-3c4d-5678-efg9h01f23i4",
    "CopySourceTagsToRestoredResource": true
}
```

Risoluzione dei problemi di ripristino dei tag

ERROR: autorizzazioni insufficienti

REMEDY: assicurati di disporre delle autorizzazioni necessarie nel ruolo di ripristino in modo da poter includere i tag nella risorsa ripristinata. La politica predefinita dei ruoli di servizio AWS gestito per i ripristini contiene le autorizzazioni necessarie per questa attività. AWSBackupServiceRolePolicyForRestores

Se scegli di utilizzare un ruolo personalizzato, assicurati che siano presenti le seguenti autorizzazioni:

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`

- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

Per ulteriori informazioni, consulta Autorizzazioni API.

Stati del processo di ripristino

Puoi visualizzare lo stato di un processo di ripristino nella pagina Processi della console di AWS Backup . Gli stati del processo di ripristino includono: pending (in sospeso), running (in esecuzione), aborted (interrotto), completed (completato) e failed (non riuscito).

Argomenti

- Ripristino dei dati S3
- Ripristino di una macchina virtuale utilizzando AWS Backup
- Ripristino di un file system FSX
- Ripristino di un volume Amazon EBS
- Ripristino di un file system Amazon EFS
- Ripristino di una tabella Amazon DynamoDB
- Ripristino di un database RDS
- Ripristino di un cluster Amazon Aurora
- Ripristino di un'istanza Amazon EC2
- Ripristino di un volume Storage Gateway
- Ripristino di una tabella Amazon Timestream
- Ripristino di un cluster Amazon Redshift
- Ripristino di database SAP HANA su un'istanza Amazon EC2
- Ripristino di un cluster DocumentDB
- Ripristino di un cluster Neptune
- Ripristina i backup CloudFormation dello stack

Ripristino dei dati S3

Puoi ripristinare i dati S3 di cui hai eseguito il backup utilizzando nella classe AWS Backup di storage S3 Standard. Puoi ripristinare tutti gli oggetti in un bucket o oggetti specifici. Puoi ripristinarli in un bucket nuovo o esistente.

Autorizzazioni di ripristino Amazon S3

Prima di iniziare a ripristinare le risorse, assicurati che il ruolo che stai utilizzando disponga di autorizzazioni sufficienti.

Per ulteriori informazioni, consulta le seguenti voci sulle politiche:

1. `AWSBackupServiceRolePolicyForS3Restore`
2. `AWSBackupServiceRolePolicyForRestores`
3. Politiche gestite per AWS Backup

Considerazioni sul ripristino di Amazon S3

- AWS Backup crea un backup di tutte le versioni di S3, ma ripristina solo la versione più recente dallo stack di versioni in qualsiasi momento.
- Le liste di controllo degli accessi (ACL) devono essere abilitate nel bucket di destinazione, altrimenti il processo non andrà a buon fine. Per abilitare le ACL, segui le istruzioni nella pagina Configurazione delle ACL.
- I ripristini di oggetti vengono ignorati se il bucket di origine contiene un oggetto con lo stesso nome o ID versione.
- Se ripristini oggetti specifici, puoi ripristinare la versione corrente di un oggetto.
- Quando esegui il ripristino nel bucket S3 originale,
  - AWS Backup non esegue un ripristino distruttivo, il che significa AWS Backup che non inserisce un oggetto in un bucket al posto di un oggetto già esistente, indipendentemente dalla versione.
  - Un marker di eliminazione nella versione corrente viene considerato come un oggetto inesistente, quindi può verificarsi un ripristino.
  - AWS Backup non elimina oggetti (senza marcatori di eliminazione) da un bucket durante un ripristino (esempio: le chiavi attualmente nel bucket che non erano presenti durante il backup rimarranno).

- Ripristino di copie tra regioni
  - Sebbene i backup S3 possano essere copiati tra regioni, i processi di ripristino vengono eseguiti solo nella stessa regione in cui si trova il backup o la copia originale.

    Example

    Esempio: un bucket S3 creato nella regione Stati Uniti orientali (Virginia settentrionale) può essere copiato nella regione Canada (Centrale). Il processo di ripristino può essere avviato utilizzando il bucket originale nella regione Stati Uniti orientali (Virginia settentrionale) e ripristinato in tale regione, oppure il processo di ripristino può essere avviato utilizzando la copia nella regione Canada (Centrale) e ripristinato in tale regione.
  - Il metodo di crittografia originale non può essere utilizzato per ripristinare un punto di ripristino (backup) copiato da un'altra regione. La AWS KMS crittografia delle copie tra regioni non è disponibile per le risorse Amazon S3; utilizza invece un tipo di crittografia diverso per un processo di ripristino.

Usa la AWS Backup console per ripristinare i punti di ripristino di Amazon S3

Per ripristinare i dati di Amazon S3 utilizzando la AWS Backup console:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e seleziona l'ID della risorsa Amazon S3 che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionato. Per ripristinare una risorsa:

   a. Nel riquadro Backup, scegli l'ID del punto di ripristino della risorsa.

   b. Nell'angolo superiore destro del riquadro, scegliere Ripristina.

      In alternativa, puoi accedere al vault di backup, trovare il punto di ripristino, quindi fare clic su Azioni e scegliere Ripristina.
4. Se stai ripristinando un backup continuo, nel riquadro Ora di ripristino, seleziona una delle opzioni:

   a. Accetta l'impostazione predefinita per ripristinare all'Ora ripristinabile più recente.

   b. Specifica data e ora in cui eseguire il ripristino.
5. Nel riquadro Impostazioni, seleziona Ripristina l'intero bucket o Ripristino a livello di elemento.

a. Se scegli il ripristino a livello di elemento, ripristini fino a 5 elementi (oggetti o cartelle in un bucket) per processo di ripristino specificando l'URI S3 di ciascun elemento che identifica in modo univoco l'oggetto.

   Per ulteriori informazioni sugli URI del bucket S3, consulta Metodi di accesso a un bucket nella Guida per l'utente di Amazon Simple Storage Service.

b. Scegli Aggiungi elemento per specificare un altro elemento da ripristinare.

6. Scegli la Destinazione di ripristino. Puoi scegliere Ripristina nel bucket della fonte, Utilizza bucket esistente o Crea nuovo bucket.

> **Note**
>
> Il bucket di destinazione di ripristino deve avere il controllo delle versioni attivato. AWS Backup ti avvisa se il bucket selezionato non soddisfa questo requisito.

   a. Se scegli Usa bucket esistente, seleziona il bucket S3 di destinazione dal menu a discesa che mostra tutti i bucket esistenti nella tua regione corrente. AWS

   b. Se scegli Crea un nuovo bucket, digita il Nome del nuovo bucket. Il controllo delle versioni S3 è abilitato per impostazione predefinita nel nuovo bucket. Le impostazioni Blocco dell'accesso pubblico verranno disattivate per impostazione predefinita. Puoi modificare queste impostazioni dopo aver creato il bucket in S3.

7. Per la crittografia degli oggetti nel tuo bucket S3, puoi scegliere la crittografia degli oggetti ripristinata. Utilizza chiavi di crittografia originali (di default), chiave Amazon S3 (SSE-S3) o chiave AWS Key Management Service (SSE-KMS).

   Queste impostazioni si applicano solo alla crittografia degli oggetti nel bucket S3. Ciò non influisce sulla crittografia del bucket stesso.

   a. Usa chiavi di crittografia originali (impostazione predefinita) ripristina gli oggetti con le stesse chiavi di crittografia utilizzate dall'oggetto di origine. Se un oggetto di origine non era crittografato, questo metodo ripristina l'oggetto senza crittografia.

      Questa opzione di ripristino consente di scegliere facoltativamente una chiave di crittografia sostitutiva per crittografare gli oggetti di ripristino se la chiave originale non è disponibile.

   b. Se scegli Chiave Amazon S3 (SSE-S3), non è necessario specificare altre opzioni.

c. Se scegli AWS Key Management Service la chiave (SSE-KMS), puoi effettuare le seguenti scelte: Chiave gestita da AWS (aws/s3), Scegli tra le tue AWS KMS chiavi o Inserisci la chiave ARN. AWS KMS

   i. Se scegli Chiave gestita da AWS (aws/s3), non è necessario specificare altre opzioni.

   ii. Se scegli tra le tue AWS KMS chiavi, seleziona una chiave dal menu a discesa. AWS KMS In alternativa, scegli Crea chiave.

   iii. Se inserisci AWS KMS la chiave ARN, digita l'ARN nella casella di testo. In alternativa, scegli Crea chiave.

8. Nel riquadro Ripristina ruolo scegliere il ruolo IAM che AWS Backup assumerà per questo ripristino.
9. Scegli Restore backup (Ripristina backup). Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.

Usa l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino di Amazon S3

Utilizza `StartRestoreJob`. Durante i ripristini di Amazon S3 puoi specificare i seguenti metadati:

```
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
 required for item-level restore.
NewBucket // Boolean to indicate whether to create a new bucket.
Encrypted // Boolean to indicate whether to encrypt the restored data.
CreationToken // An idempotency token.
EncryptionType // The type of encryption to encrypt your restored objects. Options
 are original (same encryption as the original object), SSE-S3, or SSE-KMS).
RestoreTime // The restore time (only valid for continuous recovery points where it is
 required, in format 2021-11-27T03:30:27Z).

// Optional metadata:
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
aws:backup:request-id
```

Stato del punto di ripristino

I punti di ripristino sono caratterizzati da uno stato.

`PARTIAL`lo stato indica che non è stato AWS Backup possibile creare il punto di ripristino prima della chiusura della finestra di backup. Per aumentare la finestra del piano di backup utilizzando l'API, vedi UpdateBackupPlan. Puoi anche aumentare la finestra del piano di backup utilizzando la console scegliendo e modificando il piano di backup.

`EXPIRED`lo stato indica che il punto di ripristino ha superato il periodo di conservazione, ma non AWS Backup dispone dell'autorizzazione o non è altrimenti in grado di eliminarlo. Per eliminare manualmente questi punti di ripristino, consulta Passaggio 3: Eliminare i punti di ripristino nella sezione Pulizia delle risorse di Nozioni di base.

Lo stato `STOPPED` si verifica in un backup continuo in cui un utente ha eseguito alcune azioni che causano la disabilitazione del backup continuo. Ciò può essere causato dalla rimozione delle autorizzazioni, dalla disattivazione del controllo delle versioni, dalla disattivazione degli eventi inviati ad Amazon EventBridge o dalla disattivazione delle EventBridge regole messe in atto da. AWS Backup

Per risolvere lo stato `STOPPED`, assicurati che tutte le autorizzazioni richieste siano in essere e che il controllo delle versioni sia abilitato sul bucket S3. Una volta soddisfatte queste condizioni, l'istanza successiva di una regola di backup in esecuzione comporterà la creazione di un nuovo punto di ripristino continuo. Non è necessario eliminare i punti di ripristino con stato STOPPED.

Ripristino di una macchina virtuale utilizzando AWS Backup

Puoi ripristinare una macchina virtuale su VMware, VMware Cloud on, VMware Cloud on AWS, un volume Amazon EBS o su AWS Outposts un'istanza Amazon EC2. Il ripristino (o la migrazione) di una macchina virtuale su EC2 richiede una licenza. Per impostazione predefinita, AWS includerà una licenza (a pagamento). Per ulteriori informazioni, vedere Opzioni di licenza nella Guida per l'utente di VM Import/Export.

È possibile ripristinare una macchina virtuale VMware utilizzando la console o tramite. AWS Backup AWS CLI Quando viene ripristinata una macchina virtuale, la cartella VMware Tools non è inclusa. Consulta la documentazione di VMware per reinstallare VMware Tools.

AWS Backup i ripristini delle macchine virtuali non sono distruttivi, ossia AWS Backup non sovrascrivono le macchine virtuali esistenti durante un ripristino. Al contrario, il processo di ripristino implementa una nuova macchina virtuale.

Attività

- Considerazioni sul ripristino di una macchina virtuale su un'istanza Amazon EC2

- Usa la AWS Backup console per ripristinare i punti di ripristino delle macchine virtuali
- Utilizzalo AWS CLI per ripristinare i punti di ripristino delle macchine virtuali

Considerazioni sul ripristino di una macchina virtuale su un'istanza Amazon EC2

- Il ripristino (o la migrazione) di una macchina virtuale su EC2 richiede una licenza. Per impostazione predefinita, AWS includerà una licenza (a pagamento). Per ulteriori informazioni, vedere Opzioni di licenza nella Guida per l'utente di VM Import/Export.
- Esiste un limite massimo di 5 TB (terabyte) per ogni disco della macchina virtuale.
- Non è possibile specificare una key pair quando si ripristina la macchina virtuale su un'istanza. Puoi aggiungere una key pair `authorized_keys` durante il lancio (tramite i dati utente dell'istanza) o dopo il lancio (come descritto in questa sezione sulla risoluzione dei problemi nella Guida per l'utente di Amazon EC2).
- Verifica che il tuo sistema operativo sia supportato per l'importazione e l'esportazione da Amazon EC2 nella VM Import/Export User Guide.
- Consulta le limitazioni relative all'importazione di macchine virtuali in Amazon EC2 nella VM Import/Export User Guide.
- Quando esegui il ripristino su un'istanza Amazon EC2 utilizzando AWS CLI, devi specificare. `"RestoreTo":"EC2Instance"` Tutti gli altri attributi hanno valori predefiniti.

Usa la AWS Backup console per ripristinare i punti di ripristino delle macchine virtuali

Puoi ripristinare una macchina virtuale da più posizioni nel riquadro di navigazione a sinistra della AWS Backup console:

- Scegli Hypervisor per visualizzare i punti di ripristino per macchine virtuali gestite da un hypervisor connesso a AWS Backup.
- Scegli Macchine virtuali per visualizzare i punti di ripristino per macchine virtuali in tutti gli hypervisor connessi a AWS Backup.
- Scegli Backup vault per visualizzare i punti di ripristino archiviati in un AWS Backup vault specifico.
- Scegli Risorse protette per visualizzare i punti di ripristino su tutte le tue risorse AWS Backup protette.

Se è necessario ripristinare una macchina virtuale che non dispone più di una connessione con Backup gateway, scegli Vault di backup o Risorse protette per individuare il punto di ripristino.

Opzioni

- Ripristina su VMware
- Ripristino su un volume Amazon EBS
- Ripristina su un'istanza Amazon EC2

Per ripristinare una macchina virtuale su VMware, VMware Cloud on e VMware Cloud on AWSAWS Outposts

1. Nelle visualizzazioni Hypervisor o Macchine virtuali, scegli il nome della VM da ripristinare. Nella vista Risorse protette, scegli l'ID risorsa della macchina virtuale da ripristinare.
2. Scegli il pulsante radiale accanto all'ID punto di ripristino da ripristinare.
3. Scegli Restore (Ripristina).
4. Scegli il Tipo di ripristino.
    a. Ripristino completo ripristina tutti i dischi della macchina virtuale.
    b. Ripristino a livello di disco ripristina una selezione definita dall'utente di uno o più dischi. Utilizza il menu a discesa per selezionare i dischi da ripristinare.
5. Scegli la Posizione di ripristino. Le opzioni sono VMware, VMware Cloud on e VMware Cloud on. AWS AWS Outposts
6. Se stai eseguendo un ripristino completo, passa alla fase successiva. Se stai eseguendo un ripristino a livello di disco, verrà visualizzato un menu a discesa in Dischi VM. Scegli uno o più volumi avviabili da ripristinare.
7. Seleziona un Hypervisor dal menu a discesa per gestire la macchina virtuale ripristinata
8. Per la macchina virtuale ripristinata, utilizza le best practice della macchina virtuale dell'organizzazione per specificare:
    a. Nome
    b. Percorso (ad esempio `/datacenter/vm`)
    c. Nome risorsa di calcolo (ad esempio VMHost o Cluster)

Se un host fa parte di un cluster, non è possibile eseguire il ripristino sull'host ma solo sul cluster specificato.

d. Datastore

9. Per Ripristina ruolo, seleziona Ruolo predefinito (scelta consigliata) o Scegli un ruolo IAM utilizzando il menu a discesa.
10. Scegli Restore backup (Ripristina backup).
11. Facoltativo: verifica quando lo stato del processo di ripristino è `Completed`. Nel riquadro di navigazione a sinistra, scegli Processi.

Per ripristinare una macchina virtuale su un volume Amazon EBS

1. Nelle visualizzazioni Hypervisor o Macchine virtuali, scegli il nome della VM da ripristinare. Nella vista Risorse protette, scegli l'ID risorsa della macchina virtuale da ripristinare.
2. Scegli il pulsante radiale accanto all'ID punto di ripristino da ripristinare.
3. Scegli Restore (Ripristina).
4. Scegli il Tipo di ripristino.

   - Ripristino del disco ripristina una selezione definita dall'utente di un disco. Utilizza il menu a discesa per selezionare il disco da ripristinare.

5. Scegli la Posizione di ripristino come Amazon EBS.
6. Nel menu a discesa Disco VM, scegli il volume avviabile da ripristinare.
7. Per Tipo di volume EBS, scegli il tipo di volume.
8. Scegli la zona di disponibilità.
9. Crittografia (facoltativo). Seleziona la casella se scegli di crittografare il volume EBS.
10. Seleziona la tua chiave KMS dal menu.
11. Per il ruolo di ripristino, seleziona il ruolo predefinito (consigliato) o Scegli un ruolo IAM.
12. Scegli Restore backup (Ripristina backup).
13. Facoltativo: verifica quando lo stato del processo di ripristino è `Completed`. Nel riquadro di navigazione a sinistra, scegli Processi.
14. Facoltativo: consulta Come creare un volume logico LVM su un intero volume Amazon EBS? per ulteriori informazioni su come montare volumi gestiti e accedere ai dati sul volume Amazon EBS ripristinato.

Per ripristinare una macchina virtuale su un'istanza Amazon EC2

1. Nelle visualizzazioni Hypervisor o Macchine virtuali, scegli il nome della VM da ripristinare. Nella vista Risorse protette, scegli l'ID risorsa della macchina virtuale da ripristinare.
2. Scegli il pulsante radiale accanto all'ID punto di ripristino da ripristinare.
3. Scegli Restore (Ripristina).
4. Scegli il Tipo di ripristino.

   - Ripristino completo ripristina completamente il file system, inclusi la cartella e i file a livello di root.
5. Scegli la Posizione di ripristino come Amazon EC2.
6. Per tipo di istanza, scegli la combinazione di elaborazione e memoria necessaria per eseguire l'applicazione sulla nuova istanza.

   > **Tip**
   >
   > Scegli un tipo di istanza che corrisponda o superi le specifiche della macchina virtuale originale. Per ulteriori informazioni, consulta la Amazon EC2 Instance Types Guide.
7. Per Virtual Private Cloud (VPC), scegli un cloud privato virtuale (VPC), che definisce l'ambiente di rete per l'istanza.
8. Per Subnet, scegli una delle sottoreti nel VPC. L'istanza riceve un indirizzo IP privato dall'intervallo di indirizzi della sottorete.
9. Per i gruppi di sicurezza, scegli un gruppo di sicurezza che funga da firewall per il traffico verso la tua istanza.
10. Per il ruolo di ripristino, seleziona il ruolo predefinito (consigliato) o Scegli un ruolo IAM.
11. Facoltativo: per eseguire uno script sull'istanza all'avvio, espandi Impostazioni avanzate e inserisci lo script in Dati utente.
12. Scegli Restore backup (Ripristina backup).
13. Facoltativo: verifica quando lo stato del processo di ripristino è `Completed`. Nel riquadro di navigazione a sinistra, scegli Processi.

Utilizzalo AWS CLI per ripristinare i punti di ripristino delle macchine virtuali

Utilizza `StartRestoreJob`.

Puoi specificare i seguenti metadati per il ripristino di una macchina virtuale su Amazon EC2 e Amazon EBS:

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

È possibile specificare i seguenti metadati per il ripristino di una macchina virtuale su VMware, VMware Cloud on e VMware cloud on AWS Outpost: AWS

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

Questo esempio mostra come eseguire un ripristino completo su VMware:

```
'{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-
east-1:209870788375:hypervisor/hype-9B1AB1F1","VMName":"name","VMPath":"/Labster/
```

```
vm","ComputeResourceName":"Cluster","VMDatastore":"vsanDatastore","DisksToRestore":"[{\"DiskId
\":\"2000\",\"Label\":\"Hard disk 1\"}]","vmId":"vm-101"}'
```

Ripristino di un file system FSX

Le opzioni di ripristino disponibili quando si utilizza AWS Backup per ripristinare i file system Amazon FSx sono le stesse del backup nativo di Amazon FSx. Puoi utilizzare il punto di ripristino di un backup per creare un nuovo file system e ripristinare un' point-in-time istantanea di un altro file system.

Quando ripristina i file system Amazon FSx AWS Backup , crea un nuovo file system e lo popola con i dati (Amazon FSx NetApp for ONTAP consente di ripristinare un volume su un file system esistente). Ciò è simile al modo in cui Amazon FSx nativo esegue il backup e il ripristino dei file system. Il ripristino di un backup su un nuovo file system richiede lo stesso tempo della creazione di un nuovo file system. I dati ripristinati dal backup vengono caricati in modo differito sul file system. Pertanto, si potrebbe verificare una latenza leggermente superiore durante il processo.

> **Note**
>
> Non è possibile eseguire il ripristino in un file system Amazon FSx esistente e non è possibile ripristinare singoli file o cartelle.
> FSx per ONTAP non supporta il backup di determinati tipi di volume, inclusi volumi DP (protezione dei dati), volumi LS (condivisione del carico), volumi completi o volumi su file system completi. Per ulteriori informazioni, consulta FSx for ONTAP Working with backups.
> AWS Backup gli archivi che contengono punti di ripristino dei file system Amazon FSx sono visibili all'esterno di. AWS Backup Puoi ripristinare i punti di ripristino utilizzando Amazon FSx ma non eliminarli.

Puoi vedere i backup creati dalla funzionalità di backup automatico integrata di Amazon FSx dalla AWS Backup console. Puoi anche ripristinare questi backup utilizzando. AWS Backup Tuttavia, non è possibile eliminare questi backup o modificare le pianificazioni di backup automatiche dei file system Amazon FSx utilizzati. AWS Backup

Puoi ripristinare i backup creati AWS Backup utilizzando la AWS Backup console, l'API o. AWS CLI Questa sezione mostra come utilizzare la AWS Backup console per ripristinare i file system Amazon FSx.

Usa la AWS Backup console per ripristinare i punti di ripristino Amazon FSx

Ripristino di un file system FSx per Windows File Server

Per ripristinare un file system FSx per Windows File Server

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e seleziona l'ID della risorsa Amazon FSx che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Scegli l'ID del punto di ripristino della risorsa.
4. Nell'angolo in alto a destra del riquadro, scegli Ripristina per aprire la pagina Ripristina backup.
5. Nella sezione Dettagli del file system, l'ID del backup viene visualizzato in ID backup e il tipo di file system viene visualizzato in Tipo di file system. Puoi ripristinare entrambi i file system FSx per Windows File Server e FSx for Lustre.
6. Per Tipo di distribuzione, accetta l'impostazione predefinita. Non puoi modificare il tipo di implementazione di un file system durante il ripristino.
7. Scegli il Tipo di storage da utilizzare. Se la capacità di storage del file system è inferiore a 2.000 GiB, non puoi utilizzare il tipo di storage HDD.
8. Per Capacità di throughput, scegli Capacità di throughput consigliata per utilizzare la velocità consigliata di 16 MB al secondo (MBps) oppure scegli Specifica la capacità di throughput e inserisci una nuova velocità.
9. Nella sezione Rete e sicurezza, fornisci le informazioni richieste.
10. Se stai eseguendo il ripristino di un file system FSx per Windows File Server, fornisci le informazioni di Autenticazione di Windows utilizzate per accedere al file system oppure puoi crearne uno nuovo.

> **Note**
>
> Durante il ripristino di un backup, non puoi modificare il tipo di Active Directory sul file system.

Per ulteriori informazioni su Microsoft Active Directory, consulta Funzionamento con Active Directory in Amazon FSx per Windows File Server nella Guida per l'utente di Amazon FSx per Windows File Server.

11. (Facoltativo) Nella sezione Backup e manutenzione, fornisci le informazioni per impostare le preferenze di backup.
12. Nella sezione Ripristina ruolo, scegli il ruolo IAM utilizzato da AWS Backup per creare e gestire automaticamente i backup. Ti consigliamo di scegliere il Ruolo predefinito. Se non esiste un ruolo predefinito, verrà creato automaticamente con le autorizzazioni corrette. Puoi anche fornire il ruolo IAM.
13. Verifica tutte le voci e scegli Ripristina backup.

Ripristino di un file system Amazon FSx per Lustre

AWS Backup supporta i file system Amazon FSx for Lustre che hanno un tipo di distribuzione di storage persistente e non sono collegati a un repository di dati come Amazon S3.

Per ripristinare un file system Amazon FSx per Lustre

1. Apri la console all'indirizzo https://console.aws.amazon.com/backup AWS Backup .
2. Nel riquadro di navigazione, scegli Risorse protette e seleziona l'ID della risorsa Amazon FSx che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Scegli l'ID del punto di ripristino della risorsa.
4. Nell'angolo in alto a destra del riquadro, scegli Ripristina per aprire la pagina Ripristina backup in un nuovo file system.
5. Nella sezione Impostazioni, l'ID del backup viene visualizzato in ID backup e il tipo di file system viene visualizzato in Tipo di file system. Tipo di file system deve essere Lustre.
6. (Facoltativo) Immetti un nome per il file system.
7. Scegli un tipo di distribuzione. AWS Backup supporta solo il tipo di distribuzione persistente. Non puoi modificare il tipo di implementazione di un file system durante il ripristino.

   Il tipo di implementazione persistente è destinato allo storage a lungo termine. Per informazioni dettagliate sulle opzioni di implementazione di FSx per Lustre, consulta Utilizzo delle opzioni di implementazione disponibili per file system Amazon FSx per Lustre nella Guida per l'utente di Amazon FSx per Lustre.
8. Scegli la velocità di trasmissione effettiva per unità di storage che desideri utilizzare.
9. Specifica la Capacità di storage da utilizzare. Immetti una capacità compresa tra 32 GiB e 64.436 GiB.

10. Nella sezione Rete e sicurezza, fornisci le informazioni richieste.
11. (Facoltativo) Nella sezione Backup e manutenzione, fornisci le informazioni per impostare le preferenze di backup.
12. Nella sezione Ripristina ruolo, scegli il ruolo IAM utilizzato da AWS Backup per creare e gestire automaticamente i backup. Ti consigliamo di scegliere il Ruolo predefinito. Se non esiste un ruolo predefinito, verrà creato automaticamente con le autorizzazioni corrette. Puoi anche fornire il ruolo IAM.
13. Verifica tutte le voci e scegli Ripristina backup.

Ripristino di volumi Amazon FSx NetApp for ONTAP

Per ripristinare i volumi Amazon FSx for NetApp ONTAP:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e seleziona l'ID della risorsa Amazon FSx che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Scegli l'ID del punto di ripristino della risorsa.
4. Nell'angolo in alto a destra del riquadro, scegli Ripristina per aprire la pagina Ripristina.

   Nella prima sezione, Dettagli del file system, viene visualizzato l'ID del punto di ripristino, l'ID del file system e il tipo di file system.
5. In Opzioni di ripristino, sono disponibili diverse selezioni. Innanzitutto, scegli il File system dal menu a discesa.
6. Quindi, scegli la Macchina virtuale per lo storage preferita dal menu a discesa.
7. Immetti un nome per il volume.
8. Specifica il Percorso di collegamento, che è la posizione all'interno del file system in cui verrà montato il volume.
9. Specifica le Dimensioni del volume in megabyte (MB) in corso di creazione.
10. (Facoltativo) Puoi abilitare la casella Abilita efficienza di archiviazione. Ciò consentirà la deduplicazione, la compressione e la compattazione.
11. Nel menu a discesa Policy per la suddivisione della capacità del pool, seleziona la preferenza di suddivisione in più livelli.

12. Nella sezione Autorizzazioni di ripristino, scegli il ruolo IAM da utilizzare per ripristinare i backup. AWS Backup
13. Verifica tutte le voci e scegli Ripristina backup.

Ripristino di un file system Amazon FSx per OpenZFS

Per ripristinare un file system Amazon FSx per OpenZFS

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e seleziona l'ID della risorsa Amazon FSx che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Scegli l'ID del punto di ripristino della risorsa.
4. Nell'angolo in alto a destra del riquadro, scegli Ripristina per aprire la pagina Ripristina backup.

   Nella sezione Dettagli del file system, l'ID del backup viene visualizzato in ID backup e il tipo di file system viene visualizzato in Tipo di file system. Il tipo di file system deve essere FSx per OpenZFS.
5. In Opzioni di ripristino, puoi selezionare Ripristino rapido o Ripristino standard. Il ripristino rapido utilizzerà le impostazioni predefinite del file system di origine. Se stai eseguendo Ripristino rapido, vai al passaggio 7.

   Se scegli Ripristino standard, specifica le seguenti configurazioni aggiuntive:

   a. IOPS dell'SSD assegnati: puoi scegliere il pulsante di opzione Automatico oppure puoi scegliere l'opzione Assegnati dall'utente, se disponibile.
   b. Capacità effettiva di trasmissione: puoi scegliere la Capacità di throughput consigliata di 64 MB/sec oppure scegliere Specifica la capacità di throughput.
   c. (Facoltativo) Gruppi di sicurezza VPC: puoi specificare i gruppi di sicurezza VPC da associare all'interfaccia di rete del file system.
   d. Chiave di crittografia: specifica la AWS Key Management Service chiave per proteggere i dati del file system ripristinati a riposo.
   e. (Facoltativo) Configurazione del volume di root: questa configurazione è compressa per impostazione predefinita. Puoi espanderla facendo clic sull'accento circonflesso (freccia) rivolto verso il basso. La creazione di un file system da un backup creerà un nuovo file system; i volumi e gli snapshot manterranno le configurazioni di origine.

f. (Facoltativo) Backup e manutenzione: per impostare un backup pianificato, fai clic sull'Accento circonflesso (freccia) rivolto verso il basso per espandere la sezione. Puoi scegliere la finestra di backup, ora e minuto, periodo di conservazione e finestra di manutenzione settimanale.

6. (Facoltativo) Puoi immettere un nome per il volume.
7. La Capacità di archiviazione dell'SSD visualizzerà la capacità di storage del file system.
8. Scegli il cloud privato virtuale (VPC) da cui è possibile accedere al file system.
9. Nel menu a discesa Sottorete, scegli la sottorete in cui risiede l'interfaccia di rete del file system.
10. Nella sezione Restore role, scegli il ruolo IAM che AWS Backup utilizzerai per creare e gestire i backup per tuo conto. Ti consigliamo di scegliere il Ruolo predefinito. Se non esiste un ruolo predefinito, verrà creato automaticamente con le autorizzazioni corrette. Puoi anche scegliere un ruolo IAM.
11. Verifica tutte le voci e scegli Ripristina backup.

Usa l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino Amazon FSx

Per ripristinare Amazon FSx utilizzando l'API o la CLI, utilizza `StartRestoreJob`. Durante i ripristini di Amazon FSx è possibile specificare i seguenti metadati:

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

Metadati di ripristino di FSx per Windows File Server

Durante un ripristino di FSx per Windows File Server è possibile specificare i seguenti metadati:

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

Metadati di ripristino di FSx per Lustre

Durante un ripristino di FSx per Lustre, è possibile specificare `PerUnitStorageThroughput` e `DriveCacheType`.

Metadati di ripristino di FSx for ONTAP

Durante un ripristino di FSx for ONTAP è possibile specificare i seguenti metadati:

- Nome #name del volume da creare
- OntapConfiguration: # Configurazione ontap
- `junctionPath`
- `sizeInMegabytes`
- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

Metadati di ripristino di FSx for OpenZFS

Durante un ripristino di FSx per OpenZFS è possibile specificare i seguenti metadati:

- `ThroughputCapacity`
- `DesklopsConfiguration`
- Se si specifica Iops, è necessario includere un valore compreso tra 0 e 160.000, ma non includere Mode.

Esempio di comando di ripristino CLI:

```
aws backup start-restore-job --recovery-point-arn "arn:aws:fsx:us-west-2:1234:backup/
backup-1234" --iam-role-arn "arn:aws:iam::1234:role/Role" --resource-
type "FSx" --region us-west-2 --metadata 'SubnetIds="[\"subnet-1234\",
\"subnet-5678\"]",StorageType=HDD,SecurityGroupIds="[\"sg-bb5efdc4\",
\"sg-0faa52\"]",WindowsConfiguration="{\"DeploymentType\": \"MULTI_AZ_1\",
\"PreferredSubnetId\": \"subnet-1234\",\"ThroughputCapacity\": \"32\"}"'
```

Esempio di metadati di ripristino:

```
"restoreMetadata":  "{\"StorageType\":\"SSD\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:123456789012:key/123456a-123b-123c-defg-1h2i2345678\",\"StorageCapacity
\":\"1200\",\"VpcId\":\"vpc-0ab0979fa431ad326\",\"FileSystemType\":\"LUSTRE\",
\"LustreConfiguration\":\"{\\\"WeeklyMaintenanceStartTime\\\":\\\"4:10:30\\\",\\
\"DeploymentType\\\":\\\"PERSISTENT_1\\\",\\\"PerUnitStorageThroughput\\\":50,\\
\"CopyTagsToBackups\\\":true}\",\"FileSystemId\":\"fs-0ca11fb3d218a35c2\",\"SubnetIds
\":\"[\\\"subnet-0e66e94eb43235351\\\"]\"}"
```

Ripristino di un volume Amazon EBS

Quando ripristini uno snapshot di Amazon Elastic Block Store (Amazon EBS), AWS Backup crea un nuovo volume Amazon EBS da collegare alla tua istanza Amazon EC2.

Puoi scegliere di ripristinare lo snapshot come un volume EBS o come un volume AWS Storage Gateway .

Usa la AWS Backup console per ripristinare i punti di ripristino Amazon EBS

Per ripristinare un volume Amazon EBS

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, seleziona Risorse protette, quindi scegli l'ID della risorsa EBS che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
4. Specificare i parametri di ripristino per la risorsa. I parametri di ripristino immessi sono specifici del tipo di risorsa selezionato.

   Per Tipo di risorsa, scegli la AWS risorsa da creare durante il ripristino di questo backup.

5. Se si sceglie Volume EBS, specificare i valori per Tipo di volume, Dimensioni (GiB), e scegliere una Zona di disponibilità.

   - Dopo Velocità di trasmissione effettiva, sarà visualizzata una casella di controllo opzionale Crittografa questo volume. Questa opzione rimarrà attiva se il punto di ripristino EBS è crittografato.

     È possibile specificare una chiave KMS o creare una AWS KMS chiave.

   Se scegli Volume Storage Gateway, seleziona un Gateway in uno stato raggiungibile. Scegli anche Nome di destinazione iSCSI.

   - Per gateway Volume archiviato, scegli un ID disco.
   - Per gateway Volume memorizzato nella cache, scegli una capacità pari almeno alla risorsa protetta.
6. Per il ruolo di ripristino, scegli il ruolo IAM che AWS Backup assumerai per questo ripristino.

   > **Note**
   >
   > Se il ruolo AWS Backup predefinito non è presente nel tuo account, viene creato un ruolo predefinito con le autorizzazioni corrette. Puoi eliminare questo ruolo predefinito o renderlo inutilizzabile.
7. Scegli Restore backup (Ripristina backup).

   Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.

Il ripristino di uno snapshot EBS archiviato lo sposta temporaneamente dall'archiviazione a freddo a quella a caldo per creare un nuovo volume EBS. Questo tipo di ripristino comporta un costo di recupero una tantum. I costi per l'archiviazione a caldo e a freddo vengono fatturati durante il periodo di ripristino. I volumi EBS in cold storage non possono essere ripristinati su un volume gateway di Backup.

È possibile ripristinare uno snapshot EBS archiviato nell'archiviazione a freddo utilizzando la console AWS Backup o la riga di comando. Il ripristino dall'archiviazione a freddo può richiedere fino a 72 ore. Per ulteriori informazioni, consulta Archive Amazon EBS snapshot nella Amazon EBS User Guide.

Console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Vai a Vault di backup > *Vault* > Ripristina snapshot EBS archiviato.
3. Nella sezione Impostazioni inserisci un valore compreso tra 0 e 180 inclusi, per indicare il numero di giorni del periodo di ripristino temporaneo di uno snapshot archiviato.
4. Immetti altre impostazioni: tipo di volume, dimensione, IOPS, zona di disponibilità, velocità di trasmissione effettiva e crittografia.
5. Scegli il ruolo di ripristino.
6. Seleziona Ripristina backup. Nella finestra popup che viene visualizzata, verifica gli snapshot e il tipo di ripristino. Quindi, seleziona Ripristina snapshot.

AWS CLI

1. Utilizzare `start-restore-job`
2. Includi i parametri.
3.
4.
5.

Usa l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino Amazon EBS

Per ripristinare Amazon EBS utilizzando l'API o la CLI, utilizza `StartRestoreJob`. Durante i ripristini di Amazon ENS puoi specificare i seguenti metadati:

```
availabilityZone
volumeType
volumeSize
iops
throughput
temporaryRestoreDays
encrypted // if set to true, encryption will be enabled as volume is restored
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
 of default KMS Key Id
aws:backup:request-id
```

Esempio:

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

Ripristino di un file system Amazon EFS

Se è in corso il ripristino di un'istanza Amazon Elastic File System (Amazon EFS), puoi eseguire un ripristino completo o un ripristino a livello di elemento.

Ripristino completo

Quando si esegue il ripristino completo, viene ripristinato l'intero file system.

AWS Backup non supporta ripristini distruttivi con Amazon EFS. Un ripristino distruttivo si verifica quando un file system ripristinato elimina o sovrascrive il file system di origine o esistente. Invece, AWS Backup ripristina il file system in una directory di ripristino esterna alla directory principale.

Ripristino a livello di elemento

Quando esegui un ripristino a livello di elemento, AWS Backup ripristina un file o una directory specifici. È necessario specificare il percorso relativo alla radice del file system. Ad esempio, se il file system è montato in `/user/home/myname/efs` e il percorso del file è `user/home/myname/efs/file1`, immettere **`/file1`**. I percorsi fanno distinzione tra maiuscole e minuscole. I caratteri jolly e le stringhe regex non sono supportati. Il percorso potrebbe essere diverso da quello presente nell'host se il file system viene montato utilizzando un punto di accesso.

Quando si utilizza la console per eseguire un ripristino EFS, è possibile selezionare fino a 10 elementi. Quando si utilizza la CLI per ripristinare, non esiste un limite di elementi; tuttavia, esiste un limite di 200 KB sulla lunghezza dei metadati di ripristino che possono essere passati.

È possibile ripristinare tali elementi in un file system nuovo o esistente. In entrambi i casi, AWS Backup crea una nuova directory Amazon EFS (`aws-backup-restore_`*`datetime`*) esterna alla directory principale per contenere gli elementi. La gerarchia completa degli elementi specificati viene mantenuta nella directory di ripristino. Ad esempio, se la directory A contiene le sottodirectory B, C e D, AWS Backup mantiene la struttura gerarchica quando A, B, C e D vengono ripristinate. A prescindere che si esegua un ripristino a livello di elemento Amazon EFS su un file system nuovo o esistente, ogni tentativo di ripristino crea una nuova directory di ripristino fuori dalla directory principale per contenere i file ripristinati. Se si tenta di eseguire più ripristini per lo stesso percorso, potrebbero esistere diverse directory contenenti gli elementi ripristinati.

> **Note**
>
> Se si conserva un solo backup settimanale, è possibile ripristinare lo stato del file system solo come era al momento in cui è stato eseguito il backup. Non è possibile eseguire il ripristino da backup incrementali precedenti.

Usa la AWS Backup console per ripristinare un punto di ripristino Amazon EFS

Per ripristinare un file system Amazon EFS

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Il vault di backup EFS riceve la policy di accesso `Deny backup:StartRestoreJob` al momento della creazione. Se è la prima volta che si esegue il ripristino del vault di backup, è necessario modificare la policy di accesso come segue.

   a. Scegliere Vault di Backup.

   b. Scegli il vault di backup contenente il punto di ripristino che desideri ripristinare.

   c. Scorri verso il basso fino alla policy di accesso del vault.

   d. Se presente, elimina `backup:StartRestoreJob` da `Statement`. A tale scopo, scegli Modifica, elimina `backup:StartRestoreJob`, quindi scegli Salva policy.
3. Nel riquadro di navigazione, scegli Risorse protette e l'ID del file system EFS che si desidera ripristinare.
4. Nella pagina Dettagli della risorsa, viene visualizzato un elenco di punti di ripristino per l'ID del file system selezionato. Per ripristinare un file system, nel riquadro Backup scegli il pulsante di opzione accanto all'ID del punto di ripristino del file system. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
5. Specifica i parametri di ripristino per il file system. I parametri di ripristino immessi sono specifici del tipo di risorsa selezionato.

   È possibile eseguire un ripristino completo, che consente di ripristinare l'intero file system. In alternativa, è possibile ripristinare file e directory specifici utilizzando un Ripristino a livello di elemento.

   - Scegli l'opzione Ripristino completo per ripristinare il file system nella suo insieme, incluse tutte le cartelle e i file di livello root.

- Scegliere l'opzione Ripristino a livello di elemento per ripristinare un file o una directory specifici. Puoi selezionare e ripristinare fino a cinque elementi all'interno di Amazon EFS.

  Per ripristinare un file o una directory specifici, è necessario specificare il percorso relativo al punto di montaggio. Ad esempio, se il file system è montato in `/user/home/myname/efs` e il percorso del file è `user/home/myname/efs/file1`, immettere **`/file1`**. I percorsi fanno distinzione tra maiuscole e minuscole e non possono contenere caratteri speciali, caratteri jolly e stringhe regex.

  1. Nella casella di testo Percorso della voce immettere il percorso del file o della cartella.
  2. Scegliere Aggiungi elemento per aggiungere ulteriori file o directory. Puoi selezionare e ripristinare fino a cinque elementi nel file system EFS.

6. Per Posizione di ripristino

   - Scegli l'opzione Ripristina nella directory nel file system di origine se desideri eseguire il ripristino nel file system di origine.
   - Scegli Ripristina su un nuovo file system se desideri eseguire il ripristino in un file system diverso.

7. Per Tipo di file system

   - (Consigliato) Scegliete Regionale se desiderate ripristinare il file system su più zone di AWS disponibilità.
   - Scegli One Zone se desideri ripristinare il file system in una singola zona di disponibilità. Quindi, nel menu a discesa Zona di disponibilità, scegli la destinazione per il ripristino.

   Per ulteriori informazioni, consulta Gestione delle classi di storage Amazon EFS nella Guida per l'utente di Amazon EFS.

8. Per Prestazioni

   - Se hai scelto di eseguire un ripristino regionale, seleziona (Consigliato) Uso generale o I/O max.
   - Se hai scelto di eseguire un ripristino One Zone, devi selezionare (Consigliato) Uso generale. I ripristini One Zone non supportano I/O max.

9. Per Abilita la crittografia

- Scegliere Abilita crittografia, se si desidera crittografare il file system. Gli ID e gli alias delle chiavi KMS vengono visualizzati nell'elenco dopo essere stati creati utilizzando la console AWS Key Management Service (AWS KMS).
- Nella casella di testo Chiave KMS, scegli la chiave che desideri utilizzare dall'elenco.

10. Per il ruolo Restore, scegli il ruolo IAM che AWS Backup assumerai per questo ripristino.

> **Note**
>
> Se il ruolo AWS Backup predefinito non è presente nel tuo account, viene creato un ruolo predefinito con le autorizzazioni corrette. Puoi eliminare questo ruolo predefinito o renderlo inutilizzabile.

11. Scegli Restore backup (Ripristina backup).

    Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.

> **Note**
>
> Se si conserva un solo backup settimanale, è possibile ripristinare lo stato del file system solo come era al momento in cui è stato eseguito il backup. Non è possibile eseguire il ripristino da backup incrementali precedenti.

Usa l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino Amazon EFS

Utilizza `StartRestoreJob`. Durante il ripristino di un'istanza Amazon EFS, è possibile ripristinare un intero file system oppure file o directory specifici. Per ripristinare le risorse Amazon EFS, sono necessarie le seguenti informazioni:

- `file-system-id`— L'ID del file system Amazon EFS di cui è eseguito il backup AWS Backup. Restituito in `GetRecoveryPointRestoreMetadata`. Questo non è necessario quando viene ripristinato un nuovo file system (questo valore viene ignorato se il parametro lo `newFileSystem` è`True`).
- `Encrypted`: un valore booleano che, se true, specifica che il file system è crittografato. Se è specificato `KmsKeyId`, `Encrypted` deve essere impostato su `true`.
- `KmsKeyId`— specifica la AWS KMS chiave utilizzata per crittografare il file system ripristinato.

- `PerformanceMode`: specifica la modalità di velocità di trasmissione effettiva del file system.
- `CreationToken`: un valore fornito dall'utente che garantisce l'univocità (idempotenza) della richiesta.
- `newFileSystem`: un valore booleano che, se true, specifica che il punto di ripristino viene ripristinato in un nuovo file system Amazon EFS.
- `ItemsToRestore` : un array di un massimo di cinque stringhe in cui ogni stringa è un percorso di file. Utilizza `ItemsToRestore` per ripristinare file o directory specifici anziché l'intero file system. Questo parametro è facoltativo.

Puoi anche includere `aws:backup:request-id`.

I ripristini One Zone possono essere eseguiti includendo i parametri:

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

Per ulteriori informazioni sui valori di configurazione di Amazon EFS, consulta create-file-system.

Disabilitazione dei backup automatici in Amazon EFS

Per impostazione predefinita, Amazon EFS crea automaticamente backup di dati. Questi backup sono rappresentati come punti di ripristino in AWS Backup. I tentativi di rimuovere il punto di ripristino generano un messaggio di errore che indica che i privilegi non sono sufficienti per eseguire l'azione.

Come best practice, si consiglia di mantenere attivo questo backup automatico. In particolare in caso di cancellazione accidentale dei dati, questo backup consente il ripristino del contenuto del file system alla data dell'ultimo punto di ripristino creato.

Nell'improbabile eventualità che si desideri disattivarli, è necessario modificare la policy di accesso da `"Effect": "Deny"` a `"Effect": "Allow"`. Consulta la Guida per l'utente di Amazon EFS per ulteriori informazioni sull'attivazione/disattivazione dei backup automatici.

Ripristino di una tabella Amazon DynamoDB

Usa la AWS Backup console per ripristinare i punti di ripristino DynamoDB

Per ripristinare una tabella DynamoDB

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.

2. Nel riquadro di navigazione, scegli Risorse protette e l'ID della risorsa DynamoDB che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
4. In Impostazioni, nel campo di testoNuovo nome tabella immettere un nuovo nome di tabella.
5. Per il ruolo Restore, scegli il ruolo IAM che AWS Backup assumerai per questo ripristino.
6. Per Impostazioni di crittografia:

   a. Se il backup è gestito da DynamoDB (il suo ARN inizia `arn:aws:dynamodb` con) AWS Backup , cripta la tabella ripristinata utilizzando una chiave di proprietà. AWS

      Per scegliere una chiave diversa per crittografare la tabella ripristinata, è possibile utilizzare l' AWS Backup StartRestoreJoboperazione o eseguire il ripristino dalla console DynamoDB.

   b. Se il backup supporta la AWS Backup gestione completa (il relativo ARN inizia con`arn:aws:backup`), puoi scegliere una delle seguenti opzioni di crittografia per proteggere la tabella ripristinata:

      - (Impostazione predefinita) Chiave KMS di proprietà di DynamoDB (nessun costo aggiuntivo per la crittografia)
      - Chiave KMS gestita da DynamoDB (soggetta ai costi KMS)
      - Chiave KMS gestita dal cliente (soggetta ai costi KMS)

      Le chiavi "di proprietà di DynamoDB" e "gestite da DynamoDB" sono identiche alle chiavi "di proprietà di AWS" e "di proprietà di AWS", rispettivamente. Per chiarezza, consulta Crittografia dei dati inattivi: come funziona nella Guida per gli sviluppatori di Amazon DynamoDB.

      Per ulteriori informazioni sulla AWS Backup gestione completa, vedereBackup di DynamoDB avanzato.

> **Note**
>
> Le seguenti linee guida si applicano solo se si ripristina un backup copiato E si desidera crittografare la tabella ripristinata con la stessa chiave utilizzata per crittografare la tabella originale.
> Quando si ripristina un backup interregionale, per crittografare la tabella ripristinata utilizzando la stessa chiave utilizzata per crittografare la tabella originale, la chiave deve essere una chiave multiregionale. AWS Le chiavi possedute e gestite non sono chiavi AWS multiregionali. Per ulteriori informazioni, consulta Chiavi multi-regione nella Guida per gli sviluppatori di AWS Key Management Service .
> Quando si ripristina un backup su più account, per crittografare la tabella ripristinata utilizzando la stessa chiave utilizzata per crittografare la tabella originale, è necessario condividere la chiave dell'account di origine con l'account di destinazione. AWS Le chiavi -owned e AWS-managed non possono essere condivise tra account. Per ulteriori informazioni, consulta Consentire agli utenti in altri account di utilizzare una chiave KMS nella Guida per gli sviluppatori di AWS Key Management Service .

7. Scegli Restore backup (Ripristina backup).

   Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.

Utilizza l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino DynamoDB

Utilizza `StartRestoreJob`. Durante i ripristini di DynamoDB è possibile specificare i seguenti metadati. I metadati non rilevano la distinzione tra maiuscole e minuscole.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

Di seguito è riportato un esempio dell'argomento `restoreMetadata` per un'operazione `StartRestoreJob` nella CLI:

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-
g3hi-4567-8cjk-012345678901" \
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \
--metadata
 'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,KMSMasterKeyId=arn:aws:kms:us-
east-1:123456789012:key/abcdefg' \
--region us-east-1 \
--endpoint-url https://cell-1.gamma.us-east-1.controller.cryo.aws.a2z.com
```

L'esempio precedente crittografa la tabella ripristinata utilizzando una chiave di proprietà. AWS La parte dei metadati di ripristino che specifica la crittografia utilizzando la chiave -owned è AWS:. `\"encryptionType\":\"Default\",\"kmsMasterKeyArn\":\"Not Applicable\"`

Per crittografare la tabella ripristinata utilizzando una chiave AWS-managed, specifica i seguenti metadati di ripristino:. `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"Not Applicable\"`

Per crittografare la tabella ripristinata utilizzando una chiave gestita dal cliente, specifica i seguenti metadati di ripristino: `"encryptionType \":\"KMS\",\"kmsMasterKeyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`.

Ripristino di un database RDS

Per ripristinare un database Amazon RDS è necessario specificare più opzioni di ripristino. Per ulteriori informazioni su queste opzioni, consulta Backup e ripristino di un'istanza database di Amazon RDS nella Guida per l'utente di Amazon RDS.

Usa la AWS Backup console per ripristinare i punti di ripristino Amazon RDS

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e l'ID della risorsa Amazon RDS che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.

4. Nel riquadro Specifiche dell'istanza accettare le impostazioni predefinite o specificare le opzioni per le impostazioni Motore database, Modello di licenza, Classe dell'istanza DB, AZ multiple e Tipo di storage. Ad esempio, se desideri un'istanza database in standby, specifica Multi AZ.
5. Nel riquadro Impostazioni, specifica un nome univoco per tutte le istanze e i cluster di database di tua proprietà Account AWS nella regione corrente. L'identificatore istanze DB non fa distinzione tra maiuscole e minuscole ma è archiviato in sole lettere minuscole, come in "`mydbinstance`". Questo è un campo obbligatorio.
6. Nel riquadro Rete e sicurezza, accetta le impostazioni predefinite o specifica le opzioni per le impostazioni del Virtual Private Cloud (VPC), del gruppo di sottoreti, dell'accessibilità pubblica (di solito Sì) e della zona di disponibilità.
7. Nel riquadro Opzioni del database accettare le impostazioni predefinite o specificare le opzioni per Porta del database, Gruppo di parametri DB, Gruppo di opzioni, Copia i tag sugli snapshot e Autenticazione IAM DB abilitata .
8. Nel riquadro Crittografia, utilizza le impostazioni di default. Se l'istanza database di origine per lo snapshot è stata crittografata, anche l'istanza database ripristinata verrà crittografata. Questa crittografia non può essere rimossa.
9. Nel riquadro Esportazioni dei log, scegli i tipi di log da pubblicare su Amazon CloudWatch Logs. Il ruolo IAM è già definito.
10. Nel riquadro Manutenzione accettare l'impostazione predefinita o specificare l'opzione per Aggiornamento automatico della versione secondaria.
11. Nel riquadro Ripristina ruolo scegliere il ruolo IAM che AWS Backup assumerà per questo ripristino.
12. Una volta specificate tutte le impostazioni, scegliere Ripristina backup.

    Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.

Usa l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino Amazon RDS

Utilizza `StartRestoreJob`. Per informazioni sui metadati e sui valori accettati, consulta `RestoreDBInstanceFromDBSnapshot` nella Documentazione di riferimento dell'API Amazon RDS. Inoltre, AWS Backup accetta i seguenti attributi di sola informazione. Tuttavia, la loro specifica non influisce sul ripristino:

```
EngineVersion
```

```
KmsKeyId
Encrypted
vpcId
```

Ripristino di un cluster Amazon Aurora

Usa la AWS Backup console per ripristinare i punti di ripristino Aurora

AWS Backup ripristina il cluster Aurora; non crea o collega un'istanza Amazon RDS al cluster. Nei passaggi seguenti, viene illustrato come creare e collegare un'istanza Amazon RDS al cluster Aurora ripristinato tramite la CLI.

Per ripristinare un cluster Aurora è necessario specificare più opzioni di ripristino. Per informazioni su queste opzioni, consulta Panoramica di backup e ripristino di un cluster di database Aurora nella Guida per l'utente di Amazon Aurora. Le specifiche per le opzioni di ripristino sono disponibili nella guida API per. `RestoreDBClusterFromSnapshot`

Per ripristinare un cluster Amazon Aurora

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e l'ID della risorsa Aurora che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
4. Nel riquadro Specifiche dell'istanza accettare i valori predefiniti o specificare le opzioni per le impostazioni Motore database, dellaVersione motore database e Tipo di capacità.

   > **Note**
   >
   > Se è selezionato il tipo di capacità Serverless viene visualizzato un riquadro Impostazioni di capacità. Specificare le opzioni per Unità di capacità minima di Aurora e Unità di capacità massima di Aurora oppure scegliere opzioni diverse dalla sezione Configurazione di ridimensionamento aggiuntivo.

5. Nel riquadro Impostazioni, specifica un nome univoco per tutte le istanze del cluster DB di proprietà dell'utente Account AWS nella regione corrente.

6. Nel riquadro Rete e sicurezza, accettare le impostazioni predefinite o specificare le opzioni per le impostazioni di Cloud privato virtuale (VPC), Gruppo di sottoreti, e Zona di disponibilità.
7. Nel riquadro Opzioni database accettare le impostazioni predefinite o specificare le opzioni per le impostazioni Porta database, Gruppo di parametri del cluster DB e Autenticazione DB IAM abilitata.
8. Nel riquadro Backup accettare l'impostazione predefinita o specificare l'opzione per l'impostazione Copia i tag sugli snapshot.
9. Nel riquadro Backtrack accettare l'impostazione predefinita o specificare le opzioni per le impostazioni Abilita Backtrack o Disabilita Backtrack.
10. Nel riquadro Crittografia accettare l'impostazione predefinita o specificare le opzioni per le impostazioni Abilita crittografia o Disabilita crittografia.
11. Nel riquadro Esportazioni dei log, scegli i tipi di log da pubblicare su Amazon CloudWatch Logs. Il ruolo IAM è già definito.
12. Nel riquadro Ripristina ruolo scegliere il ruolo IAM che AWS Backup assumerà per questo ripristino.
13. Dopo aver specificato tutte le impostazioni, scegli Ripristina backup.

    Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.
14. Al termine del ripristino, collega il cluster Aurora ripristinato a un'istanza Amazon RDS.

    Utilizzo della AWS CLI:

    - Per Linux, macOS o Unix:

      ```
      aws rds create-db-instance --db-instance-identifier sample-instance \
                  --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
      instance-class db.r4.large
      ```

    - Per Windows:

      ```
      aws rds create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
      instance-class db.r4.large
      ```

Vedi backup e point-in-time ripristino continui (PITR) per informazioni sui backup continui e sul ripristino in un determinato momento.

Usa l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino Aurora

Utilizza `StartRestoreJob`. Durante i ripristini di Aurora puoi specificare i seguenti metadati:

```
List<String> availabilityZones;
Long backtrackWindow;
Boolean copyTagsToSnapshot;
String databaseName;
String dbClusterIdentifier;
String dbClusterParameterGroupName;
String dbSubnetGroupName;
List<String> enableCloudwatchLogsExports;
Boolean enableIAMDatabaseAuthentication;
String engine;
String engineMode;
String engineVersion;
String kmsKeyId;
Integer port;
String optionGroupName;
ScalingConfiguration scalingConfiguration;
List<String> vpcSecurityGroupIds;
```

Esempio:

```
"restoreMetadata":"{\"EngineVersion\":\"5.6.10a\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:234567890123:key/45678901-ab23-4567-8cd9-012d345e6f7\",\"EngineMode\":
\"serverless\",\"AvailabilityZones\":\"[\\\"us-east-1b\\\",\\\"us-east-1e\\\",\\
\"us-east-1c\\\"]\",\"Port\":\"3306\",\"DatabaseName\":\"\",\"DBSubnetGroupName\":
\"default-vpc-05a3b07cf6e193e1g\",\"VpcSecurityGroupIds\":\"[\\\"sg-012d52c68c6e88f00\
\\"]\",\"ScalingConfiguration\":\"{\\\"MinCapacity\\\":2,\\\"MaxCapacity\\\":64,
\\\"AutoPause\\\":true,\\\"SecondsUntilAutoPause\\\":300,\\\"TimeoutAction\\\":
\\\"RollbackCapacityChange\\\"}\",\"EnableIAMDatabaseAuthentication\":\"false\",
\"DBClusterParameterGroupName\":\"default.aurora5.6\",\"CopyTagsToSnapshot\":\"true\",
\"Engine\":\"aurora\",\"EnableCloudwatchLogsExports\":\"[]\"}"
```

Ripristino di un'istanza Amazon EC2

Quando ripristini un'istanza EC2, AWS Backup crea un'Amazon Machine Image (AMI), un'istanza, il volume root di Amazon EBS, i volumi di dati Amazon EBS (se la risorsa protetta aveva volumi di dati)

e gli snapshot di Amazon EBS. Puoi personalizzare alcune impostazioni dell'istanza utilizzando la AWS Backup console o un numero maggiore di impostazioni utilizzando o un SDK. AWS CLI AWS

Le seguenti considerazioni si applicano al ripristino delle istanze EC2:

- AWS Backup configura l'istanza ripristinata per utilizzare la stessa coppia di chiavi utilizzata originariamente dalla risorsa protetta. Non è possibile specificare una coppia di chiavi diversa per l'istanza ripristinata durante il processo di ripristino.
- AWS Backup non esegue il backup e il ripristino dei dati utente utilizzati durante l'avvio di un'istanza Amazon EC2.
- Quando configuri l'istanza ripristinata, puoi scegliere tra l'utilizzo dello stesso profilo di istanza utilizzato originariamente dalla risorsa protetta o l'avvio senza un profilo di istanza. In questo modo si impediscono possibili escalation dei privilegi. Puoi aggiornare il profilo dell'istanza ripristinata utilizzando la console Amazon EC2.

  Se utilizzi il profilo dell'istanza originale, devi concedere AWS Backup le seguenti autorizzazioni, dove l'ARN della risorsa è l'ARN del ruolo IAM associato al profilo dell'istanza.

  ```
  {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::account-id:role/role-name"
  },
  ```

- Durante un ripristino, si applicano tutte le quote e le limitazioni di configurazione di Amazon EC2.
- Se il vault contenente i punti di ripristino Amazon EC2 ha un blocco del vault, Ulteriori considerazioni sulla sicurezza consulta per ulteriori informazioni.

Usa la AWS Backup console per ripristinare i punti di ripristino di Amazon EC2

puoi ripristinare un'intera istanza Amazon EC2 da un singolo punto di ripristino, inclusi il volume root, i volumi di dati e alcune impostazioni di configurazione dell'istanza, come il tipo di istanza e la key pair.

Per ripristinare le risorse Amazon EC2 utilizzando la console AWS Backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette, quindi scegli l'ID della risorsa Amazon EC2 per aprire la pagina dei dettagli della risorsa.

3. Nel riquadro Punti di ripristino, scegli il pulsante di opzione accanto all'ID del punto di ripristino da ripristinare. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
4. Nel riquadro Impostazioni di rete, utilizziamo le impostazioni dell'istanza protetta per selezionare i valori predefiniti per il tipo di istanza, VPC, sottorete, gruppo di sicurezza e ruolo IAM dell'istanza. È possibile utilizzare questi valori predefiniti o modificarli in base alle esigenze.
5. Nel riquadro Ripristina ruolo, utilizza il ruolo predefinito o utilizza Scegli un ruolo IAM per specificare un ruolo IAM che concede l' AWS Backup autorizzazione per il ripristino del backup.
6. Nel riquadro Tag delle risorse protette, selezioniamo Copia i tag dalla risorsa protetta alla risorsa ripristinata per impostazione predefinita. Se non desideri copiare questi tag, deseleziona la casella di controllo.
7. Nel riquadro Impostazioni avanzate, accettate i valori predefiniti per le impostazioni dell'istanza o modificateli secondo necessità. Per informazioni su queste impostazioni, scegliete Informazioni per aprire il relativo riquadro di aiuto.
8. Al termine della configurazione dell'istanza, scegli Ripristina backup.

Ripristina Amazon EC2 con AWS CLI

Nell'interfaccia a riga di comando, `start-restore-job`consente di eseguire il ripristino con un massimo di 32 parametri (inclusi alcuni parametri che non sono personalizzabili tramite la AWS Backup console).

Di seguito è riportato l'elenco dei metadati che possono essere passati per ripristinare un punto di ripristino di Amazon EC2.

```
InstanceType
KeyName
SubnetId
Architecture
EnaSupport
SecurityGroupIds
IamInstanceProfileName
CpuOptions
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
CreditSpecification
Placement
RootDeviceType
```

```
RamdiskId
KernelId
UserData
Monitoring
NetworkInterfaces
ElasticGpuSpecification
CapacityReservationSpecification
InstanceMarketOptions
LicenseSpecifications
EbsOptimized
VirtualizationType
Platform
RequireIMDSv2
aws:backup:request-id
```

AWS Backup accetta i seguenti attributi di sola informazione. Tuttavia, la loro specifica non influisce sul ripristino:

```
vpcId
```

È inoltre possibile ripristinare un'istanza Amazon EC2 senza includere parametri archiviati. Questa opzione è disponibile nella scheda Risorse protette della console AWS Backup .

Ripristino di un volume Storage Gateway

Se stai ripristinando uno snapshot di AWS Storage Gateway volume, puoi scegliere di ripristinare lo snapshot come volume Storage Gateway o come volume Amazon EBS. Questo perché si AWS Backup integra con entrambi i servizi e qualsiasi snapshot di Storage Gateway può essere ripristinato su un volume Storage Gateway o su un volume Amazon EBS.

Ripristina Storage Gateway tramite la AWS Backup console

Per ripristinare un volume Storage Gateway

1. Aprire la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e l'ID della risorsa Storage Gateway che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione

accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.

4. Specificare i parametri di ripristino per la risorsa. I parametri di ripristino immessi sono specifici del tipo di risorsa selezionato.

   Per Tipo di risorsa, scegli la AWS risorsa da creare durante il ripristino di questo backup.

5. Se scegli Volume Storage Gateway, seleziona un Gateway in uno stato raggiungibile. Scegli anche Nome di destinazione iSCSI.

   1. Per gateway "Volume archiviato", scegli un ID disco.
   2. Per gateway "Volume memorizzato nella cache", scegli una capacità pari almeno alla risorsa protetta.

   Se si sceglie Volume EBS, specificare i valori per Tipo di volume, Dimensioni (GiB), e scegliere una Zona di disponibilità.

6. Per il ruolo di ripristino, scegli il ruolo IAM che AWS Backup assumerai per questo ripristino.

   > **Note**
   >
   > Se il ruolo AWS Backup predefinito non è presente nel tuo account, viene creato un ruolo predefinito con le autorizzazioni corrette. Puoi eliminare questo ruolo predefinito o renderlo inutilizzabile.

7. Scegli Restore backup (Ripristina backup).

   Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.

Ripristina Storage Gateway con AWS CLI

Nell'interfaccia a riga di comando, `start-restore-job` consente di ripristinare un volume Storage Gateway.

L'elenco seguente riporta i metadati accettati.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and Regione AWS.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
```

```
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Ripristino di una tabella Amazon Timestream

Quando si ripristina una tabella Amazon Timestream, esistono diverse opzioni da configurare, incluso il nuovo nome della tabella, il database di destinazione, le preferenze di allocazione dello storage (memoria e archivio magnetico) e il ruolo che verrà utilizzato per completare il processo di ripristino. È anche possibile scegliere un bucket Amazon S3 in cui archiviare i log di errore. Le scritture archivio magnetico sono asincrone, pertanto potrebbe essere necessario registrare gli errori.

L'archiviazione di dati Timestream ha due livelli: un archivio di memoria e un archivio magnetico. L'archivio di memoria è obbligatorio, ma è possibile trasferire la tabella ripristinata su un archivio magnetico al termine del tempo di memoria specificato. Memory Store è ottimizzato per scritture di dati ad alta velocità e point-in-time query veloci. L'archivio magnetico è ottimizzato per scritture dati late-arrival a bassa velocità di trasmissione effettiva, archiviazione di dati a lungo termine e query analitiche rapide.

Quando si ripristina una tabella Timestream, si determina per quanto tempo si desidera che la tabella rimanga in ciascun piano di storage. Utilizzando la console o l'API, puoi impostare il tempo di storage per entrambi. Tieni presente che lo storage è lineare e sequenziale. Timestream archivierà prima la tabella ripristinata nello storage in memoria, quindi la trasferirà automaticamente all'archivio magnetico quando viene raggiunto il tempo di storage in memoria.

> **Note**
>
> Il periodo di conservazione dell'archivio magnetico deve essere uguale o superiore al periodo di conservazione originale (mostrato nella parte superiore destra della console); in caso contrario, i dati andranno persi.

Esempio: si imposta l'allocazione dell'archivio di memoria per conservare i dati per una settimana e l'allocazione dell'archivio magnetico per conservare gli stessi dati per un anno. Quando i dati nell'archivio di memoria sono vecchi di una settimana, vengono spostati automaticamente nell'archivio magnetico. Vengono quindi mantenuti nell'archivio magnetico per un anno. Al termine di tale periodo, vengono eliminati da Timestream e da AWS Backup.

Per ripristinare una tabella Amazon Timestream utilizzando la console AWS Backup

Puoi ripristinare le tabelle Timestream nella AWS Backup console creata da. AWS Backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e l'ID della risorsa Amazon Timestream che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
4. Specifica le nuove impostazioni di configurazione della tabella, incluse:
   a. Nome nuova tabella, composto da 2 a 256 caratteri (lettere, numeri, trattini, punti e caratteri di sottolineatura).
   b. Database di destinazione, scelto dal menu a discesa.
5. Allocazione dello storage: imposta il tempo in cui la tabella ripristinata rimarrà per la prima volta nello storage di memoria e imposta il tempo in cui la tabella ripristinata rimarrà nello storage magnetico. Lo storage di memoria può essere impostato su ore, giorni, settimane o mesi. Lo storage magnetico può essere impostato su giorni, settimane, mesi o anni.
6. (Opzionale) Abilita scritture archivio magnetico: hai la possibilità di consentire le scritture archivio magnetico. Con questa opzione selezionata, i dati in ritardo, ovvero i dati con un timestamp che non rientra nel periodo di conservazione dello storage di memoria, verranno scritti direttamente nell'archivio magnetico.
7. (Facoltativo) Posizione dei registri degli errori di Amazon S3: puoi specificare una posizione S3 in cui verranno archiviati i log degli errori. Sfoglia i file S3 o copia e incolla il percorso file S3.

   > **Note**
   >
   > Se si sceglie di specificare una posizione nel registro degli errori S3, il ruolo utilizzato per questo ripristino deve disporre dell'autorizzazione per scrivere su un bucket S3 oppure deve contenere una policy con tale autorizzazione.

8. Scegli il ruolo IAM da passare per eseguire i ripristini. Puoi utilizzare il ruolo IAM predefinito o specificarne uno diverso.
9. Fai clic su Ripristina backup.

I processi di ripristino saranno visibili in Risorse protette. Per visualizzare lo stato attuale del processo di ripristino, fai clic sul pulsante di aggiornamento o premi CTRL-R.

Per ripristinare una tabella Amazon Timestream tramite API, CLI o SDK

Utilizza `StartRestoreJob` per ripristinare una tabella Timestream tramite API.

Per ripristinare un Timestream utilizzando il AWS CLI, utilizzate l'operazione `start-restore-job.` e specificate i seguenti metadati:

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
aws:backup:request-id
```

Di seguito è riportato un modello di esempio:

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-west-2:accountnumber:recovery-point:1a2b3cde-
f405-6789-012g-3456hi789012_beta" \
--iam-role-arn "arn:aws:iam::accountnumber:role/rolename" \
--metadata
 'TableName=tablename,DatabaseName=databasename,MagneticStoreRetentionPeriodInDays=1,MemoryStor
\":true,\"MagneticStoreRejectedDataLocation\":{\"S3Configuration\":{\"BucketName\":
\"bucketname\",\"EncryptionOption\":\"SSE_S3\"}}}"' \
--region us-west-2 \
--endpoint-url url
```

Inoltre, puoi utilizzare `DescribeRestoreJob` per fornire assistenza con le informazioni di ripristino.

In AWS CLI, utilizzate l'operazione `describe-restore-job` e utilizzate i seguenti metadati:

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
```

```
EnableMagneticStoreWrites?: boolean;
```

Di seguito è riportato un modello di esempio:

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Ripristino di un cluster Amazon Redshift

È possibile ripristinare istantanee automatiche e manuali nella AWS Backup console o tramite CLI.

Quando ripristini un cluster Amazon Redshift, le impostazioni cluster originali vengono inserite nella console per impostazione predefinita. Puoi specificare diverse impostazioni per le configurazioni seguenti. Durante il ripristino di una tabella, è necessario specificare i database di origine e di destinazione. Per ulteriori informazioni su queste configurazioni, consulta Ripristino di un cluster da uno snapshot nella Guida alla gestione di Amazon Redshift.

- Tabella singola o cluster: puoi scegliere di ripristinare un intero cluster o una singola tabella. Se scegli di ripristinare una singola tabella, sono necessari il database di origine, lo schema di origine e il nome della tabella di origine, nonché il cluster di destinazione, lo schema e il nome della nuova tabella.
- Tipo di nodo: ciascun cluster Amazon Redshift è costituito da un nodo principale e da almeno un nodo di calcolo. Durante il ripristino di un cluster, è necessario specificare il tipo di nodo che soddisfa i requisiti di CPU, RAM, capacità di storage e tipo di unità.
- Numero di nodi: durante il ripristino di un cluster, è necessario specificare il numero di nodi necessari.
- Riepilogo della configurazione
- Autorizzazioni del cluster

Per ripristinare un cluster o una tabella Amazon Redshift utilizzando la console AWS Backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e l'ID della risorsa Amazon Redshift che si desidera ripristinare.

3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Punti di ripristino scegli il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
4. Opzioni di ripristino

    a. Ripristina il cluster dallo snapshot, oppure

    b. Ripristina una singola tabella all'interno di uno snapshot in un nuovo cluster. Se scegli queste opzioni, devi configurare quanto segue:

        i. Attiva o disattiva i nomi con distinzione tra maiuscole e minuscole.

        ii. Immetti i valori della tabella di origine, inclusi il database, lo schema e la tabella. Le informazioni sulla tabella di origine sono disponibili nella console Amazon Redshift.

        iii. Immetti i valori della tabella di origine, inclusi il database, lo schema e il nome della nuova tabella.
5. Specifica le nuove impostazioni di configurazione del cluster.

    a. Per il ripristino del cluster: scegli l'identificatore del cluster, il tipo di nodo e il numero di nodi.

    b. Specifica la zona di disponibilità e le finestre di manutenzione.

    c. Puoi associare ruoli aggiuntivi facendo clic su Associa ruoli IAM.
6. Opzionale: configurazioni aggiuntive:

    a. Utilizza valori predefiniti è attivata per impostazione predefinita.

    b. Utilizza i menu a discesa per selezionare le impostazioni per Reti e sicurezza, gruppi di sicurezza del VPC, gruppo di sottoreti del cluster e zona di disponibilità.

    c. Attiva o disattiva il routing VPC avanzato.

    d. Determina se desideri rendere l'endpoint del cluster accessibile pubblicamente. In tal caso, le istanze e i dispositivi esterni al VPC possono connettersi al database tramite l'endpoint del cluster. Se questa opzione è attivata, inserisci l'indirizzo IP elastico.
7. Opzionale: configurazione del database. Puoi scegliere di inserire

    a. Porta del database (digitando nel campo di testo)

    b. Gruppi di parametri
8. Manutenzione: puoi scegliere

    a. Maintenance window (Finestra di manutenzione)

   b. Traccia di manutenzione, scegliendo tra corrente, finale o anteprima. Questo consente di controllare quale versione del cluster viene applicata durante una finestra di manutenzione.

9. Lo snapshot automatico è impostato come predefinito.

   a. Periodo di conservazione automatica degli snapshot. Il periodo di conservazione deve essere compreso tra 0 e 35 giorni. Scegli 0 per non creare snapshot automatici.

   b. Il periodo di conservazione degli snapshot manuali è compreso tra 1 e 3653 giorni.

   c. È disponibile una casella di controllo opzionale per il trasferimento del cluster. Se questa casella è selezionata, è possibile trasferire il cluster in un'altra zona di disponibilità. Dopo avere abilitato il trasferimento, puoi utilizzare l'endpoint VPC.

10. Monitoraggio: dopo il ripristino di un cluster, puoi configurare il monitoraggio tramite CloudWatch o Amazon Redshift.

11. Scegli il ruolo IAM da passare per eseguire i ripristini. Puoi utilizzare il ruolo predefinito o specificarne uno diverso.

I processi di ripristino saranno visibili in Processi. Per visualizzare lo stato attuale del processo di ripristino, fai clic sul pulsante di aggiornamento o premi CTRL-R.

Ripristino di un cluster Amazon Redshift tramite API, CLI o SDK

Utilizza `StartRestoreJob` per ripristinare un cluster Amazon Redshift.

Per ripristinare un Amazon Redshift utilizzando AWS CLI, usa il comando `start-restore-job` e specifica i seguenti metadati:

```
ClusterIdentifier // required string
AdditionalInfo // optional string
AllowVersionUpgrade // optional Boolean
AquaConfigurationStatus // optional string
AutomatedSnapshotRetentionPeriod // optional integer 0 to 35
AvailabilityZone // optional string
AvailabilityZoneRelocation // optional Boolean
ClusterParameterGroupName // optional string
ClusterSecurityGroups // optional array of strings
ClusterSubnetGroupName // optional strings
DefaultIamRoleArn // optional string
ElasticIp // optional string
Encrypted // Optional TRUE or FALSE
```

```
EnhancedVpcRouting // optional Boolean
HsmClientCertificateIdentifier // optional string
HsmConfigurationIdentifier // optional string
IamRoles // optional array of strings
KmsKeyId // optional string
MaintenanceTrackName // optional string
ManageMasterPassword // optional Boolean
ManualSnapshotRetentionPeriod // optional integer
MasterPasswordSecretKmsKeyId // optional string
NodeType // optional string
NumberOfNodes // optional integer
OwnerAccount // optional string
Port // optional integer
PreferredMaintenanceWindow // optional string
PubliclyAccessible // optional Boolean
ReservedNodeId // optional string
SnapshotClusterIdentifier // optional string
SnapshotScheduleIdentifier // optional string
TargetReservedNodeOfferingId // optional string
VpcSecurityGroupIds // optional array of strings
RestoreType // CLUSTER_RESTORE  or TABLE_RESTORE
```

Per ulteriori informazioni, consulta `RestoreFromClusterSnapshot` nella Documentazione di riferimento delle API Amazon Redshift e `restore-from-cluster-snapshot` nella Guida di AWS CLI .

Di seguito è riportato un modello di esempio:

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:backup:region:account:snapshot:name
-\-iam-role-arn "arn:aws:iam:account:role/role-name" \
-\-metadata
-\-resource-type Redshift \
-\-region Regione AWS
-\-endpoint-url URL
```

Ecco un esempio:

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:redshift:us-west-2:123456789012:snapshot:redshift-
cluster-1/awsbackup:job-c40dda3c-fdcc-b1ba-fa56-234d23209a40" \
-\-iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
```

```
-\-metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-
restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
-\-resource-type Redshift \
-\-region us-west-2 \
```

Inoltre, puoi utilizzare `DescribeRestoreJob` per fornire assistenza con le informazioni di ripristino.

In AWS CLI, utilizza l'operazione `describe-restore-job` e utilizza i seguenti metadati:

```
Region
```

Di seguito è riportato un modello di esempio:

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region Regione AWS
```

Ecco un esempio:

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
-\-region us-west-2 \
```

Ripristino di database SAP HANA su un'istanza Amazon EC2

I database SAP HANA su istanze EC2 possono essere ripristinati utilizzando la AWS Backup console, utilizzando l'API o utilizzando. AWS CLI

Argomenti

- Ripristina un database di istanze SAP HANA su Amazon EC2 utilizzando la console AWS Backup
- StartRestoreJob API per SAP HANA su EC2
- CLI per SAP HANA su EC2
- Risoluzione dei problemi

Ripristina un database di istanze SAP HANA su Amazon EC2 utilizzando la console AWS Backup

Tieni presente che i processi di backup e ripristino che coinvolgono lo stesso database non possono essere eseguiti contemporaneamente. Quando si verifica un processo di ripristino del database SAP

HANA, i tentativi di eseguire il backup dello stesso database generano un errore: "Database cannot be backed up while it is stopped".

1. Accedi alla AWS Backup console utilizzando le credenziali dei prerequisiti.
2. Nel menu a discesa Posizione di ripristino di destinazione, scegli un database da sovrascrivere con il punto di ripristino utilizzato per il ripristino (tieni presente che l'istanza che ospita il database di destinazione di ripristino deve anche disporre delle autorizzazioni previste dai prerequisiti).

   > **Important**
   >
   > I ripristini del database SAP HANA sono distruttivi. Il ripristino di un database sovrascriverà il database nella posizione di ripristino di destinazione specificata.

3. Completa questo passaggio solo se stai eseguendo un ripristino della copia del sistema; in caso contrario, vai al passaggio 4.

   I ripristini delle copie del sistema sono processi di ripristino che eseguono il ripristino in un database di destinazione diverso dal database di origine che ha generato il punto di ripristino. Per i ripristini delle copie del sistema, nota il comando `aws ssm-sap put-resource-permission` fornito sulla console. Questo comando deve essere copiato, incollato ed eseguito sul computer che ha completato i prerequisiti. Durante l'esecuzione del comando, utilizza le credenziali del ruolo nel prerequisito in cui imposti le autorizzazioni richieste per la registrazione delle applicazioni.

   ```
   // Example command
   aws ssm-sap put-resource-permission \
   --region us-east-1 \
   --action-type RESTORE \
   --source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
   --resource-arn arn:aws:ssm-sap:us-east-1:112233445566:HANA/Bar/DB/HDB
   ```

4. Dopo aver scelto la posizione di ripristino, puoi visualizzare ID risorsa, Nome applicazione, Tipo di database e Istanza EC2 del database di destinazione.
5. Facoltativamente, puoi aprire Impostazioni di ripristino avanzate per modificare l'opzione di ripristino del catalogo. La selezione predefinita prevede il ripristino del catalogo più recente da AWS Backup.
6. Fai clic su Ripristina backup.

7. La posizione di destinazione verrà sovrascritta durante il ripristino ("ripristino distruttivo"), quindi è necessario confermare l'autorizzazione nella successiva finestra di dialogo pop-up.

   a. Per procedere, è necessario comprendere che il database esistente verrà sovrascritto da quello che si sta ripristinando.

   b. Dopodiché, è necessario confermare che i dati esistenti verranno sovrascritti. Per confermare e procedere, digita overwrite nel campo di immissione di testo.

8. Fai clic su Ripristina backup.

Se la procedura è andata a buon fine, nella parte superiore della console verrà visualizzato un banner blu. Ciò significa che il processo di ripristino è in corso. Verrà eseguito il reindirizzamento automatico alla pagina Processi e il processo di ripristino verrà visualizzato nell'elenco dei processi di ripristino. Lo stato del processo più recente sarà `Pending`. Puoi cercare e quindi fare clic sull'ID del processo di ripristino per visualizzare i dettagli di ciascun processo di ripristino. Puoi aggiornare l'elenco dei processi di ripristino facendo clic sul pulsante di aggiornamento per visualizzare le modifiche apportate allo stato del processo di ripristino.

StartRestoreJob API per SAP HANA su EC2

Questa azione recupera la risorsa salvata identificata da un nome della risorsa Amazon (ARN).

Sintassi della richiesta

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Parametri della richiesta URI: la richiesta non utilizza parametri URI.

Corpo della richiesta: la richiesta accetta i seguenti dati in formato JSON:

IdempotencyTokenUna stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a. `StartRestoreJob` Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

▪Tipo: stringa

Campo obbligatorio: no

Metadati

Un set di coppie chiave-valore di metadati. Contiene informazioni, come il nome di una risorsa, necessarie per ripristinare un punto di ripristino. Puoi ottenere i metadati di configurazione relativi a una risorsa al momento del backup chiamando `GetRecoveryPointRestoreMetadata`. Tuttavia, per ripristinare una risorsa potrebbero essere necessari altri valori oltre a quelli forniti da `GetRecoveryPointRestoreMetadata`. Ad esempio, potrebbe essere necessario fornire un nuovo nome di risorsa se l'originale esiste già.

È necessario includere metadati specifici per ripristinare un'istanza SAP HANA su Amazon EC2. Visualizza i StartRestoreJob metadati per gli elementi specifici di SAP HANA.

Per recuperare i metadati pertinenti, puoi utilizzare la chiamata `GetRecoveryPointRestoreMetadata`.

Esempio di un punto di ripristino standard del database SAP HANA:

```
"RestoreMetadata": {
        "BackupSize": "1660948480",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "SYSTEM",
        "HanaBackupEndTime": "1674838362",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
        "HanaBackupStartTime": "1674838349",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/DATABASENAME",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9c"
    }
```

Esempio di un punto di ripristino continuo del database SAP HANA:

```
"RestoreMetadata": {
        "AvailableRestoreBases":
 "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
        "BackupSize": "1711284224",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "TENANT",
        "EarliestRestorablePitrTimestamp": "1674764799789",
        "HanaBackupEndTime": "1668032687",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_HDB_FULL",
        "HanaBackupStartTime": "1668032667",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "LatestRestorablePitrTimestamp": "1674850299789",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/SystemDatabaseSid",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9d"
    }
```

CLI per SAP HANA su EC2

Il comando `start-restore-job` recupera la risorsa salvata identificata da un nome della risorsa Amazon (ARN). La CLI seguirà le linee guida API di cui sopra.

Riepilogo:

```
start-restore-job
--recovery-point-arn value
--metadata value
--aws:backup:request-id value
[--idempotency-token value]
[--resource-type value]
[--cli-input-json value]
[--generate-cli-skeleton value]
[--debug]
[--endpoint-url value]
[--no-verify-ssl]
[--no-paginate]
[--output value]
```

```
[--query value]
[--profile value]
[--region value]
[--version value]
[--color value]
[--no-sign-request]
[--ca-bundle value]
[--cli-read-timeout value]
[--cli-connect-timeout value]
```

Opzioni

`--recovery-point-arn` (stringa) è una stringa sotto forma di un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

`--metadata` (mappa): un set di coppie chiave-valore di metadati. Contiene informazioni, come il nome di una risorsa, necessarie per ripristinare un punto di ripristino. Puoi ottenere i metadati di configurazione relativi a una risorsa al momento del backup chiamando `GetRecoveryPointRestoreMetadata`. Tuttavia, per ripristinare una risorsa potrebbero essere necessari altri valori oltre a quelli forniti da `GetRecoveryPointRestoreMetadata`. È necessario specificare metadati per ripristinare un'istanza SAP HANA su Amazon EC2:

- `aws:backup:request-id`: questa è una qualsiasi stringa UUID utilizzata per idempotenza. Non altera in alcun modo l'esperienza di ripristino.
- `aws:backup:TargetDatabaseArn`: specifica il database in cui eseguire il ripristino. Questo è l'ARN del database SAP HANA su Amazon EC2.
- `CatalogRestoreOption`: specifica da dove ripristinare il catalogo. Uno di `NO_CATALOG`, `LATEST_CATALOG_FROM_AWS_BACKUP`, `CATALOG_FROM_LOCAL_PATH`
- `LocalCatalogPath`: Se il valore CatalogRestoreOption dei metadati è`CATALOG_FROM_LOCAL_PATH`, specifica il percorso del catalogo locale sull'istanza EC2. Questo deve essere un percorso di file valido nell'istanza EC2.
- `RecoveryType`: attualmente sono supportati i tipi di ripristino `FULL_DATA_BACKUP_RECOVERY`, `POINT_IN_TIME_RECOVERY` e `MOST_RECENT_TIME_RECOVERY`.

key = (stringa); value = (stringa). Sintassi abbreviata:

```
KeyName1=string,KeyName2=string
```

Sintassi JSON:

```
{"string": "string"
  ...}
```

`--idempotency-token` è una stringa scelta dal cliente che puoi utilizzare per distinguere tra chiamate a `StartRestoreJob` altrimenti identiche. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

`--resource-type` è una stringa che avvia un processo per ripristinare un punto di ripristino per una delle seguenti risorse: `SAP HANA on Amazon EC2` per SAP HANA su Amazon EC2. Facoltativamente, le risorse SAP HANA possono essere contrassegnate utilizzando il comando `aws ssm-sap tag-resource`

Output: `RestoreJobId` è una stringa che identifica in modo univoco il processo che ripristina un punto di ripristino.

Risoluzione dei problemi

Se durante il tentativo di eseguire un'operazione di backup si verifica uno dei seguenti errori, consulta la risoluzione associata.

- Errore: errore log di backup continuo

  Per mantenere i punti di ripristino per i backup continui, i log vengono creati da SAP HANA per tutte le modifiche. Quando i log non sono disponibili, lo stato di ciascuno di questi punti di ripristino continui è `STOPPED`. L'ultimo punto di ripristino valido che può essere utilizzato per il ripristino è quello con lo stato `AVAILABLE`. Se i dati di log mancano per il tempo tra i punti di ripristino con uno stato `STOPPED` e i punti con uno stato `AVAILABLE`, non è possibile garantire che il ripristino abbia esito positivo in questi orari. Se inserisci una data e un'ora all'interno di questo intervallo, AWS Backup tenterà di eseguire il backup, ma utilizzerà l'orario di ripristino più vicino disponibile. Questo errore verrà visualizzato dal messaggio `“Encountered an issue with log backups. Please check SAP HANA for details."`

  Risoluzione: nella console, viene visualizzata l'ora ripristinabile più recente, in base ai log. Puoi inserire un'ora più recente di quella visualizzata. Tuttavia, se i dati relativi a questo periodo non sono disponibili nei registri, AWS Backup utilizzerà l'ora di ripristino più recente.

- Errore: `Internal error`

  Soluzione: crea una richiesta di supporto dalla tua console o contatta AWS Support i dettagli del ripristino, ad esempio l'ID del processo di ripristino.

- Errore: `The provided role arn:aws:iam::ACCOUNT_ID:role/ServiceLinkedRole cannot be assumed by AWS Backup`

  Risoluzione: assicurati che il ruolo assunto durante la chiamata al ripristino disponga delle autorizzazioni necessarie per creare ruoli collegati al servizio.

- Errore: `User: arn:aws:sts::ACCOUNT_ID:assumed-role/ServiceLinkedRole/AWSBackup-ServiceLinkedRole is not authorized to perform: ssm-sap:GetOperation on resource: arn:aws:ssm-sap:us-east-1:ACCOUNT_ID:...`

  Risoluzione: assicurati che il ruolo assunto durante la chiamata alle autorizzazioni di ripristino descritte nei prerequisiti sia inserito correttamente.

- Errore: `b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n`

  Risoluzione: assicurati che l'agente Backint sia stato installato correttamente. Verifica tutti i prerequisiti, in particolare Install AWS BackInt Agent and AWS Systems Manager for SAP sul tuo server delle applicazioni SAP, quindi riprova a installare l'agente. BackInt

- Errore: `IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED`

  Risoluzione: il processo di ripristino è stato annullato dal flusso di lavoro del servizio. Riprova il processo di ripristino.

- Errore: `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"`

  Risoluzione: instabilità di rete temporanea si verifica sull'istanza. Riprova a eseguire il ripristino. Se questo problema si verifica costantemente, prova ad aggiungere `ForceRetry: "true"` al file di configurazione dell'agente in `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml`.

Per qualsiasi altro problema relativo all'agente AWS Backint, consulta Risoluzione dei problemi di Backint AWS Agent per SAP HANA.

Ripristino di un cluster DocumentDB

Usa la AWS Backup console per ripristinare i punti di ripristino di Amazon DocumentDB

Per ripristinare un cluster Amazon DocumentDB è necessario specificare più opzioni di ripristino. Per informazioni su queste opzioni, consulta Ripristino da uno snapshot del cluster nella Guida per gli sviluppatori di Amazon DocumentDB.

Per ripristinare un cluster Amazon DocumentDB

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione, scegli Risorse protette e l'ID della risorsa Amazon DocumentDB che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
4. Nel riquadro Configurazione, accetta le impostazioni predefinite o specifica le opzioni per Identificatori del cluster, Versione motore, Classe istanza e Numero di istanze.
   - NOTA: se il VPC predefinito non esiste durante il ripristino, è necessario specificare una sottorete in un altro VPC.
5. Nel riquadro Rete e sicurezza, verrà visualizzato "Nessuna preferenza".
6. Nel ncryption-at-rest riquadro E, accetta l'impostazione predefinita o specifica le opzioni per le impostazioni Abilita crittografia o Disabilita crittografia.
7. Nel riquadro Opzioni del cluster, digita Porta e scegli il Gruppo di parametri del cluster.
8. Nel riquadro Backup, scegli PITR (Continuous Backup for point-in-time Recovery), backup snapshot pianificati o entrambi.
9. Nel riquadro Esportazioni dei log, scegli i tipi di log da pubblicare su Amazon CloudWatch Logs. Il ruolo IAM è già definito.
10. Nel riquadro Manutenzione, specifica una finestra di manutenzione o scegli Nessuna preferenza.
11. Nel riquadro Tag, puoi scegliere Aggiungi.
12. Per Protezione da eliminazione, puoi scegliere Abilita la protezione da eliminazione.
13. Dopo aver specificato tutte le impostazioni, scegli Ripristina backup.

Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.

14. Al termine del ripristino, collega il cluster Amazon DocumentDB ripristinato a un'istanza Amazon RDS.

Usa l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino di Amazon DocumentDB

Innanzitutto, ripristina il cluster. Utilizza `StartRestoreJob`. Durante i ripristini di Amazon DocumentDB puoi specificare i seguenti metadati:

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

Quindi, collega il cluster Amazon DocumentDB ripristinato a un'istanza Amazon RDS utilizzando `create-db-instance`.

- Per Linux, macOS o Unix:

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Per Windows:

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Ripristino di un cluster Neptune

Usa la AWS Backup console per ripristinare i punti di ripristino di Amazon Neptune

Per ripristinare un database Amazon Neptune è necessario specificare più opzioni di ripristino. Per informazioni su queste opzioni, consulta Ripristino da uno snapshot cluster database nella Guida per l'utente di Neptune.

Per ripristinare un database Neptune

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegli Risorse protette e l'ID della risorsa Neptune che desideri ripristinare.
3. Nella pagina Dettagli della risorsa viene visualizzato un elenco di punti di ripristino per l'ID risorsa selezionata. Per ripristinare una risorsa, nel riquadro Backup scegliere il pulsante di opzione accanto all'ID del punto di ripristino della risorsa. Nell'angolo superiore destro del riquadro, scegliere Ripristina.
4. Nel riquadro Specifiche dell'istanza, accetta le impostazioni predefinite o specifica il Motore DB e la Versione.
5. Nel riquadro Impostazioni, specifica un nome univoco per tutte le istanze del cluster DB di proprietà dell'utente Account AWS nella regione corrente. L'identificatore del cluster DB non fa distinzione tra maiuscole e minuscole ma è archiviato in sole lettere minuscole, come in "`mydbclusterinstance`". Questo è un campo obbligatorio.
6. Nel riquadro Opzioni del database, accetta le impostazioni predefinite o specificare le opzioni per le impostazioni Porta del database e Gruppo di parametri del cluster DB.
7. Nel riquadro Crittografia accettare l'impostazione predefinita o specificare le opzioni per le impostazioni Abilita crittografia o Disabilita crittografia.
8. Nel riquadro Esportazioni dei log, scegli i tipi di log da pubblicare su Amazon CloudWatch Logs. Il ruolo IAM è già definito.

9. Nel riquadro Ripristina ruolo scegliere il ruolo IAM che AWS Backup assumerà per questo ripristino.
10. Dopo aver specificato tutte le impostazioni, scegli Ripristina backup.

    Viene visualizzato il riquadro Lavori di ripristino. Un messaggio nella parte superiore della pagina fornisce informazioni sul lavoro di ripristino.
11. Al termine del ripristino, collega il cluster Neptune ripristinato a un'istanza Amazon RDS.

Usa l' AWS Backup API, la CLI o l'SDK per ripristinare i punti di ripristino di Neptune

Innanzitutto, ripristina il cluster. Utilizza `StartRestoreJob`. Durante i ripristini di Amazon DocumentDB puoi specificare i seguenti metadati:

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

Quindi, collega il cluster Neptune ripristinato a un'istanza Amazon RDS utilizzando `create-db-instance`.

- Per Linux, macOS o Unix:

```
aws neptune create-db-instance --db-instance-identifier sample-instance \
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- Per Windows:

```
aws neptune create-db-instance --db-instance-identifier sample-instance ^
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

Per ulteriori informazioni, consulta `RestoreDBClusterFromSnapshot` nella Documentazione di riferimento delle API di gestione Neptune e `restore-db-cluster-from-snapshot` nella Neptune CLI guide.

Ripristina i backup CloudFormation dello stack

Un backup CloudFormation composito è una combinazione di un CloudFormation modello e di tutti i punti di ripristino annidati associati. È possibile ripristinare un numero qualsiasi di punti di ripristino nidificati, ma il punto di ripristino composito (che è il punto di ripristino di primo livello) non può essere ripristinato.

Quando si ripristina un punto di ripristino del CloudFormation modello, si crea un nuovo stack con un set di modifiche per rappresentare il backup.

Ripristina CloudFormation con la AWS Backup console;

Dalla CloudFormation console puoi vedere il nuovo stack e il set di modifiche. Per ulteriori informazioni sui set di modifiche, consulta Aggiornamento di stack utilizzando i set di modifiche nella Guida per l'utente di AWS CloudFormation .

Determina da quali punti di ripristino annidati desideri eseguire il ripristino con CloudFormation lo stack, quindi ripristinali utilizzando la console. AWS Backup

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Passa a Vault di backup, seleziona il vault di backup contenente il punto di ripristino desiderato, quindi fai clic su Punti di ripristino.
3. Ripristina il punto AWS CloudFormation di ripristino del modello.

    a. Fai clic sul punto di ripristino composito contenente i punti di ripristino nidificati che desideri ripristinare per visualizzare la pagina Dettagli relativa al punto di ripristino composito.

    b. In Punti di ripristino nidificati, verranno visualizzati i punti di ripristino nidificati. Ogni punto di ripristino avrà un ID del punto di ripristino, uno stato, un ID risorsa, un tipo di risorsa, un tipo di backup e l'ora di creazione del punto di ripristino. Fai clic sul pulsante di opzione

accanto al punto di AWS CloudFormation ripristino, quindi fai clic su Ripristina. Assicurati di selezionare il punto di ripristino con il tipo di risorsa: AWS CloudFormation e il tipo di backup: backup.

4. Una volta completato il processo di ripristino del CloudFormation modello, il AWS CloudFormation modello ripristinato sarà visibile nella AWS CloudFormation console sotto Stacks.
5. In Nomi stack è disponibile il modello ripristinato con lo stato di `REVIEW_IN_PROGRESS`.
6. Fai clic sul nome dello stack per visualizzarne i relativi dettagli.
7. Sotto il nome dello stack sono disponibili delle schede. Fai clic su Set di modifiche.
8. Esegui il set di modifiche.
9. Dopo questi processi, le risorse nello stack originale verranno ricreate nel nuovo stack. Le risorse stateful verranno ricreate vuote. Per ripristinare le risorse stateful, torna all'elenco dei punti di ripristino nella AWS Backup console, seleziona il punto di ripristino necessario e avvia un ripristino.

Ripristina con CloudFormation AWS CLI

Nell'interfaccia a riga di comando, `start-restore-job`consente di ripristinare uno CloudFormation stack.

L'elenco seguente contiene i metadati accettati per ripristinare una CloudFormation risorsa.

```
// Mandatory metadata:
ChangeSetName // This is the name of the change set which will be created
StackName // This is the name of the stack that will be created by the new change set

// Optional metadata:
ChangeSetDescription // This is the description of the new change set
StackParameters // This is the JSON of the stack parameters required by the stack
aws:backup:request-id
```

Test di ripristino

Argomenti

- Panoramica
- Confronto tra test di ripristino e processo di ripristino

Panoramica

Il test di ripristino, una funzionalità offerta da AWS Backup, fornisce una valutazione automatica e periodica della fattibilità del ripristino, oltre alla possibilità di monitorare i tempi di durata dei processi di ripristino.

Innanzitutto, crea un piano di test di ripristino in cui fornisci un nome per il piano, la frequenza dei test di ripristino e l'ora di inizio prevista. Quindi, assegna le risorse da includere nel piano. Quindi scegli di includere punti di ripristino specifici o casuali nel test. AWS Backup backup deduce in modo intelligente i metadati necessari per il successo del processo di ripristino.

Quando arriva l'orario previsto dal piano, AWS Backup avvia i processi di ripristino in base al piano e monitora il tempo impiegato per completare il ripristino.

Una volta completata l'esecuzione del piano di test di ripristino, è possibile utilizzare i risultati per dimostrare la conformità ai requisiti organizzativi o di governance, ad esempio l'esito positivo degli scenari di test di ripristino o il tempo di completamento del processo di ripristino.

Facoltativamente, è possibile utilizzarlo Ripristina la convalida dei test per confermare i risultati del test di ripristino.

Una volta completata la convalida opzionale o chiusa la finestra di convalida, AWS Backup elimina le risorse coinvolte nel test di ripristino e le risorse verranno eliminate in conformità agli SLA del servizio.

Al termine del processo di test, è possibile visualizzare i risultati e l'ora di completamento.

Confronto tra test di ripristino e processo di ripristino

Il test di ripristino esegue i processi di ripristino allo stesso modo di come vengono eseguiti i ripristini on demand e utilizza gli stessi punti di ripristino (backup) di un ripristino on demand. Verranno visualizzate le chiamate a `StartRestoreJob` in CloudTrail (se l'opzione è stata attivata) per ogni processo avviato dal restore testing

Tuttavia, ci sono alcune differenze tra l'esecuzione di un test di ripristino pianificato e un'operazione di ripristino on demand:

	Test di ripristino	Ripristino
Account	La best practice consigliata è designare un account da utilizzare per i test di ripristino.	È possibile ripristinare le risorse da un account.
AWS Backup Audit Manager	Può attivare un controllo per verificare se un test di ripristino soddisfa gli obiettivi di ripristino specificati.	
Cadenza	Periodica, come parte di un piano programmato.	On demand
Regionalità	Disponibile in tutte le regioni commerciali in cui AWS Backup opera ad eccezione di Israele (Tel Aviv) Non disponibile AWS GovCloud (Stati Uniti orientali), AWS GovCloud (Stati Uniti occidentali), Cina (Pechino) e Cina (Ningxia).	Disponibile in tutte le regioni commerciali in cui opera AWS Backup
Risorse	I tipi di risorse che puoi assegnare al piano di test	Tutte le risorse possono essere ripristinate.

	Test di ripristino	Ripristino
	sono: Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, Amazon FSx (Lustre, ONTAP, OpenZFS, Windows), Amazon Neptune, Amazon RDS e Amazon S3.	
Risultati	Una volta completato il processo di test di ripristino, la risorsa ripristinata viene eliminata al termine della Ripristina la convalida dei test finestra.	Una volta completato il processo di ripristino, la versione ripristinata della risorsa rimane.
Tag	Per i tipi di risorsa che li supportano, il test applica i tag per il ripristino.	I tag sono opzionali per le risorse supportate.

Gestione del test di ripristino

È possibile creare, visualizzare, aggiornare o eliminare un piano di test di ripristino nella console AWS Backup.

Puoi usare la AWS CLI per eseguire a livello di codice operazioni per i piani di test di ripristino. Ogni CLI è specifica per il AWS servizio da cui proviene. I comandi devono essere preceduti da `aws backup`.

Eliminazione dei dati

Al termine di un test di ripristino, AWS Backup inizia a eliminare le risorse coinvolte nel test. Questa eliminazione non è immediata. Ogni risorsa ha una configurazione sottostante che determina il modo in cui tali risorse vengono archiviate e il loro ciclo di vita. Ad esempio, se i bucket Amazon S3 fanno parte del test di ripristino, le regole del ciclo di vita vengono aggiunte al bucket. L'esecuzione delle regole e l'eliminazione completa del bucket e dei relativi oggetti possono richiedere diversi giorni, ma i

costi per queste risorse vengono addebitati solo fino al giorno in cui viene avviata la regola del ciclo di vita (per impostazione predefinita è 1 giorno). La velocità di eliminazione dipende dal tipo di risorsa.

Le risorse che fanno parte di un piano di test di ripristino contengono un tag chiamato `awsbackup-restore-test`. Se un utente rimuove questo tag, AWS Backup non può eliminare la risorsa alla fine del periodo di test e dovrà invece eliminarla manualmente.

Per verificare il motivo per cui le risorse non vengono eliminate come previsto, puoi cercare tra i processi non riusciti nella console o utilizzare l'interfaccia a riga di comando per richiamare la richiesta API `DescribeRestoreJob` per recuperare i messaggi di stato dell'eliminazione.

I piani di backup (piani di test non di ripristino) ignorano le risorse create dai test di ripristino (quelle con tag `awsbackup-restore-test` o nome che inizia con`awsbackup-restore-test`).

Controllo dei costi

Il test di ripristino prevede un costo per ogni test eseguito. A seconda delle risorse incluse nel piano di test di ripristino, anche i processi di ripristino che fanno parte del piano potrebbero avere un costo. Per i dettagli completi, consulta Prezzi di AWS Backup.

Quando si imposta un piano di test di ripristino per la prima volta, può essere utile includere un numero contenuto di tipi di risorsa e risorse protette per acquisire familiarità con la funzionalità, il processo e i costi medi sostenuti. Puoi aggiornare un piano dopo averlo creato per aggiungere altri tipi di risorsa e risorse protette.

Creazione di un piano di test di ripristino

Un piano di test di ripristino è composto da due parti: la creazione del piano e l'assegnazione delle risorse.

Quando si utilizza la console, queste parti sono sequenziali. Nella prima parte, si impostano il nome, la frequenza e l'ora di inizio. Nella seconda parte si assegnano le risorse al piano di test.

Quando si utilizza AWS CLI un'API, primo utilizzo `create-restore-testing-plan`. Dopo aver ricevuto una risposta corretta e aver creato il piano, si usa `create-restore-testing-selection` per ogni tipo di risorsa da includere nel piano.

Console

Parte I: creazione di un piano di test di ripristino mediante la console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.

2. Nel pannello di navigazione a sinistra, individua e seleziona Test di ripristino.
3. Scegli Crea un piano di test di ripristino.
4. Generale

    a. Nome: digita un nome per il nuovo piano di test di ripristino. Il nome non può essere modificato dopo la creazione. Il nome deve contenere solo caratteri alfanumerici e caratteri di sottolineatura.

    b. Frequenza del test: scegli la frequenza con cui verranno eseguiti i test di ripristino.

    c. Ora di avvio: imposta l'ora (in ore e minuti) in cui preferisci iniziare il test. Puoi anche impostare il fuso orario locale in cui desideri che venga eseguito il piano di ripristino del test.

    d. Inizia entro: questo valore (in ore) è il periodo di tempo in cui è previsto l'inizio del test di ripristino. AWS Backup si impegna al massimo per avviare tutti i processi di ripristino designati entro il termine di avvio e ordomizza gli orari di avvio entro questo periodo.

5. Selezione del punto di ripristino: ti consente di impostare i vault di origine, l'intervallo dei punti di ripristino e i criteri di selezione per i punti di ripristino (backup) che desideri includere nel piano.

    a. Vault di origine: scegli se includere tutti i vault disponibili o solo vault specifici per filtrare i punti di ripristino che possono essere inclusi nel piano. Se scegli Vault specifici, seleziona dal menu a discesa i vault che desideri includere.

    b. Punti di ripristino idonei: specifica l'intervallo di tempo in base al quale vengono selezionati i punti di ripristino. Puoi selezionare da 1 a 365 giorni, da 1 a 52 settimane, da 1 a 12 mesi o 1 anno.

    c. Criteri di selezione: una volta specificato l'intervallo di date dei punti di ripristino, puoi scegliere se includere nel piano l'ultimo punto di ripristino oppure un punto di ripristino casuale. Puoi sceglierne uno casuale per valutare lo stato generale dei punti di ripristino con una frequenza più regolare, nel caso in cui sia giustificato il ripristino di una versione precedente.

    d. Punti di oint-in-time ripristino P: se il piano include risorse con punti di backup continui (point-in-time-restore/PITR), puoi selezionare questa casella per fare in modo che il piano di test includa backup continui come punti di ripristino idonei (vedi Disponibilità delle funzionalità per risorsa per quali tipi di risorse dispongono di questa funzionalità).

6. (Facoltativo) Tag aggiunti al piano di test di ripristino: puoi scegliere di aggiungere al piano di test di ripristino fino a 50 tag. Ogni tag deve essere aggiunto separatamente. Per aggiungere un nuovo tag scegli Aggiungi nuovo tag.

Parte II: assegnazione delle risorse al piano mediante la console

In questa sezione scegli le risorse di cui hai eseguito il backup per includerle nel piano di test di ripristino. Scegli il nome dell'assegnazione di risorsa, seleziona il ruolo da utilizzare per il test di ripristino e imposta il periodo di conservazione prima della pulizia. Quindi, seleziona il tipo di risorsa e l'ambito e, facoltativamente, puoi perfezionare la selezione con i tag.

> **Tip**
>
> Per tornare al piano di test di ripristino a cui desideri aggiungere le risorse, puoi andare alla console AWS Backup, selezionare Test di ripristino, quindi trovare e selezionare il piano di test desiderato.

1. Generale

   a. Nome assegnazione di risorsa: inserisci un nome per l'assegnazione di risorsa utilizzando una stringa di caratteri alfanumerici e caratteri di sottolineatura, senza spazi.

   b. Ruolo IAM di ripristino: il test deve utilizzare un ruolo Identity and Access Management (IAM) designato. Puoi scegliere il ruolo AWS Backup predefinito o uno diverso. Se il AWS Backup valore predefinito non esiste ancora al termine di questo processo, lo AWS Backup creerà automaticamente con le autorizzazioni necessarie. Il ruolo IAM che scegli per il test di ripristino deve contenere le autorizzazioni specificate in AWSBackupServicePolicyForRestores.

   c. Periodo di conservazione prima della pulizia: durante un test di ripristino, i dati di backup vengono temporaneamente ripristinati. Per impostazione predefinita, questi dati vengono eliminati al termine del test. È possibile ritardare l'eliminazione di questi dati se desideri eseguire la convalida del ripristino.

      Se prevedi di eseguire la convalida, seleziona Conserva per un numero specifico di ore e inserisci un valore compreso tra 1 e 168 ore, incluse. Tieni presente che la convalida può essere eseguita a livello di codice ma non dalla console AWS Backup .

2. Risorse protette:

a. Seleziona il tipo di risorsa: seleziona i tipi di risorsa e l'ambito dei relativi backup da includere nel piano di test delle risorse. Ogni piano può contenere più tipi di risorsa, ma ogni tipo deve essere singolarmente assegnato al piano.

b. Ambito di selezione delle risorse: una volta scelto il tipo, seleziona se desideri includere tutte le risorse protette disponibili di quel tipo o solo risorse protette specifiche.

c. (Facoltativo) Perfeziona la selezione delle risorse usando i tag: se i backup contengono tag, puoi filtrare per tag per selezionare risorse protette specifiche. Immetti la chiave del tag, la condizione per cui la chiave deve essere inclusa o meno e il valore della chiave. Quindi, seleziona il pulsante Aggiungi tag.

   I tag delle risorse protette vengono valutati controllandoli sul punto di ripristino più recente all'interno del vault di backup contenente la risorsa protetta.

3. Parametri di ripristino: alcune risorse richiedono la specifica dei parametri in preparazione a un processo di ripristino. Nella maggior parte dei casi, AWS Backup dedurrà i valori in base al backup archiviato.

   Si consiglia di mantenere questi parametri, tuttavia è possibile modificare i valori scegliendo una selezione diversa dal menu a discesa. La modifica dei valori può essere ottimale, ad esempio, per la sostituzione delle chiavi di crittografia, le impostazioni di Amazon FSx in cui i dati non possono essere dedotti e la creazione di sottoreti.

   Ad esempio, se un database RDS è uno dei tipi di risorsa assegnati al piano di test di ripristino, i parametri come zona di disponibilità, nome del database, classe di istanza del database e gruppo di sicurezza VPC vengono visualizzati con i valori dedotti che è possibile modificare, se applicabile.

AWS CLI

Il comando della CLI `CreateRestoreTestingPlan` viene utilizzato per creare un piano di test di ripristino.

Il piano di test deve contenere:

- `RestoreTestingPlan`, che deve includere un `RestoreTestingPlanName` univoco
- L'espressione cron `ScheduleExpression`
- `RecoveryPointSelection`

Sebbene chiamato in modo simile, NON è lo stesso `RestoreTestingSelection` di.

`RecoveryPointSelection`ha cinque parametri (tre obbligatori e due opzionali). I valori specificati determinano quale punto di ripristino è incluso nel test di ripristino. È necessario indicare con `Algorithm` se si desidera utilizzare il punto di ripristino più recente `SelectionWindowDays` o se si desidera un punto di ripristino casuale e indicare attraverso `IncludeVaults` quali archivi è possibile scegliere i punti di ripristino.

Una selezione può includere uno o più ARN di risorse protette oppure una o più condizioni, ma non entrambi.

Puoi includere anche:

- `ScheduleExpressionTimezone`
- `Tags`
- `CreatorRequestId`
- `StartWindowHours`

Utilizza il comando della CLI `create-restore-testing-plan`.

Una volta creato correttamente il piano, è necessario assegnargli le risorse utilizzando `create-restore-testing-selection`.

Consiste in `RestoreTestingSelectionName`, `ProtectedResourceType` e uno dei seguenti parametri:

- `ProtectedResourceArns`

- `ProtectedResourceConditions`

Ogni tipo di risorsa protetta può avere un solo valore. Una selezione di test di ripristino può includere un valore jolly ("*") per `ProtectedResourceArns` insieme a `ProtectedResourceConditions`. In alternativa, puoi includere fino a 30 ARN di risorse protette specifiche in `ProtectedResourceArns`.

Definizione del punto di ripristino

Ogni volta che viene eseguito un piano di test (in base alla frequenza e all'ora di inizio specificate), il test di ripristino ripristina un punto di ripristino idoneo per ogni risorsa protetta selezionata. Se nessun punto di ripristino per una risorsa soddisfa i criteri di selezione del punto di ripristino, tale risorsa non verrà inclusa nel test.

Un punto di ripristino per una risorsa protetta inclusa in una selezione di test è idoneo se soddisfa i criteri per il periodo di tempo specificato e include i vault nel piano di test di ripristino.

Una risorsa protetta viene selezionata se la selezione per il test delle risorse include il tipo di risorsa e se una delle seguenti condizioni è vera:

- L'ARN della risorsa è specificato in tale selezione; oppure
- Le condizioni dei tag su quella selezione corrispondono ai tag sull'ultimo punto di ripristino per la risorsa

Aggiornamento di un piano di test di ripristino

Puoi aggiornare parti del piano di test di ripristino e le relative selezioni delle risorse tramite la console o la AWS CLI.

Console

Aggiornamento dei piani di test di ripristino e delle selezioni mediante la console

Quando visualizzi la pagina dei dettagli del piano di test di ripristino nella console, puoi modificare (aggiornare) molte impostazioni del piano. Per farlo:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel pannello di navigazione a sinistra, individua e seleziona Test di ripristino.
3. Seleziona il pulsante Modifica.
4. Modifica la frequenza, l'ora di avvio e l'ora entro la quale deve iniziare il test, dopo l'ora di avvio scelta.
5. Salvare le modifiche.

AWS CLI

Aggiorna i piani e le selezioni dei test di ripristino tramite AWS CLI

Richiede UpdateRestoreTestingPlane UpdateRestoreTestingSelectionpuò essere utilizzato per inviare aggiornamenti parziali a un piano o a una selezione specificati. I nomi non possono essere modificati, ma è possibile aggiornare altri parametri. Includi solo i parametri che desideri modificare in ogni richiesta.

Prima di inviare una richiesta di aggiornamento, utilizza GetRestoreTestingPlane GetRestoreTestingSelectiondetermina se RestoreTestingSelection contiene ARN specifici o se utilizza i caratteri jolly e le condizioni.

Se la selezione del test di ripristino contiene ARN specifici (anziché il carattere jolly) e desideri modificarli in un carattere jolly con condizioni, la richiesta di aggiornamento deve includere sia il carattere jolly per l'ARN sia le condizioni. Una selezione può includere ARN di risorse protette o utilizzare il carattere jolly con condizioni, ma non entrambi.

- `get-restore-testing-plan`
- `get-restore-testing-selection`
- `update-restore-testing-plan`
- `update-restore-testing-selection`

Visualizzazione dei piani di test di ripristino esistenti

Console

Visualizzazione dei dettagli su un piano di test di ripristino esistente e sulle risorse assegnate nella console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Seleziona Test di ripristino dal pannello di navigazione a sinistra. Lo schermo mostra i piani di test di ripristino. I piani vengono visualizzati per impostazione predefinita in base all'ultimo runtime.
3. Seleziona il collegamento di un piano per visualizzarne i dettagli, tra cui un riepilogo, il nome, la frequenza, l'ora di avvio e il valore di avvio entro.

Puoi anche visualizzare le risorse protette del piano, i processi di test di ripristino degli ultimi 30 giorni inclusi nel piano e tutti i tag che puoi creare per questo piano di test.

AWS CLI

Recupero dei dettagli su un piano di test di ripristino esistente e sulla selezione dei test mediante la riga di comando

- `list-restore-testing-plan`
- `list-restore-testing-selections`
- `get-restore-testing-plan`
- `get-restore-testing-selection`

Visualizzazione dei processi di test di ripristino

Console

Visualizzazione dei processi di test di ripristino esistenti nella console

I processi di test di ripristino sono inclusi nella pagina dei processi di ripristino.

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Vai alla pagina Processi.

   In alternativa, puoi selezionare Test di ripristino, quindi scegliere un piano di test di ripristino per visualizzarne i dettagli e i processi associati.
3. Seleziona la scheda Processi di ripristino.

   In questa pagina puoi vedere lo stato, l'ora di ripristino, il tipo di ripristino, l'ID della risorsa, il tipo di risorsa, il piano di test di ripristino a cui appartiene il processo, l'ora di creazione e l'ID del punto di ripristino del processo di ripristino.

   I processi inclusi in un piano di test di ripristino hanno il tipo di ripristino Test.

I processi di test di ripristino hanno diverse categorie di stato:

- Quando uno stato richiede attenzione è sottolineato, passa il mouse sullo stato per visualizzare ulteriori dettagli, se disponibili.

- Se il test è stato avviato, verrà visualizzato uno Ripristina la convalida dei test stato di convalida (non disponibile nella console).
- Lo stato di eliminazione indica lo stato dei dati generati da un test di ripristino. Esistono tre stati di eliminazione possibili: Riuscito, Eliminazione in corso e Non riuscito.

  Se l'eliminazione di un processo di test di ripristino non riesce, è necessario rimuovere la risorsa manualmente perché il flusso di test di ripristino non è in grado di farlo automaticamente. Spesso, un'eliminazione non riesce se il tag `awsbackup-restore-test` viene rimosso dalla risorsa.

AWS CLI

Visualizzazione dei processi di test di ripristino esistenti dalla riga di comando

- `list-restore-jobs-by-protected-resource`

Eliminazione di un piano di test di ripristino

Console

Eliminazione del piano di test di ripristino nella console

1. Vai a Visualizzazione dei piani di test di ripristino esistenti per vedere gli attuali piani di test di ripristino.
2. Nella pagina dei dettagli del piano di test di ripristino, elimina un piano selezionando Elimina.
3. Dopo aver selezionato Elimina, viene visualizzata una finestra popup per confermare che desideri eliminare il piano. In questa finestra, il nome del piano di test di ripristino specifico è visualizzato in grassetto. Per procedere, digita il nome del piano di test esatto con distinzione tra maiuscole e minuscole, inclusi eventuali caratteri di sottolineatura, trattini e punti.

   Se l'opzione Elimina il piano di test di ripristino non è selezionabile, inserisci nuovamente il nome finché non corrisponde al nome visualizzato. Una volta ottenuta la corrispondenza esatta, l'opzione per eliminare il piano di test di ripristino diventa selezionabile.

AWS CLI

Eliminazione del piano di test di ripristino mediante la riga di comando

Il comando CLI DeleteRestoreTestingSelectionpuò essere utilizzato per eliminare una selezione di test di ripristino. Includi nella richiesta `RestoreTestingPlanName` e `RestoreTestingSelectionName`.

Tutte le selezioni di test associate a un piano di test devono essere eliminate prima di eliminare il piano di test. Una volta eliminate tutte le selezioni di test, puoi utilizzare la richiesta API DeleteRestoreTestingPlanper eliminare un piano di test di ripristino. È necessario includere `RestoreTestingPlanName`.

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

Audit del test di ripristino

Ripristina le integrazioni di test con AWS Backup Audit manager per aiutarti a valutare se una risorsa ripristinata è stata completata entro il tempo di ripristino previsto.

Per ulteriori informazioni, consulta il controllo Tempo di ripristino necessario per le risorse in Controlli e correzione di AWS Backup Audit Manager.

Quote e parametri del test di ripristino

- 100 piani di test di ripristino
- È possibile aggiungere 50 tag a ciascun piano di test di ripristino
- 30 selezioni per piano
- 30 ARN di risorse protette per selezione
- 30 condizioni di risorse protette per selezione (incluse `StringEquals` e `StringNotEquals`)
- 30 selettori di vault per selezione
- Numero massimo di giorni della finestra di selezione: 365 giorni
- Ore della finestra di avvio: minimo 1 ora; massimo 168 ore (7 giorni)
- Lunghezza massima del nome del piano: 50 caratteri
- Lunghezza massima del nome della selezione: 50 caratteri

Ulteriori informazioni sui limiti sono disponibili in AWS Backup quote.

Ripristina la risoluzione dei problemi relativi ai test

Se avete processi di ripristino di test con uno stato di ripristino pari a `Failed`, i seguenti motivi possono aiutarvi a determinarne la causa e a porvi rimedio.

I messaggi di errore possono essere visualizzati nella AWS Backup console nella pagina dei dettagli dello stato del lavoro o utilizzando i comandi `list-restore-jobs-by-protected-resource` CLI o. `list-restore-jobs`

1. Errore: *`No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.`*

   Soluzione 1: aggiorna la selezione del test di ripristino e sostituisci il parametro. `SubnetId` La AWS Backup console visualizza questo parametro come «Subnet».

   Soluzione 2: ricreare il VPC predefinito.

   Tipi di risorse interessati: Amazon EC2

2. Errore: *`No subnets found for the default VPC [vpc]. Please specify a subnet.`*

   Soluzione 1: aggiorna la selezione dei test di ripristino e sostituisci il parametro di `SubnetId` ripristino. La AWS Backup console visualizza questo parametro come «Subnet».

   Soluzione 2: creare una sottorete predefinita nel VPC predefinito.

   Tipi di risorse interessati: Amazon EC2

3. Errore: *`No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.`*

   Soluzione 1: aggiorna la selezione dei test di ripristino e sostituisci il parametro di `DBSubnetGroupName` ripristino. La AWS Backup console visualizza questo parametro come gruppo di sottorete.

   Soluzione 2: creare una sottorete predefinita nel VPC predefinito.

   Tipi di risorse interessati: Amazon Aurora, Amazon DocumentDB, Amazon RDS, Neptune

4. ***IAM Role cannot be assumed by AWS Backup***Errore:.

   Soluzione: il ruolo di ripristino deve essere assunto da AWS Backup. Aggiorna la policy di fiducia del ruolo in IAM per consentirne l'assunzione `"backup.amazonaws.com"` o aggiorna la selezione dei test di ripristino in modo da utilizzare un ruolo che sia assumibile da. AWS Backup

   Tipi di risorse interessati: tutti

5. Errore: *`Access denied to KMS key.`* o *`The specified AWS KMS key`* ARN *`does not exist, is not enabled or you do not have permissions to access it.`*

   Soluzione: verificare quanto segue:

   a. Il ruolo di ripristino ha accesso alla AWS KMS chiave utilizzata per crittografare i backup e, se applicabile, alla chiave KMS utilizzata per crittografare la risorsa ripristinata.

   b. Le politiche delle risorse sulle chiavi KMS di cui sopra consentono al ruolo di ripristino di accedervi.

   Se le condizioni di cui sopra non sono ancora soddisfatte, configura il ruolo di ripristino e le politiche delle risorse per un accesso appropriato. Quindi, esegui nuovamente il processo di test di ripristino.

   Tipi di risorse interessati: tutti

6. Errori: *`User ARN is not authorized to perform action on resource because no identity based policy allows the action.`* o*`Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx`*.

   Soluzione: il ruolo di ripristino non dispone di autorizzazioni adeguate. Aggiorna le autorizzazioni in IAM per il ruolo di ripristino.

   Tipi di risorse interessati: tutti

7. Errori: *`User ARN is not authorized to perform action on resource because no resource-based policy allows the action.`* o *`User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.`*

Soluzione: il ruolo di ripristino non dispone di un accesso adeguato alla risorsa specificata nel messaggio. Aggiorna la politica delle risorse sulla risorsa menzionata.

Tipi di risorse interessati: tutti

Metadati dedotti del test di ripristino

Il ripristino di un punto di ripristino richiede il ripristino dei metadati. Per eseguire il test di ripristino, AWS Backup deduce automaticamente i metadati che possono eseguire un ripristino corretto. Il comando `get-restore-testing-inferred-metadata` può essere utilizzato per visualizzare in anteprima ciò che AWS Backup dedurrà. Il comando `get-restore-job-metadata` restituisce l'insieme di metadati dedotto da. AWS Backup Tieni presente che per alcuni tipi di risorse (Amazon FSx), non AWS Backup è in grado di dedurre un set completo di metadati.

I metadati di ripristino dedotti vengono determinati durante il processo di test di ripristino. È possibile sovrascrivere determinate chiavi di ripristino dei metadati includendo il parametro `RestoreMetadataOverrides` nel corpo di `RestoreTestingSelection`. Alcune modifiche ai metadati non sono disponibili nella console. AWS Backup

Ogni risorsa supportata include chiavi e valori di metadati di ripristino dedotti e chiavi di metadati di ripristino sovrascrivibili. Si devono includere solo le coppie chiave-valore `RestoreMetadataOverrides` o le coppie chiave-valore annidate contrassegnate come *`necessario per il corretto ripristino`*, le altre sono facoltative. I valori delle chiavi non fanno distinzione tra maiuscole e minuscole.

> **Important**
>
> AWS Backup può dedurre che una risorsa debba essere ripristinata all'impostazione predefinita, ad esempio un'istanza Amazon EC2 o un cluster Amazon RDS ripristinati sul VPC predefinito. Tuttavia, se l'impostazione predefinita non è presente, ad esempio il VPC o la sottorete predefiniti sono stati eliminati e non è stato inserito alcun override dei metadati, il ripristino non avrà esito positivo.

Tipo di risorsa	Chiavi e valori dei metadati di ripristino dedotti	Metadati sovrascrivibili

DynamoDB	`deletionProtection` , dove il valore è impostato su `false`
	
	`encryptionType` è impostato su `Default`.
	
	`targetTableName` , dove il valore è impostato su un valore casuale che inizia con `awsbackup-restore-test-`
		`encryptionType`
		
		`kmsMasterKeyArn`

Amazon EBS	`availabilityZone` , il cui valore è impostato su una zona di disponibilità casuale
	
	`encrypted` , il cui valore è impostato su `true`
		`availabilityZone`
		
		`kmsKeyId`

Amazon EC2	Il valore `disableApiTermination` è impostato su `false`
	
	Il valore `instanceType` è impostato su instanceType del punto di ripristino da ripristinare
	
	Il valore `requiredImdsV2` è impostato su `true`
		`iamInstanceProfileName` il valore può essere nullo o `UseBackedUpValue`
		
		`instanceType`
		
		`requireImdsV2`
		
		`securityGroupIds`
		
		`subnetId`

Amazon EFS	Il valore `encrypted` è impostato su `true`	`kmsKeyId`

Tipo di risorsa	Chiavi e valori dei metadati di ripristino dedotti	Metadati sovrascrivibili
	Il valore `file-system-id` è impostato sull'ID file system del punto di ripristino da ripristinare `kmsKeyId value` è impostato su `alias/aws/elasticfilesystem` . Il valore `newFileSystem` è impostato su `true` Il valore `performanceMode` è impostato su `generalPurpose`	

Amazon FSx per Lustre	`lustreConfiguration` include chiavi annidate. Una chiave annidata è `automaticBackupRetentionDays` , il cui valore è impostato su `0`	`kmsKeyId`
		
		`lustreConfiguration` include la chiave annidata `logConfiguration`
		
		`securityGroupIds`
		
		`subnetIds` , *`necessario per il corretto ripristino`*

Tipo di risorsa	Chiavi e valori dei metadati di ripristino dedotti	Metadati sovrascrivibili
Amazon FSx per ONTAP NetApp	`name` è impostato su un valore casuale che inizia con `awsbackup_restore_test_` `ontapConfiguration` include chiavi annidate, tra cui: • `junctionPath` dove `/name` è il nome del volume da ripristinare • `sizeInMegabytes` , il cui valore è impostato sulla dimensione in megabyte del punto di ripristino da ripristinare • `snapshotPolicy` dove il valore è impostato su `none`	`ontapConfiguration` include specifiche chiavi annidate sovrascrivibili, tra cui: • `junctionPath` • `ontapVolumeType` • `securityStyle` • `sizeInMegabytes` • `storageEfficiencyEnabled` • `storageVirtualMachineId` , *necessario per il corretto ripristino* • `tieringPolicy`

Tipo di risorsa	Chiavi e valori dei metadati di ripristino dedotti	Metadati sovrascrivibili

Amazon FSx per OpenZFS	`openZfzConfiguration` , che include chiavi annidate, tra cui:
	• `automaticBackupRetentionDays` con il valore impostato su `0`
	• `deploymentType` con il valore impostato sul tipo di implementazione del punto di ripristino da ripristinare
	• `throughputCapacity` , il cui valore è basato su `deploymentType` . Se `deploymentType` è `SINGLE_AZ_1` , il valore è impostato su `64`; se `deploymentType` è `SINGLE_AZ_2 or MULTI_AZ_1` , il valore è impostato su `160`
		`kmsKeyId`
		`openZfsConfiguration` include specifiche chiavi annidate sovrascrivibili, tra cui:
		• `deploymentType`
		• `throughputCapacity`
		• `diskiopsConfiguration`
		`securityGroupIds`
		`subnetIds`

Tipo di risorsa	Chiavi e valori dei metadati di ripristino dedotti	Metadati sovrascrivibili

Amazon FSx per Windows File Server	`windowsConfiguration` , che include chiavi annidate tra cui:
	• `automaticBackupRetentionDays` con il valore impostato su `0`
	• `deploymentType` con il valore impostato sul tipo di implementazione del punto di ripristino da ripristinare
	• `throughputCapacity` con il valore impostato su 8
		`kmsKeyId`
		`securityGroupIds`
		`subnetIds` *necessario per il corretto ripristino*
		`windowsConfiguration` , con chiavi annidate sovrascrivibili specifiche
		• `throughputCapacity`
		• `activeDirectoryId` *necessario per il corretto ripristino se non `selfManagedActiveDirectoryConfiguration` è incluso*
		• `selfManagedActiveDirectoryConfiguration` *necessario per il corretto ripristino se non `activeDirectoryId` è incluso*
		• `preferredSubnetId`

Tipo di risorsa	Chiavi e valori dei metadati di ripristino dedotti	Metadati sovrascrivibili

Cluster Amazon RDS, Aurora, Amazon DocumentDB, Amazon Neptune	`availabilityZones` con il valore impostato su un elenco di massimo tre zone di disponibilità casuali
	
	`dbClusterIdentifier` con un valore casuale che inizia con `awsbackup-restore-test`
	
	`engine` con il valore impostato sul motore del punto di ripristino da ripristinare
		`availabilityZones`
		
		`databaseName`
		
		`dbClusterParameterGroupName`
		
		`dbSubnetGroupName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`engine`
		
		`engineMode`
		
		`engineVersion`
		
		`kmskeyId`
		
		`port`
		
		`optionGroupName`
		
		`scalingConfiguration`
		
		`vpcSecurityGroupIds`

Tipo di risorsa	Chiavi e valori dei metadati di ripristino dedotti	Metadati sovrascrivibili

Istanze Amazon RDS	`dbInstanceIdentifier` con un valore casuale che inizia con `awsbackup-restore-test-`
	
	`deletionProtection` con il valore impostato su `false`
	
	`multiAz` con il valore impostato su `false`
	
	`publiclyAccessible` con il valore impostato su false
		`allocatedStorage`
		
		`availabilityZones`
		
		`dbInstanceClass`
		
		`dbName`
		
		`dbParameterGroupName`
		
		`dbSubnetGroupName`
		
		`domain`
		
		`domainIamRoleName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`iops`
		
		`licensemodel`
		
		`multiAz`
		
		`optionGroupName`
		
		`port`
		
		`processorFeatures`
		
		`publiclyAccessible`
		
		`storageType`
		
		`vpcSecurityGroupIds`

Tipo di risorsa	Chiavi e valori dei metadati di ripristino dedotti	Metadati sovrascrivibili

Amazon Simple Storage Service (Amazon S3)	`destinationBucketName` con un valore casuale che inizia con `awsbackup-restore-test-`
	
	`encrypted` con il valore impostato su `true`
	
	`encryptionType` con il valore impostato su `SSE-S3`
	
	`newBucket` con il valore impostato su `true`
		`encryptionType`
		
		`kmsKey`

Ripristina la convalida dei test

È possibile creare una convalida basata sugli eventi che viene eseguita al termine di un processo di test di ripristino.

Innanzitutto, crea un flusso di lavoro di convalida con qualsiasi destinazione supportata da Amazon EventBridge, ad esempio AWS Lambda. In secondo luogo, aggiungi una EventBridge regola che attesti che il processo di ripristino raggiunga lo stato. `COMPLETED` In terzo luogo, crea un piano di test di ripristino (o lascia che uno esistente venga eseguito come pianificato). Infine, una volta terminato il test di ripristino, monitora i registri del flusso di lavoro di convalida per assicurarti che funzioni come previsto (una volta eseguita la convalida, nella console verrà visualizzato lo stato di convalida).AWS Backup

1. Imposta il flusso di lavoro di convalida

   È possibile configurare un flusso di lavoro di convalida utilizzando Lambda o qualsiasi altro target supportato da. EventBridge Ad esempio, se stai convalidando un test di ripristino contenente un'istanza Amazon EC2, puoi includere codice che esegue il ping di un endpoint healthcheck.

   Puoi utilizzare i dettagli dell'evento per determinare quali risorse convalidare.

Puoi utilizzare un layer Lambda personalizzato per utilizzare l'SDK più recente (poiché non `PutRestoreValidationResult` è ancora disponibile tramite Lambda SDK).

Ecco un esempio:

```
import { Backup } from "@aws-sdk/client-backup";

export const handler = async (event) => {
  console.log("Handling event: ", event);

  const restoreTestingPlanArn = event.detail.restoreTestingPlanArn;
  const resourceType = event.detail.resourceType;
  const createdResourceArn = event.detail.createdResourceArn;

  // TODO: Validate the resource

  const backup = new Backup();
  const response = await backup.putRestoreValidationResult({
    RestoreJobId: event.detail.restoreJobId,
    ValidationStatus: "SUCCESSFUL", // TODO
    ValidationStatusMessage: "" // TODO
  });

  console.log("PutRestoreValidationResult: ", response);
  console.log("Finished");
};
```

2. Aggiungi una EventBridge regola

   Crea una EventBridge regola che tenga conto dell'`COMPLETED`evento restore job.

   Facoltativamente, puoi filtrare gli eventi per tipo di risorsa o ripristinare l'ARN del piano di test. Imposta l'obiettivo di questa regola per richiamare il flusso di lavoro di convalida definito nel passaggio 1. Ecco un esempio:

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
    "Restore Job State Change"
  ],
```

```
  "detail":{
    "resourceType":[
      "..."
    ],
    "restoreTestingPlanArn":[
      "..."
    ],
    "status":[
      "COMPLETED"
    ]
  }
}
```

3. Lascia che il piano di test di ripristino venga eseguito e completato

   Il piano di test di ripristino verrà eseguito in base alla pianificazione configurata.

   Vedi Creare un piano di test di ripristino se non ne hai ancora uno o Aggiornare un piano di test di ripristino se desideri modificare le impostazioni.

4. Monitora i risultati

   Una volta che un piano di test di ripristino è stato eseguito come previsto, puoi controllare i registri del flusso di lavoro di convalida per assicurarti che abbia funzionato correttamente.

   Puoi chiamare l'API `PutRestoreValidationResult` per pubblicare i risultati, che saranno quindi visualizzabili nella AWS Backup console e tramite chiamate AWS Backup API che descrivono ed elencano i processi di ripristino, come o. `DescribeRestoreJob` `ListRestoreJob`

   Una volta impostato, lo stato di convalida non può essere modificato.

Visualizzazione di un elenco di backup

È possibile visualizzare un elenco dei backup utilizzando la AWS Backup console o a livello di programmazione.

Argomenti

- Elenco dei backup di una risorsa protetta nella console
- Elenco dei backup di un vault di backup nella console
- Elenco di backup a livello di programma

Elenco dei backup di una risorsa protetta nella console

Segui queste fasi per visualizzare un elenco di backup di una risorsa specifica nella console di AWS Backup .

1. Accedere a e aprire AWS Management Console la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione selezionare Protected resources (Risorse protette).
3. Scegliere una risorsa protetta nell'elenco per visualizzare l'elenco dei backup. Solo le risorse di cui è stato eseguito il backup AWS Backup sono elencate in Risorse protette.

Puoi visualizzare i backup per la risorsa. Da questa visualizzazione è possibile anche scegliere un backup e ripristinarlo.

Elenco dei backup di un vault di backup nella console

Segui queste fasi per visualizzare un elenco dei backup organizzati in un vault.

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Nella sezione Backup visualizzare l'elenco di tutti i backup organizzati in questo vault. In questa visualizzazione, puoi ordinare i backup in base a qualsiasi intestazione di colonna (incluso lo stato), nonché selezionare un backup per ripristinarlo, modificarlo o eliminarlo.

Elenco di backup a livello di programma

Puoi elencare i backup a livello di programma utilizzando le operazioni API `ListRecoveryPoint`:

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

Ad esempio, il comando seguente AWS Command Line Interface (AWS CLI) elenca tutti i backup con lo `EXPIRED` stato:

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
```

```
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

È possibile utilizzare AWS Backup Audit Manager per verificare la conformità delle AWS Backup politiche rispetto ai controlli definiti dall'utente. Un controllo è una procedura progettata per verificare la conformità di un requisito di backup, come la frequenza di backup o il periodo di conservazione del backup.

AWS Backup Audit Manager ti aiuta a rispondere a domande come:

- "Sto eseguendo il backup di tutte le risorse?"
- "Tutti i miei backup sono crittografati?"
- "I miei backup vengono eseguiti ogni giorno?"

È possibile utilizzare AWS Backup Audit Manager per trovare attività e risorse di backup che non sono ancora conformi ai controlli definiti. Tieni presente che, quando i controlli valutano la conformità delle risorse, verranno incluse solo le risorse attive. Ad esempio, verrà valutata un'istanza Amazon EC2 in uno stato di esecuzione. Un'istanza EC2 in uno stato di arresto non verrà inclusa nella valutazione di conformità.

Puoi inoltre utilizzarlo per generare automaticamente un percorso di audit di report giornalieri e on demand per i tuoi scopi di governance dei backup.

I passaggi seguenti forniscono una panoramica su come utilizzare AWS Backup Audit Manager. Per le procedure dettagliate, scegli uno degli argomenti alla fine di questa pagina.

1. Crea framework contenenti uno o più modelli di controllo della governance. Le domande precedenti sono esempi di tre modelli di controllo della governance. Puoi personalizzare i parametri di alcuni modelli di controllo della governance. Ad esempio, puoi personalizzare l'ultimo controllo per chiedere: “I miei backup vengono eseguiti ogni settimana?” anziché ogni giorno.
2. Visualizza il framework per vedere quante risorse sono conformi (o non conformi) ai controlli definiti in tale framework.
3. Crea report sullo stato di backup e conformità. Archivia questi report come prova dimostrabile delle pratiche di conformità o per identificare singole attività e risorse di backup che non sono ancora conformi.

   AWS Backup Audit Manager genera automaticamente un nuovo report ogni 24 ore e lo pubblica su Amazon S3. Puoi anche generare report on demand.

> **Note**
>
> Prima di creare il primo framework correlato alla conformità, è necessario attivare il monitoraggio delle risorse. In questo modo puoi AWS Config tenere traccia delle tue AWS Backup risorse. Per la documentazione tecnica su come gestire il monitoraggio delle risorse, consulta Configurazione AWS Config con la console nella Guida per gli AWS Config sviluppatori.
> Quando attivi il monitoraggio delle risorse, vengono applicati costi. Per informazioni sul monitoraggio delle risorse, sui prezzi e sulla fatturazione per AWS Backup Audit Manager, consulta Misurazione, costi e fatturazione.

Argomenti

Utilizzo dei framework di audit

Un framework è una raccolta di controlli che consentono di valutare le best practice di backup. Puoi utilizzare controlli personalizzabili predefiniti per definire le policy e valutare se le best practice di backup sono conformi alle policy. Puoi anche configurare report giornalieri automatici per ottenere informazioni dettagliate sullo stato di conformità dei framework.

Ogni framework si applica a un singolo account e. Regione AWSÈ possibile implementare un massimo di 15 framework per account per regione. Non puoi distribuire framework duplicati (framework contenenti gli stessi controlli e parametri).

Esistono due diversi tipi di framework:

- Il framework AWS Backup (consigliato): utilizza il framework AWS Backup per distribuire tutti i controlli disponibili per monitorare l'attività di backup, la copertura e le risorse in base alle best practice consigliate.

- Un framework personalizzato definito dall'utente: utilizza un framework personalizzato per scegliere uno o più controlli specifici e personalizzare i parametri di controllo.

Argomenti

Scelta dei controlli

La tabella seguente elenca i controlli AWS Backup Audit Manager, i relativi parametri personalizzabili e i tipi di risorse di AWS Config registrazione. Ogni controllo richiede il tipo di risorsa di registrazione `AWS Config: resource compliance` poiché questo tipo registra lo stato di conformità dell'utente.

Controlli disponibili

Nome del controllo	Descrizione del controllo	Parametri personalizzabili	AWS Config tipo di risorsa di registrazione
Le risorse di backup sono protette da un piano di backup	Valuta se le risorse sono protette da un piano di backup.	Nessuno	`AWS Backup: backup selection`
Il piano di backup dispone di una frequenza minima e conservazione minima	Valuta se la frequenza di backup è di almeno [1 giorno] e il periodo di conservazione è di almeno [35 giorni].	Frequenza di backup; periodo di conservazione	`AWS Backup: backup plans`

Nome del controllo	Descrizione del controllo	Parametri personalizzabili	AWS Config tipo di risorsa di registrazione
I vault impediscono l'eliminazione manuale dei punti di ripristino	Valuta se gli archivi di backup non consentono l'eliminazione manuale dei punti di ripristino ad eccezione di determinati ruoli AWS Identity and Access Management (IAM). Per impostazione predefinita, non esistono eccezioni ai ruoli IAM. Inoltre, non ci sono eccezioni ai ruoli IAM quando si implementa questo controllo con il framework. AWS Backup	Fino a 5 ruoli IAM che consentono l'eliminazione manuale dei punti di ripristino	`AWS Backup: backup vaults`
I punti di ripristino sono crittografati	Valuta se i punti di ripristino sono crittografati.	Nessuno	`AWS Backup: recovery points`
Conservazione minima stabilita per punto di ripristino	Valuta se il periodo di conservazione del punto di ripristino è di almeno [35 giorni].	Periodo di conservazione dei punti di ripristino	`AWS Backup: recovery points`

Nome del controllo	Descrizione del controllo	Parametri personalizzabili	AWS Config tipo di risorsa di registrazione
Copia di backup tra regioni pianificata	Valuta se una risorsa è configurata per creare copie dei relativi backup su un'altra Regione AWS.	Regione AWS	`AWS Backup: backup selection`
Copia di backup tra account pianificata	Valuta se per una risorsa è configurata una copia di backup tra account.	AWS ID dell'account	`AWS Backup: backup selection`
I backup sono protetti da AWS Backup Vault Lock	Valuta se una risorsa è configurata per avere backup in un vault di backup bloccato.	Numero minimo di giorni di conservazione; numero massimo di giorni di conservazione	`AWS Backup: backup selection`
È stato creato l'ultimo punto di ripristino	Valuta se un punto di ripristino è stato creato entro l'intervallo di tempo specificato.	Valore in ore [da `1` a `744`] o giorni [da `1` a `31`].	`AWS Backup recovery points`
Tempo di ripristino necessario per le risorse	Valuta se il processo di test di ripristino è stato completato entro il tempo di ripristino previsto.	Valore in minuti.	Nessuno

Per informazioni dettagliate su questi controlli, consulta Controlli e correzioni.

Per un elenco delle risorse AWS Backup supportate che non supportano tutti i controlli, consulta la sezione AWS Backup Audit Manager della Disponibilità delle funzionalità per risorsa tabella.

> **Note**
>
> Se non desideri utilizzare nessuno dei controlli precedenti, puoi comunque utilizzare AWS Backup Audit Manager per creare report giornalieri sui processi di backup, copia e ripristino. Consulta Utilizzo di report di audit.

Attivazione del monitoraggio delle risorse

Prima di creare il primo framework correlato alla conformità, è necessario attivare il monitoraggio delle risorse. In questo modo puoi AWS Config tenere traccia delle tue AWS Backup risorse. Per la documentazione tecnica su come gestire il monitoraggio delle risorse, consulta Configurazione AWS Config con la console nella Guida per gli AWS Config sviluppatori.

Quando attivi il monitoraggio delle risorse, vengono applicati costi. Per informazioni sul monitoraggio delle risorse, sui prezzi e sulla fatturazione per AWS Backup Audit Manager, consulta Misurazione, costi e fatturazione.

Argomenti

- Attivazione del monitoraggio delle risorse mediante la console
- Attivazione del monitoraggio delle risorse mediante la AWS Command Line Interface (AWS CLI)
- Attivazione del monitoraggio delle risorse mediante un modello AWS CloudFormation

Attivazione del monitoraggio delle risorse mediante la console

Per attivare il monitoraggio delle risorse mediante la console:

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di spostamento a sinistra, in Audit Manager, scegli Framework.
3. Attiva il monitoraggio delle risorse scegliendo Gestisci il monitoraggio delle risorse.
4. Scegli Vai alle AWS Config impostazioni.
5. Scegli Abilita o disabilita la registrazione.

6. Scegli di abilitare la registrazione per tutti i seguenti tipi di risorse o di abilitare la registrazione per alcuni tipi di risorse. Fai riferimento a Controlli e correzione di AWS Backup Audit Manager per i tipi di risorse richiesti per i controlli.

   - `AWS Backup: backup plans`
   - `AWS Backup: backup vaults`
   - `AWS Backup: recovery points`
   - `AWS Backup: backup selection`

   > **Note**
   >
   > AWS Backup Audit Manager richiede `AWS Config: resource compliance` ogni controllo.

7. Scegli Chiudi.
8. Attendi che il banner blu contenente il testo Attivazione del tracciamento delle risorse passi al banner verde con il testo Monitoraggio delle risorse è attivo.

È possibile verificare se è stato attivato il monitoraggio delle risorse e, in tal caso, quali tipi di risorse si stanno registrando, in due punti della AWS Backup console. Nel riquadro di navigazione a sinistra:

- Scegli Framework, quindi scegli il testo sotto lo stato del registratore AWS Config .
- Scegli Impostazioni, quindi scegli il testo sotto lo stato del registratore AWS Config .

Attivazione del monitoraggio delle risorse mediante la AWS Command Line Interface (AWS CLI)

Se non hai ancora effettuato l'onboarding AWS Config, potrebbe essere più veloce effettuare l'onboarding utilizzando il. AWS CLI

Per attivare il monitoraggio delle risorse mediante la AWS CLI:

1. Digita il seguente comando per determinare se il registratore AWS Config è già abilitato.

```
$ aws configservice describe-configuration-recorders
```

a. Se l'elenco `ConfigurationRecorders` è vuoto come il seguente:

```
{
  "ConfigurationRecorders": []
}
```

Il registratore non è abilitato. Continua con il passaggio 2 per creare il registratore.

b. Se hai già abilitato la registrazione per tutte le risorse, l'aspetto dell'output `ConfigurationRecorders` sarà simile al seguente:

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
}
```

Poiché hai abilitato tutte le risorse, hai già attivato il tracciamento delle risorse. Non è necessario completare il resto di questa procedura per utilizzare AWS Backup Audit Manager.

c. Se `ConfigurationRecorders` non è vuoto, ma non hai abilitato la registrazione per tutte le risorse, aggiungi risorse di backup al registratore esistente mediante il comando seguente. Quindi passa alla fase 3.

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders":[
    {
      "name":"default",
```

```
      "roleARN":"arn:aws:iam::accountId:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

2. Crea un AWS Config registratore con i tipi di risorse AWS Backup Audit Manager

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default, \
roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig \
--recording-group
 resourceTypes="['AWS::Backup::BackupPlan','AWS::Backup::BackupSelection', \
'AWS::Backup::BackupVault','AWS::Backup::RecoveryPoint','AWS::Config::ResourceCompliance']"
```

3. Descrivi il tuo AWS Config registratore.

```
$ aws configservice describe-configuration-recorders
```

Verifica che disponga dei tipi di risorse AWS Backup Audit Manager confrontando l'output con il seguente output previsto.

```
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
```

```
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

4. Crea un bucket Amazon S3 come destinazione per archiviare i file di configurazione. AWS Config

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. Usa *policy.json* per concedere l' AWS Config autorizzazione ad accedere al tuo bucket. Consulta il seguente esempio *policy.json*.

```
$ aws s3api put-bucket-policy --bucket MyBucket --policy file://policy.json
```

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AWSConfigBucketPermissionsCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:GetBucketAcl",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketExistenceCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:ListBucket",
      "Resource":"arn:aws:s3:::my-bucket"
```

```
    },
    {
      "Sid":"AWSConfigBucketDelivery",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

6. Configura il tuo bucket come canale di distribuzione AWS Config

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. Abilita la registrazione AWS Config

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. Verifica che `"FrameworkStatus":"ACTIVE"` nell'ultima riga dell'account `DescribeFramework` venga generato come segue.

```
$ aws backup describe-framework --framework-name test --region us-east-1
```

```
{
  "FrameworkName":"test",
 "FrameworkArn":"arn:aws:backup:us-east-1:accountId:framework:test-
f0001b0a-0000-1111-ad3d-4444f5cc6666",
  "FrameworkDescription":"",
  "FrameworkControls":[
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"1"
        }
      ],
```

```
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredFrequencyUnit",
          "ParameterValue":"hours"
        },
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"35"
        },
        {
          "ParameterName":"requiredFrequencyValue",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
```

```
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    }
  ],
  "CreationTime":1633463605.233,
  "DeploymentStatus":"COMPLETED",
  "FrameworkStatus":"ACTIVE"
}
```

Attivazione del monitoraggio delle risorse mediante un modello AWS CloudFormation

Per un AWS CloudFormation modello che attiva il monitoraggio delle risorse, vedere Utilizzo di AWS Backup Audit Manager con AWS CloudFormation.

Creazione di framework mediante la console di AWS Backup

Dopo aver attivato il monitoraggio delle risorse, crea un framework utilizzando la procedura seguente.

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel pannello di navigazione a sinistra, scegli Framework.
3. Scegli Crea framework.
4. Per Nome, immetti un nome univoco. Il nome del framework deve essere compreso tra 1 e 256 caratteri, deve iniziare con una lettera ed essere costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).
5. (Facoltativo) Inserisci una Descrizione del framework.
6. I controlli attivi verranno visualizzati in Controlli. Per impostazione predefinita, sono elencati tutti i controlli idonei per una risorsa.

   Per modificare i controlli attivi, fai clic su Modifica i controlli.

   a. La prima casella di controllo indica se il controllo è attivato. Per disattivare un controllo, deseleziona la casella.
   b. In Scegli le risorse da valutare, puoi selezionare come scegliere le risorse: in base a tipo, tag o singola risorsa.

L'elenco dei controlli AWS Backup Audit Manager descrive le opzioni di personalizzazione per ogni controllo.

7. (Facoltativo) Assegna un tag al framework scegliendo Aggiungi nuovo tag. Puoi utilizzare i tag per cercare e filtrare i framework o monitorare i costi.
8. Scegli Crea framework.

AWS Backup Audit Manager potrebbe impiegare diversi minuti per creare il framework.

Se si verifica l'errore `AlreadyExists`, esiste già un framework con gli stessi controlli e parametri. Per creare correttamente un nuovo framework, è necessario che almeno un controllo o un parametro sia diverso dai framework esistenti.

Creazione di framework utilizzando l'API AWS Backup

La tabella seguente contiene richieste API di esempio a CreateFramework per ogni controllo, insieme a risposte API di esempio alle richieste DescribeFramework corrispondenti. Per lavorare con AWS Backup Audit Manager a livello di codice, puoi fare riferimento a questi frammenti di codice.

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
`Backup resources are protected by a backup plan`	`{"FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [ {"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes":`	`{"FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [ {"ControlName": "BACKUP_RESOURCES_`

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**

	<pre>["RDS"] // Evaluate only RDS instances
	}
	}
	],
	"IdempotencyToken": "Control1",
	"FrameworkTags": {"key1": "foo"}
	}</pre>
		<pre>PROTECTED_BY_BACKUP_PLAN",
		"ControlInputParameters":[],
		"ControlScope": {"ComplianceResourceTypes": ["RDS"]
		}
		}
		],
		"CreationTime": 1516925490,
		"DeploymentStatus": "Active",
		"FrameworkStatus": "Completed",
		"IdempotencyToken": "Control1",
		"FrameworkTags": {"key1": "foo"}
		}</pre>

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
Backup plan minimum frequency and minimum retention	{"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }],	{"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": {

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
	"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }	"Tags": {"key1": "prod"} } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
Vaults prevent manual deletion of recovery points	{"FrameworkName": "Control3", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"],	{"FrameworkName": "Control3", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:r

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**

	<pre>"Complian
	ceResourceTypes":
	["AWS::Backup::Bac
	kupVault"]
	}
	}
	],
	"IdempotencyToken":
	"Control3",
	"FrameworkTags":
	{"key1": "foo"}
	}</pre>
		<pre>ole/service-role/Q
		uickSightAction"}
		],
		"ControlScope":
		{"Complia
		nceResourceIds":["
		default"],
		"Complian
		ceResourceTypes":
		["AWS::Backup::Bac
		kupVault"]
		}
		}
		],
		"CreationTime":
		1516925490,
		"DeploymentStatus":
		"Active",
		"FrameworkStatus":
		"Completed",
		"IdempotencyToken":
		"Control3",
		"FrameworkTags":
		{"key1": "foo"}
		}</pre>

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
Minimum retention established for recovery point	{"FrameworkName": "Control4", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points. }], "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control4", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control4", "FrameworkTags":

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
		<pre> {"key1": "foo"} }</pre>

Backup recovery points are encrypted	<pre>{"FrameworkName":
	 "Control5",
	 "FrameworkDescript
	ion": "This is a test
	 framework",
	 "FrameworkControls":
	  [
	  {"ControlName":
	 "BACKUP_RECOVERY_P
	OINT_ENCRYPTED",
	  "ControlInputParam
	eters":
	  [],
	  "ControlScope":
	 {} // Default scope
	 (no scope input) is all
	 recovery points
	  }
	  ],
	 "IdempotencyToken":
	 "Control5",
	 "FrameworkTags":
	  {"key1": "foo"}
	}</pre>
		<pre>{"FrameworkName":
		 "Control5",
		"FrameworkArn":
		 "arn:aws:backup:us
		-east-1:1234567890
		12:framework/Contr
		ol7-7e7655ae-1e31-
		45cb-96a0-4f43d8c1
		9642",
		 "FrameworkDescript
		ion": "This is a test
		 framework",
		  "FrameworkControls
		":
		  [
		  {"ControlName":
		 "BACKUP_RECOVERY_P
		OINT_ENCRYPTED",
		  "ControlInputParam
		eters":
		  [],
		  "ControlScope": {}
		  }
		  ],
		 "CreationTime":
		 1516925490,
		 "DeploymentStatus":
		 "Active",
		 "FrameworkStatus":
		 "Completed",
		 "IdempotencyToken":
		 "Control5",
		 "FrameworkTags":
		  {"key1": "foo"}
		}</pre>

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
Cross-Region backup copy is scheduled	{"FrameworkName": "Control6", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control6", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
Cross-account backup copy is scheduled	{"FrameworkName": "Control7", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control7", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
Backups are protected by AWS Backup Vault Lock	{"FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
Last recovery point was created	{"FrameworkName": "Control9", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control9", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
Restore time for resources meet target	{"FrameworkName":"Control10", "FrameworkDescription":"This is a test framework", "FrameworkControls":[{ "ControlName":"RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[{ "ParameterName":"maxRestoreTime", "ParameterValue":"720" }], "ControlScope":{ "ComplianceResourceIds":[ ], "ComplianceResourceTypes":["DynamoDB" // Evaluates only DynamoDB databases] } }]"IdempotencyToken":"Control10", "FrameworkTags":{ "key1":"foo" }	{"FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control10", "FrameworkTags": {"key1": "foo"} }

Controllo	Richiesta **CreateFramework**	Risposta **DescribeFramework**
	}	

Visualizzazione dello stato di conformità del framework

Dopo che è stato creato, un framework di audit viene visualizzato nella tabella Framework. È possibile visualizzare questa tabella scegliendo Frameworks nel riquadro di navigazione a sinistra della AWS Backup console. Per visualizzare i risultati di audit per il framework, scegli il relativo nome del framework. Questo consente di accedere alla pagina dei dettagli del framework, contenente due sezioni: Riepilogo e Controlli.

Nella sezione Riepilogo vengono elencati i seguenti stati da sinistra a destra:

- Stato di conformità è lo stato di conformità complessivo del framework di audit, determinato dallo stato di conformità di ciascuno dei relativi controlli. Lo stato di conformità di ogni controllo è determinato dallo stato di conformità di ogni risorsa valutata.

  Lo stato di conformità del framework è `Compliant` solo se tutte le risorse nell'ambito delle valutazioni di controllo hanno superato tali valutazioni. Se una o più risorse non superano una valutazione di controllo, lo stato di conformità sarà `Non-Compliant`. Per informazioni su come trovare le risorse non conformi, consulta Individuazione di risorse non conformi. Per informazioni su come garantire la conformità delle risorse, consulta la sezione sulla correzione di Controlli e correzione di AWS Backup Audit Manager.
- Stato del framework si riferisce all'avere attivato il monitoraggio delle risorse per tutte le risorse. I possibili stati sono:
  - `Active` quando la registrazione è attivata per tutte le risorse valutate dal framework.
  - `Partially active` quando la registrazione è disattivata per almeno una risorsa valutata dal framework.
  - `Inactive` quando la registrazione è disattivata per tutte le risorse valutate dal framework.
  - `Unavailable`quando AWS Backup Audit Manager non è in grado di convalidare lo stato della registrazione in questo momento.

  Per correggere uno stato **`Partially active`** o **`Inactive`**

  1. Scegli Framework nel pannello di navigazione a sinistra.

2. Scegli Gestisci il monitoraggio delle risorse.
3. Segui le istruzioni nella schermata popup per abilitare la registrazione che in precedenza non era abilitata per i tipi di risorse.

Per ulteriori informazioni sui tipi di risorse che richiedono il monitoraggio delle risorse in base ai controlli inclusi nei framework, consulta il componente delle risorse di Controlli e correzione di AWS Backup Audit Manager.

- Stato dell'implementazione si riferisce allo stato di implementazione del framework. Questo stato deve essere nella maggior parte dei casi `Completed`, ma può anche essere `Create in progress`, `Update in progress`, `Delete in progress` e `Failed`.
  - Uno status di `Failed` indica che il framework non è stato distribuito correttamente. Elimina il framework, quindi ricrea il framework tramite la console AWS Backup o tramite l'API AWS Backup.
- Controlli conformi mostrano un conteggio di controlli del framework con tutte le valutazioni superate.
- Controlli non conformi mostrano un conteggio di controlli del framework con almeno una valutazione non superata.

Nella sezione Controlli vengono visualizzate le informazioni seguenti:

- Stato del controllo si riferisce allo stato di conformità di ogni controllo. Un controllo può essere `Compliant`, a indicare che tutte le risorse superano tale valutazione, `Non-compliant`, a indicare che almeno una risorsa non ha superato tale valutazione o `Insufficient data`, a indica che il controllo non ha trovato alcuna risorsa da valutare nell'ambito della valutazione.
- Ambito di valutazione potrebbe limitare ogni controllo a uno o più tipi di risorse, un ID risorsa o una chiave tag e un valore tag, in base al modo in cui il controllo è stato personalizzato durante la creazione del framework di verifica. Se tutti i campi sono vuoti (come mostrato da un trattino, "-"), il controllo valuta tutte le risorse applicabili.

Esito di risorse non conformi

AWS Backup Audit Manager consente di individuare le risorse non conformi in due modi.

- Durante la visualizzazione dello stato di conformità del framework, scegli il nome del controllo nella sezione Dettagli. In questo modo si accede alla AWS Config console, dove è possibile visualizzare un elenco delle risorse a disposizione. `Non-Compliant`
- Dopo aver creato un piano di report con il modello di conformità delle risorse che include il framework, puoi visualizzare il report per identificare tutte le risorse `Non-Compliant` su tutti i controlli.

  Inoltre, `Resource compliance report` mostra l'ultima volta che AWS Backup Audit Manager ha valutato ciascun controllo.

Aggiornamento dei framework di audit

Puoi aggiornare la descrizione, i controlli e i parametri di un framework di audit esistente.

Per aggiornare un framework esistente

1. Nel riquadro di navigazione a sinistra AWS Backup della console, scegli Frameworks.
2. Scegli il framework che desideri modificare in base al nome del framework.
3. Scegli Modifica.

Aggiornamento dei framework di audit

Per eliminare un framework esistente

1. Nel riquadro di navigazione a sinistra AWS Backup della console, scegli Frameworks.
2. Scegli il framework che desideri eliminare in base al nome del framework.
3. Scegli Elimina.
4. Digita il nome del framework e scegli Elimina framework.

Utilizzo dei report di audit

AWS Backup I report di Audit Manager sono prove generate automaticamente dell' AWS Backup attività dell'utente, ad esempio:

- Quali processi di backup sono terminati e quando
- Le risorse di cui è stato eseguito il backup

Esistono due tipi di report. Quando crei un report, scegli il tipo da creare.

Uno è il report sui processi, che mostra i processi completati nelle ultime 24 ore e tutti i processi attivi. I report sui processi non mostrano lo stato `completed with issues`. Per trovare questo stato, puoi filtrare i `Completed` lavori con uno o più messaggi di stato. AWS Backup includerà un messaggio di stato come parte dello stato di un `Completed` lavoro solo se il messaggio richiede attenzione o azione.

Il secondo è un report di conformità. I report di conformità possono monitorare i livelli di risorse o i diversi controlli in vigore.

AWS Backup Audit Manager fornisce un report giornaliero nel tuo bucket Amazon S3. Se il report è relativo alla regione e all'account correnti, puoi scegliere di riceverlo nel formato CSV o JSON. In caso contrario, il report è disponibile in formato CSV. La tempistica del rapporto giornaliero potrebbe variare nell'arco di diverse ore perché AWS Backup Audit Manager esegue la randomizzazione per mantenere le sue prestazioni. Puoi anche eseguire un report on demand in qualsiasi momento.

Tutti i titolari di un account possono creare report tra regioni; i titolari di un account di gestione e amministratore delegato possono inoltre creare report su più account.

È possibile disporre di un massimo di 20 piani di report per persona. Account AWS

> **Note**
>
> Risorse come RDS che non sono in grado di visualizzare byte di dati incrementali di un backup specifico visualizzeranno il valore `backupSizeInBytes` come 0.

Per consentire all' AWS Backup Audit Manager di creare report giornalieri o su richiesta, è necessario innanzitutto creare un piano di report da un modello di rapporto.

Argomenti

- Scelta del modello di report
- Creazione di piani di report mediante la console di AWS Backup
- Creazione di piani di report utilizzando l'API AWS Backup
- Creazione di report on demand
- Visualizzazione dei report di audit

- Aggiornamento dei piani di report
- Eliminazione di piani di report

Scelta del modello di report

Un modello di report definisce le informazioni incluse dal piano di report nel report. Quando automatizzi i report utilizzando un piano di report, AWS Backup Audit Manager ti fornisce i report per le 24 ore precedenti. AWS Backup Audit Manager crea questi report tra l'1 e le 5 del mattino UTC. Offre i seguenti modelli di report.

Modelli di report di backup

Modelli di report di backup. Questi modelli forniscono aggiornamenti quotidiani sui processi di backup, ripristino o copia. Puoi utilizzare questi report per monitorare la posizione operativa e identificare eventuali errori che potrebbero richiedere ulteriori interventi. Nella tabella seguente sono elencati i nomi dei modelli di report di backup e il relativo output di esempio.

Modello di report di backup	Report di esempio in formato JSON
BACKUP_JOB_REPORT	{ "reportItems": [{ "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2", "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC656AC", "jobStatus": "COMPLETED", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75", "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a", "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",

Modello di report di backup	Report di esempio in formato JSON


```
      "creationDate": "2021-07-
14T23:53:47.229Z",
      "completionDate": "2021-07-
15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:
ec2:us-west-2::image/ami-03
0cafb98e5a6dcdf",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 858993459
2,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-vault:Default",
      "iamRoleArn": "arn:aws:
iam::112233445566:role/service-
role/AWSBackupDefaultServiceRole"
    }
  ]
}
```

Modello di report di backup	Report di esempio in formato JSON

COPY_JOB_REPORT	{
	  "reportItems": [
	    {
	      "reportTimePeriod": "2021-07-14T15:48:31Z - 2021-07-15T15:48:31Z",
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "copyJobId": "E0AD48A9-0560-B668-3EF0-941FDC0AD6B1",
	      "jobStatus": "RUNNING",
	      "resourceType": "EC2",
	      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75",
	      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a",
	      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",
	      "creationDate": "2021-07-15T15:42:04.771Z",
	      "backupSizeInBytes": 8589934592,
	      "sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-007b3819f25697299",
	      "sourceBackupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
	      "destinationRecoveryPointArn": "arn:aws:ec2:us-east-2::image/ami-0eba2199a0bcece3c",
	      "destinationBackupVaultArn": "arn:aws:backup:us-east-2:112233445566:backup-vault:Default",
	      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	    }

Modello di report di backup	Report di esempio in formato JSON
	<pre>] }</pre>

RESTORE_JOB_REPORT	<pre>{
	  "reportItems": [
	    {
	      "reportTimePeriod": "2021-07-
	14T15:53:30Z - 2021-07-15T15:53:3
	0Z",
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "restoreJobId": "4CACA67D-4E12-
	DC05-6C2B-0E97D01FA41E",
	      "jobStatus": "RUNNING",
	      "recoveryPointArn": "arn:aws:
	ec2:us-west-2::image/ami-00
	201ecb57a5271ae",
	      "creationDate": "2021-07-
	15T15:52:49.797Z",
	      "backupSizeInBytes": 858993459
	2,
	      "percentDone": "0.00%",
	      "iamRoleArn": "arn:aws:
	iam::112233445566:role/service-
	role/AWSBackupDefaultServiceRole"
	    }
	  ]
	}</pre>

Modelli di report di conformità

I modelli di report di conformità forniscono report giornalieri sulla conformità delle attività e delle risorse di backup rispetto ai controlli definiti in uno o più framework. Se lo stato di conformità di uno dei framework è `Non-compliant`, occorre esamina un report di conformità per identificare le risorse non conformi.

Tipi di modelli di report di conformità

- `Control compliance report` consente di tenere traccia dello stato di conformità dei controlli definiti nei framework.
- `Resource compliance report` consente di tenere traccia dello stato di conformità delle risorse rispetto ai controlli definiti nei framework. Questi report includono risultati di valutazione dettagliati, incluse informazioni identificative sulle risorse non conformi che puoi utilizzare per identificare e correggere tali risorse.

Nella tabella seguente viene mostrato un output di esempio di un report di conformità.

Modello di report di conformità	Report di esempio in formato JSON
`CONTROL_COMPLIANCE_REPORT`	`{ "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08-17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_Hours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7",`

Modello di report di conformità	Report di esempio in formato JSON


```
      "frameworkDescription": "A test
 framework",
      "controlName": "BACKUP_P
LAN_MIN_FREQUENCY_AND_MIN_R
ETENTION_CHECK",
      "controlComplianceStatus":
 "NON_COMPLIANT",
      "lastEvaluationTime": "2021-08-
17T03:21:19.995Z",
      "numResourcesCompliant": 0,
      "numResourcesNonCompliant": 25,
      "controlScope": "{Complia
nceResourceTypes: [],}",
      "controlParameters": "{\"requi
redFrequencyValue\":\"1\",\
"requiredRetentionDays\":\"35\",
\"requiredFrequencyUnit\":\"hours
\"}"
    }
  ]
}
```

Modello di report di conformità	Report di esempio in formato JSON

RESOURCE_COMPLIANCE_REPORT	{
	  "reportItems": [
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-63c74e66",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.963Z"
	    },
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-b3d7c218",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.961Z"
	    }
	  ]
	}

Creazione di piani di report mediante la console di AWS Backup

Esistono due tipi di report. Uno è il report sui processi, che mostra i processi completati nelle ultime 24 ore e tutti i processi attivi. Il secondo è un report di conformità. I report di conformità possono monitorare i livelli di risorse o i diversi controlli in vigore. Quando crei un report, scegli il tipo di report da creare.

NOTA: a seconda del tipo di account, la visualizzazione della console può variare. Funzionalità multi-account sono visibili sono negli account di gestione.

Analogamente ad un piano di backup, un piano di report viene creato per automatizzare la creazione dei report e definire il bucket Amazon S3 di destinazione. Un piano di report richiede che si disponga di un bucket S3 per ricevere i report. Per istruzioni sulla configurazione di un nuovo bucket S3, consulta Fase 1: creare il primo bucket S3 nella Guida per l'utente di Amazon Simple Storage Service.

Per creare il tuo piano di report nella AWS Backup console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, scegli Report.
3. Scegli Crea piano di report.
4. Scegli uno dei modelli di report dall'elenco a discesa.
5. Inserisci un Nome del piano di report univoco. Il nome deve essere compreso tra 1 e 256 caratteri, deve iniziare con una lettera ed essere costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).
6. (Facoltativo) Inserisci una Descrizione del piano di report.
7. Modelli di report di conformità per un solo account. Scegli uno o più framework su cui generare un report. Puoi aggiungere un massimo di 1.000 framework a un piano di report.

    1. Scegli la tua AWS regione utilizzando il menu a discesa.
    2. Scegli un framework da tale regione utilizzando il menu a discesa.
    3. Scegli Aggiungi framework.
8. (Facoltativo) Per aggiungere tag al piano di report, scegli Aggiungi tag al piano di report.
9. Se utilizzi un account di gestione, puoi specificare quali account desideri includere in questo piano di report. Puoi selezionare Solo il mio account, che genererà report solo sull'account al quale hai effettuato l'accesso. In alternativa, puoi selezionare Uno o più account nella mia organizzazione (disponibile per gli account di gestione e amministratore delegato).

10. Se stai creando un report di conformità per una sola regione, ignora questo passaggio. Puoi selezionare le regioni da includere nel report. Fai clic sul menu a discesa per visualizzare le regioni disponibili. Seleziona Tutte le regioni disponibili o le regioni che preferisci.

    - La casella di controllo Includi nuove regioni quando sono incorporate in Backup Audit Manager attiverà l'inclusione di nuove regioni nei report quando diventano disponibili.

11. Scegli il Formato file del report. Tutti i report possono essere esportati nel formato CSV. Inoltre, i report per una singola regione e una singola regione possono essere esportati nel formato JSON.
12. Scegli il Nome bucket S3 utilizzando l'elenco a discesa.
13. (Facoltativo) Inserisci un prefisso del bucket.

    AWS Backup invia il tuo account corrente, i report della regione corrente as`s3://`*`your-bucket-name`*`/prefix/Backup/`*`accountID`*`/`*`Region`*`/year/month/day/report-name`.

    AWS Backup invia i report relativi a più account a `s3://`*`your-bucket-name`*`/prefix/Backup/crossaccount/`*`Region`*`/year/month/day/report-name`

    AWS Backup invia i tuoi report interregionali a `s3://`*`your-bucket-name`*`/prefix/Backup/`*`accountID`*`/crossregion/year/month/day/report-name`
14. Scegli Crea piano di report.

Successivamente, devi consentire al tuo bucket S3 di ricevere report da. AWS Backup Dopo aver creato un piano di report, AWS Backup Audit Manager genera automaticamente una policy di accesso ai bucket S3 da applicare.

Se crittografi il tuo bucket utilizzando una chiave KMS personalizzata, la politica delle chiavi KMS deve soddisfare i seguenti requisiti:

- L'`Principal`attributo deve includere l'`AWSServiceRolePolicyForBackupReports`ARN del ruolo collegato al servizio Backup Audit Manager.

- L'`Action`attributo deve includere almeno `kms:GenerateDataKey` e`kms:Decrypt`.

La politica AWSServiceRolePolicyForBackupReportsdispone di queste autorizzazioni.

Per visualizzare e applicare questa policy di accesso al bucket S3

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, scegli Report.
3. In Nome del piano report, seleziona un piano di report scegliendo il relativo nome.
4. Scegli Modifica.
5. Scegli Visualizza la policy di accesso per il bucket S3. Puoi anche utilizzare la policy alla fine di questa procedura.
6. Scegli Copia le autorizzazioni.
7. Scegli Modifica la policy del bucket. Tieni presente che fino alla prima creazione del report di backup, il ruolo collegato al servizio a cui si fa riferimento nella policy del bucket S3 non esisterà ancora, con conseguente errore «Principal non valido».
8. Copia le autorizzazioni nella policy.

Policy del bucket di esempio

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:role/aws-service-role/
reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
      },
      "Action":"s3:PutObject",
      "Resource":[
        "arn:aws:s3:::BucketName/*"
      ],
      "Condition":{
        "StringEquals":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Se utilizzi un bucket S3 di destinazione AWS Key Management Service per crittografare il bucket S3 di destinazione che memorizza i report, includi le seguenti azioni nella tua policy:

```
"Action":[
  "kms:GenerateDataKey",
  "kms:Encrypt"
],
"Resource":[
  "*"
],
```

Creazione di piani di report utilizzando l'API AWS Backup

Puoi anche utilizzare i piani di report a livello di codice.

Esistono due tipi di report. Uno è il report sui processi, che mostra i processi completati nelle ultime 24 ore e tutti i processi attivi. Il secondo è un report di conformità. I report di conformità possono monitorare i livelli di risorse o i diversi controlli in vigore. Quando crei un report, scegli il tipo di report da creare.

Analogamente ad un piano di backup, un piano di report viene creato per automatizzare la creazione dei report e definire il bucket Amazon S3 di destinazione. Un piano di report richiede che si disponga di un bucket S3 per ricevere i report. Per istruzioni sulla configurazione di un nuovo bucket S3, consulta Fase 1: creare il primo bucket S3 nella Guida per l'utente di Amazon Simple Storage Service.

Se crittografi il tuo bucket utilizzando una chiave KMS personalizzata, la politica delle chiavi KMS deve soddisfare i seguenti requisiti:

- L'`Principal`attributo deve includere l'`AWSServiceRolePolicyForBackupReports`ARN del ruolo collegato al servizio Backup Audit Manager.

- L'`Action`attributo deve includere almeno `kms:GenerateDataKey` e`kms:Decrypt`.

La politica AWSServiceRolePolicyForBackupReportsdispone di queste autorizzazioni.

Per i report account singolo, regione singola, utilizza la seguente sintassi per chiamare CreateReportPlan.

```
{
   "ReportPlanName": "string",
   "ReportPlanDescription": "string",
   "ReportSetting": {
        "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
 CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT.
 Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
   "ReportDeliveryChannel": {
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is
 CSV if left blank.
   },
   "ReportPlanTags": {
       "string" : "string" // Optional.
   },
   "IdempotencyToken": "string"
}
```

Quando chiami DescribeReportPlan con il nome univoco di un piano di report, l'API di AWS Backup risponde con le seguenti informazioni.

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

Per i report multi-account, multi-regione, utilizza la seguente sintassi per chiamare CreateReportPlan.

```
{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ], *//Organization report only support CSV file*
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ], // Use string value of "ROOT" to include all
 organizational units
      "OrganizationUnits": [ "string" ],
      "Regions": ["string"], // Use wildcard value in string to include all Regions
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "ReportTemplate": "string"
   }
}
```

Quando chiami DescribeReportPlan con il nome univoco di un piano di report, l'API di AWS Backup risponde con le seguenti informazioni per i piani multi-account, multi-regione:

```
{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts":[ "string" ],
         "OrganizationUnits":[ "string" ],
```

```
            "Regions": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "ReportTemplate": "string"
         }
      }
}
```

Creazione di report on demand

Puoi generare nuovi report a tuo piacimento creando un rapporto su richiesta con i seguenti passaggi. AWS Backup Audit Manager invia il report su richiesta al bucket Amazon S3 specificato nel piano di report.

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, scegli Report.
3. In Nome del piano report, seleziona un piano di report scegliendo il relativo nome.
4. Scegli Crea report on demand.

Puoi generare un report on demand per un piano di report esistente.

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, scegli Report.
3. In Piani di report, seleziona un piano di report facendo clic sul pulsante di opzione accanto al nome del piano di report.
4. Fai clic su Azioni, quindi su Crea report on demand.

Puoi eseguire questa operazione per più report, anche durante la generazione dei report.

Visualizzazione dei report di audit

È possibile aprire, visualizzare e analizzare i report di AWS Backup Audit Manager utilizzando i programmi normalmente utilizzati per lavorare con i file CSV o JSON. Tieni presente che i report multi-regione o multi-account sono disponibili solo in formato CSV.

I file di grandi dimensioni vengono suddivisi in più report se la dimensione totale del file supera i 50 MB. Se i file risultanti superano i 50 MB, AWS Backup Audit Manager creerà file CSV aggiuntivi con il resto del rapporto.

Per visualizzare un report

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, scegli Report.
3. In Nome del piano report, seleziona un piano di report scegliendo il relativo nome.
4. In Processi di report, fai clic sul collegamento al report per visualizzare il report.
5. Se Stato report del report presenta una sottolineatura punteggiata, selezionala per visualizzare informazioni sul report.
6. Scegli quale report visualizzare entro il relativo Tempo di completamento.
7. Scegli il Collegamento S3. Viene visualizzato il bucket S3 di destinazione.
8. In Nome, scegli il nome del report che desideri visualizzare.
9. Per salvare il report nel computer, scegli Esegui il download.

Aggiornamento dei piani di report

Puoi aggiornare la descrizione di un piano di report esistente, la destinazione di distribuzione e il formato. Se applicabile, puoi anche aggiungere o rimuovere framework dal piano di report.

Per aggiornare un piano di report esistente

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel riquadro di navigazione a sinistra, scegli Report.
3. In Nome del piano report, seleziona un piano di report scegliendo il relativo nome.
4. Scegli Modifica.
5. Puoi modificare i dettagli del piano di report, inclusi il nome e la descrizione del report, nonché gli account e le regioni inclusi nel report.

Eliminazione di piani di report

Puoi eliminare un piano di report esistente. Quando elimini un piano di report, gli eventuali report già creati da tale piano di report rimarranno nel bucket Amazon S3 di destinazione.

Per eliminare un piano di report esistente

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.

2. Nel riquadro di navigazione a sinistra, scegli Report.
3. In Nome del piano report, seleziona un piano di report scegliendo il relativo nome.
4. Scegli Elimina.
5. Inserisci il nome del piano di report, quindi scegli Elimina piano di report.

Utilizzo di AWS Backup Audit Manager con AWS CloudFormation

Forniamo i seguenti AWS CloudFormation modelli di esempio come riferimento:

Argomenti

Attivazione del monitoraggio delle risorse

Il modello seguente attiva il monitoraggio delle risorse come descritto in Attivazione del monitoraggio delle risorse.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceTypes
      - Label:
          default: Delivery Channel Configuration
        Parameters:
          - DeliveryChannelName
          - Frequency
      - Label:
```

```
          default: Delivery Notifications
        Parameters:
          - TopicArn
          - NotificationEmail
    ParameterLabels:
      AllSupported:
        default: Support all resource types
      IncludeGlobalResourceTypes:
        default: Include global resource types
      ResourceTypes:
        default: List of resource types if not all supported
      DeliveryChannelName:
        default: Configuration delivery channel name
      Frequency:
        default: Snapshot delivery frequency
      TopicArn:
        default: SNS topic name
      NotificationEmail:
        default: Notification Email (optional)

Parameters:
  AllSupported:
    Type: String
    Default: True
    Description: Indicates whether to record all supported resource types.
    AllowedValues:
      - True
      - False

  IncludeGlobalResourceTypes:
    Type: String
    Default: True
    Description: Indicates whether AWS Config records all supported global resource
 types.
    AllowedValues:
      - True
      - False

  ResourceTypes:
    Type: List<String>
    Description: A list of valid AWS resource types to include in this recording group,
 such as AWS::EC2::Instance or AWS::CloudTrail::Trail.
    Default: <All>
```

```
  DeliveryChannelName:
    Type: String
    Default: <Generated>
    Description: The name of the delivery channel.

  Frequency:
    Type: String
    Default: 24hours
    Description: The frequency with which AWS Config delivers configuration snapshots.
    AllowedValues:
      - 1hour
      - 3hours
      - 6hours
      - 12hours
      - 24hours

  TopicArn:
    Type: String
    Default: <New Topic>
    Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification
 Service (Amazon SNS) topic that AWS Config delivers notifications to.

  NotificationEmail:
    Type: String
    Default: <None>
    Description: Email address for AWS Config notifications (for new topics).

Conditions:
  IsAllSupported: !Equals
    - !Ref AllSupported
    - True
  IsGeneratedDeliveryChannelName: !Equals
    - !Ref DeliveryChannelName
    - <Generated>
  CreateTopic: !Equals
    - !Ref TopicArn
    - <New Topic>
  CreateSubscription: !And
    - !Condition CreateTopic
    - !Not
      - !Equals
        - !Ref NotificationEmail
        - <None>
```

```
Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours

Resources:

  ConfigBucket:
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
      BucketEncryption:
          ServerSideEncryptionConfiguration:
            - ServerSideEncryptionByDefault:
                SSEAlgorithm: AES256

  ConfigBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AWSConfigBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/AWSLogs/
${AWS::AccountId}/*"
```

```
          - Sid: AWSConfigBucketSecureTransport
            Action:
              - s3:*
            Effect: Deny
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/*"
            Principal: "*"
            Condition:
              Bool:
                aws:SecureTransport:
                  false

  ConfigTopic:
    Condition: CreateTopic
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Sub "config-topic-${AWS::AccountId}"
      DisplayName: AWS Config Notification Topic
      KmsMasterKeyId: "alias/aws/sns"

  ConfigTopicPolicy:
    Condition: CreateTopic
    Type: AWS::SNS::TopicPolicy
    Properties:
      Topics:
        - !Ref ConfigTopic
      PolicyDocument:
        Statement:
          - Sid: AWSConfigSNSPolicy
            Action:
              - sns:Publish
            Effect: Allow
            Resource: !Ref ConfigTopic
            Principal:
              Service:
                - config.amazonaws.com

  EmailNotification:
    Condition: CreateSubscription
    Type: AWS::SNS::Subscription
    Properties:
      Endpoint: !Ref NotificationEmail
      Protocol: email
```

```
      TopicArn: !Ref ConfigTopic

  ConfigRecorderServiceRole:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: config.amazonaws.com
      Description: Service Role for AWS Config

  ConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    DependsOn:
      - ConfigBucketPolicy
      - ConfigRecorderServiceRole
    Properties:
      RoleARN: !Sub arn:${AWS::Partition}:iam::${AWS::AccountId}:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
      RecordingGroup:
        AllSupported: !Ref AllSupported
        IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
        ResourceTypes: !If
          - IsAllSupported
          - !Ref AWS::NoValue
          - !Ref ResourceTypes

  ConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    DependsOn:
      - ConfigBucketPolicy
    Properties:
      Name: !If
        - IsGeneratedDeliveryChannelName
        - !Ref AWS::NoValue
        - !Ref DeliveryChannelName
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: !FindInMap
          - Settings
          - FrequencyMap
          - !Ref Frequency
      S3BucketName: !Ref ConfigBucket
      SnsTopicARN: !If
        - CreateTopic
        - !Ref ConfigTopic
        - !Ref TopicArn
```

Distribuzione dei controlli predefiniti

Il modello seguente crea un framework con i controlli predefiniti descritti in Controlli e correzione di AWS Backup Audit Manager.

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
        - ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
            - ParameterName: requiredFrequencyUnit
              ParameterValue: 'hours'
            - ParameterName: requiredFrequencyValue
              ParameterValue: '24'
          ControlScope:
            Tags:
              - Key: customizedKey
                Value: customizedValue
        - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
          ControlInputParameters:
            - ParameterName: crossRegionList
              ParameterValue: 'eu-west-2'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
          ControlInputParameters:
            - ParameterName: crossAccountList
              ParameterValue: '111122223333'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
        - ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
        - ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
          ControlInputParameters:
            - ParameterName: maxRestoreTime
```

```
              ParameterValue: '720'

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

Esenzione dei ruoli IAM dalla valutazione del controllo

Il controllo BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED consente di esentare fino a cinque ruoli IAM che possono comunque eliminare manualmente i punti di ripristino. Il modello seguente distribuisce questo controllo ed esenta inoltre due ruoli IAM.

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
          ControlInputParameters:
            - ParameterName: "principalArnList"
              ParameterValue: !Sub
 "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/
ConfigRole"

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

Creazione di un piano di report

Il modello seguente crea un piano di report.

```
Description: "Basic AWS::Backup::ReportPlan template"

Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
```

```
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"

Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:
        Formats:
          - "CSV"
        S3BucketName: !Ref S3BucketName
        S3KeyPrefix: !Ref S3KeyPrefix
      ReportSetting:
        ReportTemplate: !Ref ReportTemplate
        Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
        Accounts: ['123456789098']
        OrganizationUnits: ['ou-abcd-1234wxyz']
      ReportPlanTags:
        - Key: "a"
          Value: "1"
        - Key: "b"
          Value: "2"

Outputs:
  ReportPlanArn:
    Value: !GetAtt TestReportPlan.ReportPlanArn
```

Utilizzo di AWS Backup Audit Manager con AWS Audit Manager

AWS Backup I controlli di Audit Manager sono mappati a controlli standard predefiniti AWS Audit Manager, che consentono di importare i risultati della conformità di AWS Backup Audit Manager AWS Audit Manager nei report. Questa operazione può essere eseguita per aiutare un responsabile della conformità, un responsabile dell'audit o un altro collega che genera report sulle attività di backup come parte della posizione di conformità complessiva dell'organizzazione.

Puoi importare i risultati di conformità dei controlli di AWS Backup Audit Manager nei tuoi AWS Audit Manager framework. AWS Audit Manager Per consentire la raccolta automatica dei dati dai controlli

AWS Backup Audit Manager, crea un controllo personalizzato AWS Audit Manager utilizzando le istruzioni per la personalizzazione di un controllo esistente nella Guida per l'AWS Audit Manager utente. Mentre segui queste istruzioni, tieni presente che la fonte di dati per i AWS Backup controlli è AWS Config.

Per un elenco dei AWS Backup controlli, vedi Scelta dei controlli.

Controlli e correzioni

Questa pagina elenca i controlli disponibili per AWS Backup Audit Manager. Puoi scegliere il riquadro informativo corretto per visualizzare un elenco di controlli e passare a un controllo specifico. Per confrontare rapidamente i controlli, consulta la tabella in Scelta dei controlli. Per definire i controlli a livello di codice, consulta i frammenti di codice in Creazione di framework mediante l'API di AWS Backup .

Puoi utilizzare fino a 50 controlli per account e per regione. L'utilizzo dello stesso controllo in due framework diversi equivale all'utilizzo di due controlli del limite di controllo 50.

In questa pagina viene elencato ciascun controllo con le seguenti informazioni:

- Descrizione. I valori tra parentesi ("[ ]") sono i valori predefiniti dei parametri.
- Le risorse valutate dal controllo.
- I parametri del controllo.
- Occasione in cui si verifica l'esecuzione del controllo.
- L'ambito del controllo, come segue:
  - Puoi specificare Risorse per tipo scegliendo uno o più servizi supportati da AWS Backup.
  - Puoi specificare un ambito di Risorse con tag con una singola chiave tag e un valore opzionale.
  - Puoi specificare una singola risorsa utilizzando l'elenco a discesa Risorsa singola.
- Procedure di correzione per rendere conformi le risorse applicabili.

Tieni presente che, quando i controlli valutano la conformità delle risorse, verranno incluse solo le risorse attive. Ad esempio, un'istanza Amazon EC2 in stato di esecuzione verrà valutata dal controllo Ultimo punto di ripristino creato. Un'istanza EC2 in uno stato di arresto non verrà inclusa nella valutazione di conformità.

Le risorse di backup sono protette da un piano di backup

Descrizione: valuta se le risorse sono protette da un piano di backup.

Risorsa: `AWS Backup: backup selection`

Parametri: nessuno

Si verifica: automaticamente ogni 24 ore

Ambito:

- Risorse con tag
- Risorse per tipo (impostazione predefinita)
- Risorsa singola

Correzione: assegnare le risorse a un piano di backup. AWS Backup protegge automaticamente le risorse dopo averle assegnate a un piano di backup. Per ulteriori informazioni, consulta Assegnazione di risorse a un piano di backup.

Frequenza minima e conservazione minima del piano di backup

Descrizione: valuta se i piani di backup contengono almeno una regola di backup per la quale la frequenza di backup è pari ad almeno [1 giorno] e il periodo di conservazione è pari ad almeno [35 giorni].

Risorsa: `AWS Backup: backup plans`

Parametri:

- Frequenza di backup richiesta in numero di ore o giorni.
- Periodo di conservazione richiesto in numero di giorni, settimane, mesi o anni. Si consiglia un periodo di conservazione a caldo di almeno una settimana per consentire l'esecuzione AWS Backup di backup incrementali quando possibile, evitando costi aggiuntivi.

Si verifica: modifiche alla configurazione

Ambito:

- Risorse con tag

- Risorsa singola

Correzione: aggiorna un piano di backup per modificare la relativa frequenza di backup, il periodo di conservazione o entrambi. L'aggiornamento del piano di backup modifica il periodo di conservazione dei punti di ripristino creati dal piano dopo l'aggiornamento.

I vault impediscono l'eliminazione manuale dei punti di ripristino

Descrizione: valuta se i vault di backup non consentono l'eliminazione manuale dei punti di ripristino ad eccezione di determinati ruoli IAM.

Risorsa: `AWS Backup: backup vaults`

Parametri: il nome della risorsa Amazon (ARN) di un massimo di cinque ruoli IAM consentivano l'eliminazione manuale dei punti di ripristino.

Si verifica: modifiche alla configurazione

Ambito:

- Risorse con tag
- Risorsa singola

Conservazione: creare o modificare una policy di accesso basata su risorse su un vault di backup. Per un esempio di policy e istruzioni su come impostare una policy di accesso del vault di backup, consulta Negare l'accesso per eliminare i punti di ripristino in un vault di backup.

I punti di ripristino sono crittografati

Descrizione: valuta se i punti di ripristino sono crittografati.

Risorsa: `AWS Backup: recovery points`

Parametri: nessuno

Si verifica: modifiche alla configurazione

Ambito:

- Risorse con tag

Correzione: configurare la crittografia per i punti di ripristino. Il modo in cui si configura la crittografia per i punti di AWS Backup ripristino varia a seconda del tipo di risorsa.

È possibile configurare la crittografia per i tipi di risorse che supportano la AWS Backup gestione completa nell'utilizzo AWS Backup. Se il tipo di risorsa non supporta la AWS Backup gestione completa, devi configurarne la crittografia di backup seguendo le istruzioni del servizio, come la crittografia Amazon EBS nella Amazon Elastic Compute Cloud User Guide. Per visualizzare l'elenco dei tipi di risorse che supportano la AWS Backup gestione completa, consulta la sezione « AWS Backup Gestione completa» della Disponibilità delle funzionalità per risorsa tabella.

Conservazione minima stabilita per punto di ripristino

Descrizione: valuta se il periodo di conservazione del punto di ripristino è pari ad almeno [35 giorni].

Risorsa: `AWS Backup: recovery points`

Parametri: periodo di conservazione del punto di ripristino richiesto in numero di giorni, settimane, mesi o anni. Consigliamo un periodo di conservazione a caldo di almeno una settimana per consentire l'esecuzione AWS Backup di backup incrementali quando possibile, evitando costi aggiuntivi.

Si verifica: modifiche alla configurazione

Ambito:

- Risorse con tag

Correzione: modifica i periodi di conservazione dei punti di ripristino. Per ulteriori informazioni, consulta Modifica di un backup.

Copia di backup tra regioni pianificata

Descrizione: valuta se una risorsa è configurata per creare copie dei relativi backup in un'altra AWS regione.

Risorsa: `AWS Backup: backup selection`

Parametri:

- Seleziona il/i in cui deve esistere la copia di backup (facoltativo) Regione AWS

- Regione

Si verifica: automaticamente ogni 24 ore

Ambito:

- Risorse con tag
- Risorse per tipo
- Risorsa singola

Correzione: aggiorna un piano di backup per modificare il Regione AWS luogo in cui deve esistere la copia di backup.

Copia di backup tra account pianificata

Descrizione: valuta se una risorsa è configurata per creare copie dei backup in un altro account. Puoi aggiungere fino a 5 account che devono essere valutati dal controllo. L'account di destinazione deve trovarsi nella stessa organizzazione dell'account di origine in AWS Organizations.

Risorsa: `AWS Backup: backup selection`

Parametri:

- Seleziona gli ID AWS dell'account in cui deve esistere la copia di backup (opzionale)
- ID account

Si verifica: automaticamente ogni 24 ore

Ambito:

- Risorse con tag
- Risorse per tipo
- Risorsa singola

Correzione: aggiorna un piano di backup per modificare o aggiungere gli ID dell' AWS account in cui deve esistere la copia.

I backup sono protetti da AWS Backup Vault Lock

Descrizione: valuta se una risorsa dispone di backup immutabili archiviati in un vault di backup bloccato.

Risorsa: `AWS Backup: backup selection`

Parametri:

- Inserisci i giorni di conservazione minimi e massimi per AWS Backup Vault Lock (opzionale)
- Numero minimo di giorni di conservazione
- Numero massimo di giorni di conservazione

Si verifica: automaticamente ogni 24 ore

Ambito:

- Risorse con tag
- Risorse per tipo
- Risorsa singola

Correzione: blocca un vault di backup per impostare il nome, modificare il numero giorni di conservazione minimo, il numero di giorni di conservazione massimo o entrambi. Può anche includere `ChangeableForDays` per un blocco del vault in modalità di conformità.

È stato creato l'ultimo punto di ripristino

Descrizione: questo controllo valuta se un punto di ripristino è stato creato entro il periodo di tempo specificato (in giorni o ore).

Il controllo è conforme se per la risorsa è stato creato un punto di ripristino entro il periodo di tempo specificato. Il controllo è non conforme se un punto di ripristino non è stato creato entro il numero di giorni o di ore specificato.

Risorsa: `AWS Backup: recovery points`

Parametri:

- Inserisci l'intervallo di tempo specificato in numeri interi, espressi in ore o giorni.

- I valori di `hours` possono essere compresi tra `1` e `744`.
- I valori di `days` possono essere compresi tra `1` e `31`.

Si verifica: automaticamente ogni 24 ore

Ambito:

- Risorse con tag
- Risorse per tipo
- Risorsa singola

Correzione:

- Aggiorna un piano di backup per modificare l'intervallo di tempo specificato di creazione del punto di ripristino.
- Inoltre, puoi creare un backup on demand.

Tempo di ripristino necessario per le risorse

Descrizione: valuta se il ripristino delle risorse protette è stato completato entro il tempo di ripristino previsto.

Questo controllo verifica se il tempo di ripristino di una particolare risorsa soddisfa la durata prevista. La regola è NON_COMPLIANT se `LatestRestoreExecutionTimeMinutes` di un tipo di risorsa è superiore a `maxRestoreTime` in minuti.

Parametri:

- `maxRestoreTime` (in minuti)

Si verifica: automaticamente ogni 24 ore

Ambito:

- Risorse con tag
- Risorse per tipo
- Risorsa singola

> **Note**
>
> AWS Backup non fornisce alcun accordo sul livello di servizio (SLA) per i tempi di ripristino. I tempi di ripristino possono variare in base al carico e alla capacità del sistema, anche per ripristini contenenti le stesse risorse.

Gestione AWS Backup delle risorse su più risorse Account AWS

> **Note**
>
> Prima di gestire le risorse su più Account AWS account AWS Backup, gli account devono appartenere alla stessa organizzazione del AWS Organizations servizio.

Puoi utilizzare la funzionalità di gestione tra account AWS Backup per gestire e monitorare i processi di backup, ripristino e copia tra quelli con Account AWS AWS Organizations cui configuri. AWS Organizationsè un servizio che offre una gestione basata su policy per più utenti Account AWS da un unico account di gestione. Consente di standardizzare il modo in cui vengono implementate le policy di backup, riducendo al minimo gli errori manuali e gli sforzi contemporaneamente. Puoi identificare facilmente le risorse in tutti gli account che soddisfano i criteri a cui sei interessato attraverso un'unica visualizzazione centralizzata.

Se lo configuri AWS Organizations, puoi configurare AWS Backup il monitoraggio delle attività in tutti i tuoi account in un unico posto. Puoi anche creare una policy di backup e applicarla ad account selezionati che fanno parte della tua organizzazione e visualizzare le attività aggregate dei job di backup direttamente dalla AWS Backup console. Questa funzionalità consente agli amministratori di backup di monitorare in modo efficace lo stato dei processi di backup in centinaia di account in tutta l'azienda da un singolo account di gestione. Si applicano quote per AWS Organizations.

Ad esempio, crea una policy di backup A che richiede backup giornalieri di risorse specifiche e li conserva per 7 giorni. Applica la policy di backup A all'intera organizzazione. In questo modo a ogni account dell'organizzazione viene assegnata tale policy di backup con il corrispondente piano di backup visibile nell'account. Quindi, crea una UO denominata Finanza di cui intendi conservare i backup per soli 30 giorni. In questo caso, occorre una policy di backup B che sostituisce il valore del ciclo di vita e che deve essere collegata alla UO Finanza. Ciò significa che tutti gli account nella UO Finanza ottengono un nuovo piano di backup efficace che esegue backup giornalieri di tutte le risorse specificate e li conserva per 30 giorni.

In questo esempio, le policy di backup A e B sono state unite in una singola policy di backup, che definisce la strategia di protezione per tutti gli account nella UO denominata Finanza. Tutti gli altri account dell'organizzazione rimangono protetti dalla policy di backup A. L'unione viene eseguita

solo per le policy di backup che condividono lo stesso nome del piano di backup. Puoi anche far coesistere le policy A e B in un determinato account senza alcuna unione e utilizzare operatori di unione avanzati solo nella vista JSON della console. Per informazioni dettagliate sull'unione di policy, consulta Definizione di policy, sintassi delle policy ed ereditarietà delle policy nella Guida per l'utente di AWS Organizations . Per ulteriori riferimenti e casi d'uso, consulta il blog Managing backups at scale in your AWS Organizations using AWS Backup e il video tutorial Managing backup at scale in your using. AWS Organizations AWS Backup

Consulta la sezione Disponibilità delle funzionalità per AWS regione per scoprire dove è disponibile la funzionalità di gestione tra account.

Per utilizzare la gestione di più account, è necessario attenersi alla seguente procedura:

1. Crea un account di gestione AWS Organizations e aggiungi account sotto l'account di gestione.
2. Abilita la funzionalità di gestione tra account in AWS Backup.
3. Crea una politica di backup da applicare a tutti gli utenti del tuo Account AWS account di gestione.

> **Note**
>
> Per i piani di backup gestiti da Organizations, le impostazioni di consenso esplicito delle risorse nell'account di gestione sostituiscono quelle in un account membro, anche se sono configurati uno o più account amministratore delegato. Gli account amministratore delegato sono account membro con funzionalità avanzate e non possono sostituire le impostazioni di un account di gestione.

4. Gestisci i processi di backup, ripristino e copia in tutti i tuoi Account AWS.

Argomenti

- Creazione di un account di gestione in Organizations
- Abilitazione della gestione di più account
- Amministratore delegato
- Creazione di una policy di backup
- Monitoraggio delle attività in più Account AWS
- Regole di consenso esplicito delle risorse
- Definizione di policy, sintassi delle policy ed ereditarietà delle policy

Creazione di un account di gestione in Organizations

Innanzitutto, devi creare la tua organizzazione e configurarla con AWS gli account dei membri in AWS Organizations.

Per creare un account di gestione in AWS Organizations e aggiungere account

- Per istruzioni, consulta Tutorial: creazione e configurazione di un'organizzazione nella Guida per l'utente di AWS Organizations .

Abilitazione della gestione di più account

Prima di poter utilizzare la gestione tra account in AWS Backup, devi abilitare la funzionalità (ovvero attivarla). Dopo averla abilitata, puoi creare policy di backup che consentano di automatizzare la gestione simultanea di più account.

Per abilitare la gestione di più account

1. Apri il file all' Console di backup AWS indirizzo https://console.aws.amazon.com/backup/. Accedi utilizzando le credenziali dell'account di gestione.
2. Nel riquadro di navigazione a sinistra, scegliere Impostazioni per aprire la pagina di gestione di più account.
3. Nella sezione Policy di backup, scegliere Abilita.

   Ciò consente di accedere a tutti gli account e di creare policy che automatizzano la gestione simultanea di più account nell'organizzazione.
4. Nella sezione Monitoraggio di più account, scegliere Abilita.

   In questo modo puoi monitorare le attività di backup, copia e ripristino di tutti gli account dell'organizzazione dall'account di gestione.

Amministratore delegato

L'amministrazione delegata offre agli utenti assegnati in un account membro registrato un modo pratico per eseguire la maggior parte delle attività AWS Backup amministrative. È possibile scegliere di delegare l'amministrazione AWS Backup a un account membro interno AWS Organizations,

estendendo così la capacità di gestione AWS Backup dall'esterno dell'account di gestione a tutta l'organizzazione.

Per impostazione predefinita, un account di gestione è l'account utilizzato per modificare e gestire le policy. Utilizzando la funzionalità di amministratore delegato, puoi delegare queste funzioni di gestione agli account membro designati. A loro volta, tali account possono gestire policy, in aggiunta all'account di gestione.

Dopo che è stato correttamente registrato per l'amministrazione delegata, un account membro diventa un account amministratore delegato. Tieni presente che gli account, non gli utenti, sono designati come amministratori delegati.

L'abilitazione di account amministratore delegato consente di gestire le policy di backup, ridurre al minimo il numero di utenti con accesso all'account di gestione ed eseguire il monitoraggio dei processi su più account.

Di seguito è riportata una tabella che mostra le funzioni dell'account di gestione, gli account delegati come amministratori di Backup e gli account membri dell' AWS organizzazione.

> **Note**
>
> Gli account amministratore delegato sono account membro con funzionalità avanzate che non possono sostituire le impostazioni di consenso esplicito del servizio di altri account membro, come invece possono gli account di gestione.

PRIVILEGI	GESTIONE DELL'ACCOUNT	AMMINISTRATORE DELEGATO	ACCOUNT MEMBRO
Registrare/annullare la registrazione degli account amministr atore delegato	Sì	No	No
Gestisci le politiche di backup tra gli account in AWS Organizations	Sì	Sì	No

PRIVILEGI	GESTIONE DELL'ACCOUNT	AMMINISTRATORE DELEGATO	ACCOUNT MEMBRO
Monitorare processi in più account	Sì	Sì	No

Prerequisiti

Prima di poter delegare l'amministrazione dei backup, è necessario registrare almeno un account membro nell' AWS organizzazione come amministratore delegato. Per poter registrare un account come amministratore delegato, è necessario innanzitutto configurare quanto segue:

- AWS Organizations deve essere abilitato e configurato con almeno un account membro oltre all'account di gestione predefinito.
- Nella AWS Backup console, assicurati che le politiche di backup, il monitoraggio tra account e le funzionalità di backup tra account siano attivate. Queste si trovano sotto il riquadro Amministratori delegati nella console. AWS Backup
  - Il monitoraggio di più account consente di monitorare l'attività di backup su tutti gli account dell'organizzazione dall'account di gestione, nonché dagli account amministratore delegato.
  - Facoltativo: backup su più account, che consente agli account dell'organizzazione di copiare i backup su altri account (per le risorse multiaccount supportate da Backup).
  - Abilita AWS Backup l'accesso al servizio con.

La configurazione dell'amministrazione delegata comprende due fasi. La prima fase consiste nel delegare il monitoraggio dei processi in più account. La seconda fase consiste nel delegare la gestione delle policy di backup.

Registrazione di un account membro come un account amministratore delegato

Questa è la prima sezione: Utilizzo della AWS Backup console per registrare un account amministratore delegato per monitorare i lavori tra account. Per delegare AWS Backup le politiche, utilizzerai la console Organizations nella sezione successiva.

Per registrare un account membro utilizzando la AWS Backup Console:

1. Apri il file Console di backup AWS all'indirizzo https://console.aws.amazon.com/backup/. Accedi utilizzando le credenziali dell'account di gestione.
2. In Il mio account, nella navigazione a sinistra della console, scegli Impostazioni.
3. Nel riquadro Amministratore delegato, fai clic su Registra amministratore delegato o Aggiungi amministratore delegato.
4. Nella pagina Registra amministratore delegato, seleziona l'account che desideri registrare, quindi scegli Registra account.

Questo account designato verrà ora registrato come un amministratore delegato, con privilegi amministrativi per monitorare i processi tra account all'interno dell'organizzazione, nonché visualizzare e modificare policy (delega di policy). Questo account membro non può registrare o annullare la registrazione di altri account amministratore delegato. Puoi utilizzare la console per registrare fino a cinque account come amministratori delegati.

Per registrare un account membro in modo programmatico:

Utilizza il comando della CLI `register-delegated-administrator`. Puoi specificare i seguenti parametri nella richiesta CLI:

- `service-principal`
- `account-id`

Di seguito è riportato un esempio di richiesta CLI per registrare un account membro in modo programmatico:

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Annullamento della registrazione di un account membro

Utilizzate la seguente procedura per rimuovere l'accesso amministrativo AWS Backup annullando la registrazione di un account membro AWS dell'organizzazione che era stato precedentemente designato come amministratore delegato.

Per annullare la registrazione di un account membro utilizzando la console

1. Aprire il file all'indirizzo https://console.aws.amazon.com/backup/. Console di backup AWS Accedi utilizzando le credenziali dell'account di gestione.
2. In Il mio account, nella navigazione a sinistra della console, scegli Impostazioni.
3. Nella sezione Amministratore delegato, fai clic su Annulla registrazione dell'account.
4. Scegli gli account di cui desideri annullare la registrazione.
5. Nella finestra di dialogo Annulla registrazione dell'account, esamina le implicazioni sulla sicurezza, quindi digita `confirm` per completare l'annullamento della registrazione.
6. Scegli `Deregister account`.

Per annullare la registrazione di un account membro in modo programmatico:

Utilizza il comando CLI `deregister-delegated-administrator` per annullare la registrazione di un account amministratore delegato. Puoi specificare i seguenti parametri nella richiesta API:

- `service-principal`
- `account-id`

Di seguito è riportato un esempio di una richiesta CLI per annullare la registrazione di un account membro in modo programmatico:

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Delega le AWS Backup politiche tramite AWS Organizations

All'interno della AWS Organizations console, è possibile delegare l'amministrazione di più policy, incluse le policy di Backup.

Dall'account di gestione che ha eseguito l'accesso alla console di AWS Organizations, puoi creare, visualizzare o eliminare una policy di delega basata sulle risorse per l'organizzazione. Per la procedura di delega delle policy, consulta Creazione di una policy di delega basata sulle risorse nella Guida per l'utente di AWS Organizations .

Creazione di una policy di backup

Dopo aver abilitato la gestione di più account, crea una policy di backup di più account dall'account di gestione.

> **Warning**
>
> Quando crei una policy con JSON, i nomi di chiave duplicati verranno rifiutati. Il nome di ogni chiave deve essere univoco se in un'unica politica sono inclusi più piani, regole o selezioni.

Crea una policy di backup tramite la console AWS Backup

1. Nel riquadro di navigazione a sinistra selezionare Policy. Nella pagina Policy di backup, scegliere Crea policy di backup.
2. Nella sezione Dettagli, immettere il nome della policy di backup e fornire una descrizione.
3. Nella sezione Dettagli dei piani di backup, scegliere la scheda Editor visivo ed effettuare le seguenti operazioni:

   a. In Nome del piano di Backup, immettere un nome.

   b. In Regioni, scegliere una regione dall'elenco.
4. Nella sezione Configurazione regola di Backup, scegliere Aggiungi regola di Backup.

   Il numero massimo di regole per piano di backup è 10. Se un piano contiene più di 10 regole, il piano di backup verrà ignorato e non verrà creato alcun backup.

   a. In Nome regola, immettere un nome per la regola. Il nome della regola fa distinzione tra maiuscole e minuscole e può contenere solo caratteri alfanumerici o trattini.

   b. In Pianifica,scegliere una frequenza di backup nell'elenco Frequenza e selezionare una delle opzioni di Finestra di Backup. Ti consigliamo di scegliere Utilizza le impostazioni predefinite della finestra di backup - scelta consigliata.
5. In Ciclo di vita, scegliere le impostazioni del ciclo di vita desiderate.
6. In Nome del vault di Backup, immettere un nome. Questo è il vault di backup in cui verranno archiviati i punti di ripristino creati dai backup.

   Assicurati che l'archivio di backup esista in tutti i tuoi account. AWS Backup non verifica questo.

7. (opzionale) Scegli una regione di destinazione dall'elenco se desideri che i tuoi backup vengano copiati in un'altra Regione AWS e aggiungi tag. Puoi scegliere i tag per i punti di ripristino creati, indipendentemente dalle impostazioni di copia in più regioni. Puoi inoltre aggiungere altre regole.
8. Nella sezione Assegnazione delle risorse, fornisci il nome del ruolo AWS Identity and Access Management (IAM). Per utilizzare il ruolo AWS Backup di servizio, fornisci`service-role/AWSBackupDefaultServiceRole`.

   AWS Backup assume questo ruolo in ciascun account per ottenere le autorizzazioni necessarie per eseguire processi di backup e copia, incluse le autorizzazioni relative alle chiavi di crittografia, ove applicabili. AWS Backup utilizza questo ruolo anche per eseguire eliminazioni del ciclo di vita.

   > **Note**
   >
   > AWS Backup non convalida che il ruolo esista o se il ruolo possa essere assunto.
   > Per i piani di backup creati dalla gestione tra più account, AWS Backup utilizzerà le impostazioni di attivazione dell'account di gestione e sostituirà le impostazioni degli account specifici.
   > Per ciascun account a cui desideri aggiungere policy di backup, devi creare i vault e i ruoli IAM autonomamente.

9. Aggiungi tag per selezionare le risorse di cui desideri eseguire il backup. Il numero massimo di tag consentito è 30.

   AWS Organizations la policy consente di specificare un massimo di 30 tag se viene creato un piano di backup tramite la policy Organizations. È possibile includere tag aggiuntivi utilizzando più assegnazioni di risorse o utilizzando più piani di backup.

   Se il numero di tag è superiore a 30 nella stessa selezione di backup, modificando o utilizzando la selezione esistente`@@append`, il piano di backup non sarà più valido e verrà rimosso dall'account locale.
10. Nella sezione Impostazioni avanzate, scegli Windows VSS se la risorsa di cui stai eseguendo il backup esegue Microsoft Windows su un'istanza Amazon EC2. Ciò consente di eseguire backup di Windows VSS coerenti con le applicazioni.

> **Note**
>
> AWS Backup attualmente supporta backup coerenti con le applicazioni di risorse in esecuzione solo su Amazon EC2. Non tutti i tipi di istanze o applicazioni sono supportati per i backup di Windows VSS. Per ulteriori informazioni, consulta Creazione di backup Windows VSS.

11. Scegliere Aggiungi piano di backup per aggiungerlo alla policy, quindi scegliere Crea policy di backup.

    La creazione di una policy di backup non protegge le risorse finché non vengono collegate agli account. Puoi scegliere il nome della policy e visualizzare i dettagli.

    Di seguito è riportato un esempio di AWS Organizations policy che crea un piano di backup. Se si abilita il backup di Windows VSS, è necessario aggiungere le autorizzazioni che consentano di eseguire backup coerenti con le applicazioni, come illustrato nella sezione `advanced_backup_settings` della policy.

```
{
  "plans": {
    "PiiBackupPlan": {
      "regions": {
        "@@append":[
          "us-east-1",
          "eu-north-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {
            "@@assign": "cron(0 0/1 ? * * *)"
          },
          "start_backup_window_minutes": {
            "@@assign": "60"
          },
          "complete_backup_window_minutes": {
            "@@assign": "604800"
          },
          "target_backup_vault_name": {
            "@@assign": "FortKnox"
```

```
          },
          "recovery_point_tags": {
            "owner": {
              "tag_key": {
                "@@assign": "Owner"
              },
              "tag_value": {
                "@@assign": "Backup"
              }
            }
          },
          "lifecycle": {
            "delete_after_days": {
              "@@assign": "365"
            },
            "move_to_cold_storage_after_days": {
              "@@assign": "180"
            }
          },
          "copy_actions": {
            "arn:aws:backup:eu-north-1:$account:backup-vault:myTargetBackupVault" :
 {
            "target_backup_vault_arn" : {
            "@@assign" : "arn:aws:backup:eu-north-1:$account:backup-
vault:myTargetBackupVault"  },
              "lifecycle": {
                "delete_after_days": {
                  "@@assign": "365"
                },
                "move_to_cold_storage_after_days": {
                  "@@assign": "180"
                }
              }
            }
          }
        },
        "selections": {
          "tags": {
            "SelectionDataType": {
              "iam_role_arn": {
                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
              },
              "tag_key": {
```

```
              "@@assign": "dataType"
            },
            "tag_value": {
              "@@assign": [
                "PII",
                "RED"
              ]
            }
          }
        }
      },
      "backup_plan_tags": {
        "stage": {
          "tag_key": {
            "@@assign": "Stage"
          },
          "tag_value": {
            "@@assign": "Beta"
          }
        }
      }
    }
  }
}
```

12. Nella sezione Destinazioni, scegliere l'unità organizzativa o l'account a cui si desidera collegare la policy e selezionare Collega. La policy può anche essere aggiunta a singoli account o unità organizzative.

> **Note**
>
> Assicurati di convalidare la policy e di includere tutti i campi obbligatori nella policy. Se parti della policy non sono valide, AWS Backup le ignora, mentre quelle valide funzioneranno come previsto. Attualmente, AWS Backup non convalida la correttezza AWS Organizations delle politiche.
>
> Se si applica una policy all'account di gestione e una policy diversa a un account membro e tali policy sono in conflitto (ad esempio, i periodi di conservazione dei backup sono diversi), entrambe le policy verranno eseguite senza problemi (ovvero, le policy verranno eseguite in maniera indipendente per ciascun account). Ad esempio, se la policy dell'account di gestione esegue il backup di un volume Amazon EBS una volta

al giorno e la policy locale esegue il backup di un volume EBS una volta alla settimana, entrambi le policy verranno eseguite.
Se i campi obbligatori non sono presenti nella policy effettiva che verrà applicata a un account, probabilmente a causa dell'unione tra policy diverse, AWS Backup non applica alcuna policy all'account. Se alcune impostazioni non sono valide, le AWS Backup regola.

Indipendentemente dalle impostazioni di attivazione in un account membro in un piano di backup creato in base a una politica di backup, AWS Backup utilizzerà le impostazioni di attivazione specificate nell'account di gestione dell'organizzazione.

Quando si collega una policy a un'unità organizzativa, ogni account che ne fa parte la ottiene automaticamente, mentre ogni account rimosso dall'unità organizzativa la perde. I piani di backup corrispondenti vengono eliminati automaticamente da tale account.

Monitoraggio delle attività in più Account AWS

Per monitorare i processi di backup, copia e ripristino in più account, devi abilitare il monitoraggio di più account. Ciò consente di monitorare le attività di backup in tutti gli account dall'account di gestione dell'organizzazione. Dopo l'attivazione, tutti i processi dell'organizzazione creati sono visibili. Quando si disattiva, AWS Backup mantiene i processi nella visualizzazione aggregata per 30 giorni (dal raggiungimento di uno stato terminale). I processi creati dopo la disattivazione non sono visibili e non mostrano i processi di backup appena creati. Per le istruzioni di attivazione, consulta Abilitazione della gestione di più account.

Per monitorare più account

1. Aprire il file all' Console di backup AWS indirizzo https://console.aws.amazon.com/backup/. Accedi utilizzando le credenziali dell'account di gestione.
2. Nel riquadro di navigazione a sinistra, scegliere Impostazioni per aprire la pagina di gestione di più account.
3. Nella sezione Monitoraggio di più account, scegliere Abilita.

   In questo modo puoi monitorare le attività di backup e ripristino di tutti gli account dell'organizzazione dall'account di gestione.
4. Nel riquadro di navigazione a sinistra, selezionare Monitoraggio di più account.

5. Nella pagina Monitoraggio di più account, scegliere la scheda Lavori di Backup, Lavori di ripristino o Copia attività per visualizzare tutti i processi creati in tutti gli account. Puoi vedere ognuno di questi lavori per Account AWS ID e puoi vedere tutti i lavori in un determinato account.
6. Nella casella di ricerca è possibile filtrare i processi in base all'ID account, Stato o ID lavoro.

   Ad esempio, puoi scegliere la scheda Lavori di Backup e visualizzare tutti i processi di backup creati in tutti gli account. Puoi filtrare l'elenco in base all' ID account e visualizzare tutti i processi di backup creati in tale account.

Regole di consenso esplicito delle risorse

Se il piano di backup di un account membro è stato creato in base a una politica di backup a livello di organizzazione, le impostazioni di AWS Backup attivazione per l'account di gestione Organizations sostituiranno le impostazioni di opt-in di quell'account membro, ma solo per quel piano di backup.

Se l'account membro dispone anche di piani di backup a livello locale creati dagli utenti, questi seguiranno le impostazioni di consenso esplicito dell'account membro, senza riferimento alle impostazioni di consenso esplicito dell'account di gestione di Organizations.

Definizione di policy, sintassi delle policy ed ereditarietà delle policy

I seguenti argomenti sono documentati nella Guida per l'utente. AWS Organizations

- Policy di backup: consulta Policy di backup.
- Sintassi delle policy: consulta Sintassi ed esempi delle policy di backup.
- Ereditarietà per i tipi di policy di gestione: consulta Comprendere l'ereditarietà delle policy di gestione.

AWS Backup e AWS CloudFormation

In generale

Con AWS CloudFormation, è possibile eseguire il provisioning e gestire le risorse AWS in modo sicuro e ripetibile utilizzando i modelli creati. Puoi utilizzare i modelli di AWS CloudFormation e StackSets per gestire i piani di backup, le selezioni delle risorse di backup e i vault di backup. Per informazioni sull'utilizzo di AWS CloudFormation, consulta Come funziona AWS CloudFormation? nella Guida per l'utente di AWS CloudFormation.

Prima di creare il modello di AWS CloudFormation o StackSet, considera quanto segue:

- Crea modelli separati per i piani di backup e i vault di backup. Puoi eliminare solo i vault di backup vuoti. Non puoi eliminare uno stack che include vault di backup se questi contengono punti di ripristino.
- Verifica di avere un ruolo di servizio disponibile prima di creare lo stack. Il ruolo di servizio AWS Backup predefinito viene creato automaticamente la prima volta che si assegnano risorse a un piano di backup. Se non sono state assegnate risorse al piano di backup, farlo prima di creare lo stack. Puoi inoltre specificare un ruolo personalizzato che hai creato. Per ulteriori informazioni sui ruoli, consulta Ruoli di servizio IAM.

Implementazione di un vault di backup, di un piano di backup e di assegnazione delle risorse utilizzando AWS CloudFormation

Per modelli di AWS CloudFormation di esempio che distribuiscono un vault di backup, piani di backup e l'assegnazione delle risorse, consulta Assegnazione di risorse utilizzando AWS CloudFormation.

Implementazione di piani di backup mediante AWS CloudFormation

Per modelli di AWS CloudFormation di esempio che distribuiscono piani di backup, consulta Modelli di AWS CloudFormation per piani di backup.

Implementazione di framework e piani di report di AWS Backup Audit Manager utilizzando AWS CloudFormation.

Per modelli di AWS CloudFormation di esempio che distribuiscono framework e piani di report di AWS Backup Audit Manager, consulta Modelli di AWS CloudFormation per piani di backup.

Implementazione di piani di backup su più account mediante AWS CloudFormation

Puoi utilizzare AWS CloudFormation StackSets su più account in una AWS Organization. I modelli di esempio sono disponibili nella Guida per l'utente di AWS CloudFormation.

Un ottimo punto di partenza e di riferimento è la pubblicazione Automate centralized backup at scale across AWS services using AWS Backup. Con Ibukun Oyewumi e Sabith Venkitachalapathy (luglio 2.021).

Ulteriori informazioni su AWS CloudFormation

Per informazioni sull'utilizzo di AWS CloudFormation con AWS Backup, consulta AWS Backup Resource Type Reference nella Guida per l'utente di AWS CloudFormation.

Per informazioni sul controllo dell'accesso alle risorse del servizio AWS durante l'utilizzo di AWS CloudFormation, consulta Controllo degli accessi con AWS Identity and Access Management nella Guida per l'utente di AWS CloudFormation.

Sicurezza in AWS Backup

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 Backup, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la responsabilità dell'utente AWS Backup include, a titolo esemplificativo ma non esaustivo, quanto segue. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, nonché le leggi e le normative applicabili.
  - Rispondere alle comunicazioni ricevute da AWS.
  - Gestione delle credenziali utilizzate dall'utente e dal suo team. Per ulteriori informazioni, vedere Gestione delle identità e degli accessi in AWS Backup.
  - Configurazione dei piani di backup e dell'assegnazione delle risorse per riflettere le policy di protezione dei dati aziendali dell'organizzazione. Per ulteriori informazioni, consulta Gestione dei piani di backup.
  - Verifica regolarmente la tua capacità di individuare specifici punti di ripristino e di ripristinarli. Per ulteriori informazioni, consulta Utilizzo dei backup.
  - Incorporazione di AWS Backup procedure nelle procedure scritte di disaster recovery e continuità aziendale dell'organizzazione. Per un punto di partenza, consulta Guida introduttiva a AWS Backup.
  - Garantire che i dipendenti conoscano e si siano esercitati AWS Backup a utilizzare le procedure organizzative in caso di emergenza. Per ulteriori informazioni, visitare il sito AWS Well-Architected Framework.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Backup. I seguenti argomenti mostrano come eseguire la configurazione AWS Backup

per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS Backup le tue risorse.

Argomenti

Convalida della conformità per AWS Backup

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS 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:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Architecting for HIPAA Security and Compliance on Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni idonee all'HIPAA. AWS

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la 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)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: 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— 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.

Protezione dei dati in AWS Backup

AWS Backup 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 AWS partner del Partner Network (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 configurare account utente individuali con AWS Identity and Access Management (IAM). In questo modo a ogni utente vengono assegnate solo le autorizzazioni necessarie per svolgere il proprio lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza il protocollo Secure Sockets Layer (SSL)/Transport Layer Security (TLS) per comunicare con le risorse AWS .
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi.

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 lavori con AWS Backup o altri AWS servizi che utilizzano la console, l'API o AWS gli SDK. AWS CLI Gli eventuali dati immessi in AWS Backup 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.

Crittografia per i backup in AWS Backup

> **Note**
>
> AWS Backup Audit Manager consente di rilevare automaticamente i backup non crittografati.

È possibile configurare la crittografia per i tipi di risorse che supportano la AWS Backup gestione completa nell'utilizzo. AWS Backup Se il tipo di risorsa non supporta la AWS Backup gestione completa, devi configurarne la crittografia di backup seguendo le istruzioni del servizio, come la crittografia Amazon EBS nella Amazon Elastic Compute Cloud User Guide. Per visualizzare l'elenco dei tipi di risorse che supportano la AWS Backup gestione completa, consulta la sezione « AWS Backup Gestione completa» della Disponibilità delle funzionalità per risorsa tabella.

Nella tabella seguente sono elencati i vari tipi di risorsa supportati e viene indicato il modo in cui la crittografia viene configurata per i backup e se è supportata la crittografia indipendente per i backup. Quando AWS Backup esegue la crittografia di un backup in modo indipendente, utilizza l'algoritmo di crittografia AES-256 standard del settore.

Tipo di risorsa	Come configurare la crittografia	AWS Backup Crittografia indipendente
Amazon Simple Storage Service (Amazon S3)	I backup di Amazon S3 sono crittografati utilizzando una chiave AWS KMS (AWS Key Management Service) associata al backup vault. La chiave AWS KMS può essere una CMK gestita dal cliente o una AWS CMK gestita dal servizio. AWS Backup AWS Backup crittografa tutti i backup anche se i bucket Amazon S3 di origine non sono crittografati.	Supportato
Macchine virtuali VMware	I backup delle macchine virtuali sono sempre crittografati. La chiave di AWS KMS crittografia per i backup delle macchine virtuali è configurata nell' AWS Backup archivio in cui sono archiviati i backup delle macchine virtuali.	Supportato
Amazon DynamoDB dopo l'attivazione Backup di DynamoDB avanzato	I backup di DynamoDB sono sempre crittografati. La chiave di AWS KMS crittografia per i backup DynamoDB è configurata nel AWS Backup	Supportato

Tipo di risorsa	Come configurare la crittografia	AWS Backup Crittografia indipendente
	vault in cui sono archiviati i backup DynamoDB.	
Amazon DynamoDB senza abilitazione Backup di DynamoDB avanzato	I backup di DynamoDB sono crittografati automaticamente con la stessa chiave crittografica utilizzata per crittografare la tabella DynamoDB di origine. Gli snapshot delle tabelle DynamoDB non crittografati non sono a loro volta crittografati. **Note** AWS Backup Per creare un backup di una tabella DynamoDB crittografata, è necessario aggiungere le `kms:Decrypt` autorizzazioni `kms:GenerateDataKey` e il ruolo IAM utilizzato per il backup. In alternativa, è possibile utilizzare il ruolo di servizio predefinito. AWS Backup	Non supportato

Tipo di risorsa	Come configurare la crittografia	AWS Backup Crittografia indipendente
Amazon Elastic File System (Amazon EFS)	I backup di Amazon EFS sono sempre crittografati. La chiave di AWS KMS crittografia per i backup di Amazon EFS è configurata nel AWS Backup vault in cui sono archiviati i backup di Amazon EFS.	Supportato
Amazon Elastic Block Store (Amazon EBS)	Per impostazione predefinita, i backup di Amazon EBS sono crittografati utilizzando la chiave utilizzata per crittografare il volume di origine oppure non sono crittografati. Durante il ripristino, puoi scegliere di sostituire il metodo di crittografia predefinito specificando una chiave KMS.	Non supportato
AMI Amazon Elastic Compute Cloud (Amazon EC2)	Le AMI non sono crittografate. Le istantanee EBS sono crittografate secondo le regole di crittografia predefinite per i backup EBS (vedi la voce relativa a EBS). Le istantanee EBS di dati e volumi root possono essere crittografate e collegate a un'AMI.	Non supportato

Tipo di risorsa	Come configurare la crittografia	AWS Backup Crittografia indipendente
Amazon Relational Database Service (Amazon RDS)	Gli snapshot di Amazon RDS vengono crittografati automaticamente con la stessa chiave di crittografia utilizzata per crittografare il database Amazon RDS di origine. Gli snapshot dei database di Amazon RDS non crittografati non sono a loro volta crittografati. **Note** AWS Backup attualmente supporta tutti i motori di database Amazon RDS, incluso Amazon Aurora.	Non supportato
Amazon Aurora	Gli snapshot dei cluster Aurora vengono crittografati automaticamente con la stessa chiave di crittografia utilizzata per crittografare il cluster Amazon Aurora di origine. Gli snapshot dei cluster Aurora non crittografati non sono a loro volta crittografati.	Non supportato

Tipo di risorsa	Come configurare la crittografia	AWS Backup Crittografia indipendente
AWS Storage Gateway	Gli snapshot di Storage Gateway svengono crittografati automaticamente con la stessa chiave di crittografia utilizzata per crittografare il volume Storage Gateway di origine. Gli snapshot dei volumi di Storage Gateway non crittografati non sono a loro volta crittografati. **Note** Per abilitare Storage Gateway non è necessario utilizzare una chiave gestita dal cliente in tutti i servizi. È sufficiente copiare il backup di Storage Gateway in un vault per il quale è stata configurata una chiave KMS. Questo perché Storage Gateway non dispone di una chiave AWS KMS gestita specifica per il servizio.	Non supportato

Tipo di risorsa	Come configurare la crittografia	AWS Backup Crittografia indipendente
Amazon FSx	Le funzionalità di crittografia per i file system Amazon FSx differiscono in base al file system sottostante. Per ulteriori informazioni su un particolare file system di Amazon FSx, consulta la Guida per l'utente FSx appropriata.	Non supportato
Amazon DocumentDB	Gli snapshot dei cluster Amazon DocumentDB vengono crittografati automaticamente con la stessa chiave di crittografia utilizzata per crittografare il cluster Amazon DocumentDB di origine. Gli snapshot dei cluster Amazon DocumentDB non crittografati non sono a loro volta crittografati.	Non supportato
Amazon Neptune	Gli snapshot dei cluster Neptune vengono crittografati automaticamente con la stessa chiave di crittografia utilizzata per crittografare il cluster Neptune di origine. Gli snapshot dei cluster Neptune non crittografati non sono a loro volta crittografati.	Non supportato

Tipo di risorsa	Come configurare la crittografia	AWS Backup Crittografia indipendente
Amazon Timestream	I backup degli snapshot delle tabelle Timestream sono sempre crittografati. La chiave crittografica di AWS KMS per i backup di Timestream è configurata nel vault di backup in cui sono archiviati i backup di Timestream.	Supportato
Amazon Redshift	Gli snapshot dei cluster Amazon Redshift vengono crittografati automaticamente con la stessa chiave di crittografia utilizzata per crittografare il cluster Amazon Redshift di origine. Gli snapshot dei cluster Amazon Redshift non crittografati non sono a loro volta crittografati.	Non supportato
AWS CloudFormation	CloudFormation i backup sono sempre crittografati. La chiave di CloudFormation crittografia per i CloudFormation backup è configurata nell' CloudFormation archivio in cui sono archiviati i CloudFormation backup.	Supportato

Tipo di risorsa	Come configurare la crittografia	AWS Backup Crittografia indipendente
Database SAP HANA su istanze Amazon EC2	I backup dei database SAP HANA sono sempre crittografati. La chiave di AWS KMS crittografia per i backup del database SAP HANA è configurata nell' AWS Backup archivio in cui sono archiviati i backup del database.	Supportato

Crittografia per le copie di backup

Quando si utilizza AWS Backup per copiare i backup tra account o regioni, crittografa AWS Backup automaticamente tali copie per la maggior parte dei tipi di risorse, anche se il backup originale non è crittografato. AWS Backup crittografa la tua copia utilizzando la chiave KMS del vault di destinazione. Tuttavia, anche le istantanee dei cluster Aurora, Amazon DocumentDB e Neptune non crittografate non sono crittografate.

Copie di crittografia e backup

La copia su più account con chiavi KMS AWS gestite non è supportata per le risorse che non sono completamente gestite da. AWS Backup Fai riferimento a Gestione completa AWS Backup per determinare quali risorse sono completamente gestite.

Per le risorse completamente gestite da AWS Backup, i backup sono crittografati con la chiave di crittografia del backup vault. Per le risorse che non sono completamente gestite da AWS Backup, le copie tra account utilizzano la stessa chiave KMS della risorsa di origine. Per ulteriori informazioni, consulta Chiavi di crittografia e copie tra account

Crittografia delle credenziali dell'hypervisor delle macchine virtuali

Le macchine virtuali gestite da un hypervisor utilizzano AWS Backup Gateway per connettere i sistemi on-premise a AWS Backup. È importante che gli hypervisor dispongano di un sistema di sicurezza altrettanto solido e affidabile. Questa sicurezza può essere ottenuta crittografando l'hypervisor, tramite chiavi di AWS proprietà o tramite chiavi gestite dal cliente.

AWS chiavi possedute e gestite dal cliente

AWS Backup fornisce la crittografia delle credenziali dell'hypervisor per proteggere le informazioni sensibili di accesso dei clienti utilizzando chiavi di crittografia AWS proprietarie. In alternativa è possibile utilizzare chiavi gestite dal cliente.

Per impostazione predefinita, le chiavi utilizzate per crittografare le credenziali nell'hypervisor sono chiavi di proprietà.AWS AWS Backup utilizza queste chiavi per crittografare automaticamente le credenziali dell'hypervisor. Non è possibile visualizzare, gestire o utilizzare chiavi AWS di proprietà, né controllarne l'utilizzo. Tuttavia, non è necessario effettuare alcuna operazione o modificare programmi per proteggere le chiavi che eseguono la crittografia dei dati. Per ulteriori informazioni, consulta le chiavi AWS possedute nella Guida per AWS KMS gli sviluppatori.

In alternativa, le credenziali possono essere crittografate utilizzando chiavi gestite dal cliente. AWS Backup supporta l'uso di chiavi simmetriche gestite dal cliente create, possedute e gestite dall'utente per eseguire la crittografia. Poiché hai il pieno controllo di questo tipo di crittografia, puoi eseguire attività come:

- Stabilire e mantenere le policy relative alle chiavi
- Stabilire e mantenere le policy e le sovvenzioni IAM
- Abilitare e disabilitare le policy delle chiavi
- Ruotare i materiali crittografici delle chiavi
- Aggiungere tag
- Creare alias delle chiavi
- Pianificare l’eliminazione delle chiavi

Quando utilizzi una chiave gestita dal cliente, AWS Backup verifica se il tuo ruolo è autorizzato a decrittografare utilizzando questa chiave (prima dell'esecuzione di un processo di backup o ripristino). Per avviare un processo di backup o ripristino è necessario aggiungere l'azione `kms:Decrypt` al ruolo utilizzato.

Poiché l'azione `kms:Decrypt` non può essere aggiunta al ruolo di backup predefinito, per utilizzare le chiavi gestite dal cliente è necessario utilizzare un ruolo diverso dal ruolo di backup predefinito.

Per ulteriori informazioni, consulta Chiavi gestite dal cliente nella Guida per gli sviluppatori di AWS Key Management Service .

Autorizzazione richiesta quando si utilizzano le chiavi gestite dal cliente

AWS KMS richiede una concessione per utilizzare la chiave gestita dal cliente. Quando importi una configurazione dell'hypervisor crittografata con una chiave gestita dal cliente, AWS Backup crea una concessione per tuo conto inviando una `CreateGrant`richiesta a. AWS KMS AWS Backup utilizza le concessioni per accedere a una chiave KMS in un account cliente.

Puoi revocare l'accesso alla concessione o rimuovere AWS Backup l'accesso alla chiave gestita dal cliente in qualsiasi momento. In tal caso, tutti i gateway associati all'hypervisor non potranno più accedere al nome utente e alla password dell'hypervisor crittografati dalla chiave gestita dal cliente, il che influirà sui processi di backup e ripristino. In particolare, i processi di backup e ripristino eseguiti sulle macchine virtuali in questo hypervisor avranno esito negativo.

Backup Gateway utilizza l'operazione `RetireGrant` per rimuovere un'autorizzazione quando si elimina un hypervisor.

Monitoraggio delle chiavi crittografiche

Quando utilizzi una chiave gestita AWS KMS dal cliente con AWS Backup le tue risorse, puoi utilizzare AWS CloudTrailAmazon CloudWatch Logs per tenere traccia delle richieste AWS Backup inviate a AWS KMS.

Cerca AWS CloudTrail gli eventi con i seguenti `"eventName"` campi per monitorare AWS KMS le operazioni chiamate AWS Backup ad accedere ai dati crittografati dalla chiave gestita dal cliente:

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

Gestione delle identità e degli accessi in AWS Backup

L'accesso a AWS Backup richiede credenziali. Tali credenziali devono essere dotate delle autorizzazioni per accedere alle risorse AWS , come ad esempio un database Amazon DynamoDB o un volume Amazon EFS. Inoltre, i punti di ripristino creati da AWS Backup per alcuni servizi AWS Backup supportati non possono essere eliminati utilizzando il servizio di origine (come Amazon EFS). Puoi eliminare questi punti di ripristino utilizzando AWS Backup.

Le seguenti sezioni forniscono dettagli su come utilizzare AWS Identity and Access Management (IAM) e su come AWS Backup proteggere l'accesso alle risorse.

> **Warning**
>
> AWS Backup utilizza lo stesso ruolo IAM che hai scelto per l'assegnazione delle risorse per gestire il ciclo di vita del punto di ripristino. Se elimini o modifichi quel ruolo, AWS Backup non puoi gestire il ciclo di vita del punto di ripristino. Quando ciò si verifica, proverà a utilizzare un ruolo collegato ai servizi per gestire il ciclo di vita. In una piccola percentuale di casi, inoltre, anche questa opzione potrebbe non funzionare, lasciando punti di ripristino di `EXPIRED` nello spazio di archiviazione, il che potrebbe comportare costi indesiderati. Per eliminare i punti di ripristino di `EXPIRED`, eliminali manualmente utilizzando la procedura descritta in Eliminazione dei backup.

Argomenti

Autenticazione

L'accesso AWS Backup o i AWS servizi di cui si sta eseguendo il backup richiedono credenziali che AWS possono essere utilizzate per autenticare le richieste. Puoi accedere AWS con uno qualsiasi dei seguenti tipi di identità:

- Account AWS utente root: quando ti registri AWS, fornisci un indirizzo email e una password associati al tuo AWS account. Questo è l'utente root dell'Account AWS . Le sue credenziali forniscono l'accesso completo a tutte le tue AWS risorse.

> **Important**
>
> Per motivi di sicurezza, si consiglia di utilizzare l'utente root solo per creare un amministratore. L'amministratore è un utente IAM con autorizzazioni complete per l'account Account AWS. Potrai quindi utilizzare questo utente amministratore per creare altri utenti e ruoli IAM con autorizzazioni limitate. Per ulteriori informazioni, consulta Best practice di IAM e Creazione del primo utente e gruppo di amministrazione di IAM nella Guida per l'utente di IAM.

- Utente IAM - Un utente IAM è un'identità all'interno dell' Account AWS dotato di autorizzazioni personalizzate specifiche (ad esempio quella di creare un vault di backup in cui archiviare i backup). Puoi utilizzare un nome utente e una password IAM per accedere a AWS pagine Web sicure come AWS Discussion Forums o Center. AWS Management ConsoleAWS Support

  Oltre a un nome utente e una password, è possibile anche generare chiavi di accesso per ciascun utente. È possibile utilizzare queste chiavi quando si accede ai AWS servizi in modo programmatico, tramite uno dei numerosi SDK o utilizzando (AWS Command Line InterfaceAWS CLI). L'SDK e gli strumenti AWS CLI utilizzano le chiavi di accesso per firmare crittograficamente la tua richiesta. Se non si utilizzano gli strumenti di AWS , è necessario firmare la richiesta personalmente. Per ulteriori informazioni sulle richieste di autenticazione, consulta la pagina relativa al processo di firma Signature Version 4 nella Riferimenti generali di AWS.
- Ruolo IAM - Un ruolo IAM è un'identità IAM che è possibile creare nell'account e che dispone di autorizzazioni specifiche. È simile a un utente IAM user, ma non è associato a una persona specifica. Un ruolo IAM consente di ottenere chiavi di accesso temporanee che possono essere utilizzate per accedere a servizi AWS e risorse. I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:
  - Accesso utente federato: invece di creare un utente IAM, puoi utilizzare identità utente preesistenti provenienti dalla AWS Directory Service tua directory utenti aziendale o da un provider di identità web. Sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando è richiesto l'accesso tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consulta la sezione relativa a utenti federati e ruoli nella Guida per l'utente di IAM.
  - Amministrazione su più account: puoi utilizzare un ruolo IAM nel tuo account per concedere altre Account AWS autorizzazioni per amministrare le risorse del tuo account. Per un esempio, consulta Tutorial: Delegate Access Across Account AWS Using IAM Roles nella IAM User Guide.

- AWS accesso al servizio: puoi utilizzare un ruolo IAM nel tuo account per concedere a un AWS servizio le autorizzazioni per accedere alle risorse del tuo account. Per ulteriori informazioni, consulta Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'utente IAM.
- Applicazioni in esecuzione su Amazon Elastic Compute Cloud (Amazon EC2): puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza Amazon EC2 e che effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Controllo accessi

È possibile disporre di credenziali valide per autenticare le richieste, ma a meno che non si disponga delle autorizzazioni appropriate, non è possibile accedere a AWS Backup risorse come gli archivi di backup. Inoltre, non è possibile eseguire il backup di AWS risorse come i volumi Amazon Elastic Block Store (Amazon EBS).

Ogni AWS risorsa è di proprietà di un Account AWS utente 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 AWS Identity and Access Management (IAM) (ovvero utenti, gruppi e ruoli). Anche alcuni servizi supportano il collegamento di policy di autorizzazione alle risorse.

> **Note**
>
> Un amministratore account (o un utente amministratore) è un utente con autorizzazioni di amministratore. Per ulteriori informazioni, consulta Best practice IAM nella Guida per l'utente di IAM.

Quando si concedono le autorizzazioni, è necessario specificare gli utenti che le riceveranno e le risorse per cui si concedono, nonché le operazioni specifiche da consentire su tali risorse.

Nelle sezioni seguenti viene descritto come funzionano le policy di accesso e come si utilizzano per proteggere i backup.

Argomenti

Risorse e operazioni

Una risorsa è un oggetto che esiste all'interno di un servizio. AWS Backup le risorse includono piani di backup, archivi di backup e backup. Backup è un termine generico che si riferisce ai vari tipi di risorse di backup esistenti in AWS. Ad esempio, gli snapshot Amazon EBS, gli snapshot Amazon Relational Database Service (Amazon RDS) e i backup Amazon DynamoDB sono tutti tipi di risorse di backup.

Nel AWS Backup, i backup vengono anche chiamati punti di ripristino. Durante l'utilizzo AWS Backup, lavori anche con le risorse di altri AWS servizi che stai cercando di proteggere, come i volumi Amazon EBS o le tabelle DynamoDB. A tali risorse sono associati Amazon Resource Names (ARN) univoci. Gli ARN identificano in modo univoco le risorse. AWS Quando è necessario specificare una risorsa in modo inequivocabile in tutto AWS, ad esempio nelle policy IAM o nelle chiamate API, è necessario indicare un ARN.

La tabella seguente elenca le risorse, le risorse secondarie, il formato ARN e un ID univoco di esempio.

AWS Backup ARN di risorse

Tipo di risorsa	Formato ARN	Esempio di ID univoco
Piano di backup	`arn:aws:backup:`*`region`*`:`*`account-id`*`:backup-plan:*`	

Tipo di risorsa	Formato ARN	Esempio di ID univoco
Vault di backup	`arn:aws:backup:`*`region`*`:`*`account-id`*`:backup-vault:*`	
Punto di ripristino per Amazon EBS	`arn:aws:ec2:`*`region`*`::snapshot/*`	`snapshot/snap-05f426fd8kdjb4224`
Punto di ripristino per immagini Amazon EC2	`arn:aws:ec2:`*`region`*`::image/ami-*`	`image/ami-1a2b3e4f5e6f7g890`
Punto di ripristino per Amazon RDS	`arn:aws:rds:`*`region`*`:`*`account-id`*`:snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Punto di ripristino per Aurora	`arn:aws:rds:`*`region`*`:`*`account-id`*`:cluster-snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Punto di ripristino per Storage Gateway	`arn:aws:ec2:`*`region`*`::snapshot/*`	`snapshot/snap-0d40e49137e31d9e0`
Punto di ripristino per DynamoDB senza Backup di DynamoDB avanzato	`arn:aws:dynamodb:`*`region`*`:`*`account-id`*`:table/*/backup/*`	`table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3`
Punto di ripristino per DynamoDB con Backup di DynamoDB avanzato abilitato	`arn:aws:backup:`*`region`*`:`*`account-id`*`:recovery-point:*`	`12a34a56-7bb8-901c-cd23-4567d8e9ef01`

Tipo di risorsa	Formato ARN	Esempio di ID univoco
Punto di ripristino per Amazon EFS	`arn:aws:backup:region:account-id:recovery-point:*`	`d99699e7-e183-477e-bfcd-ccb1c6e5455e`
Punto di ripristino per Amazon FSx	`arn:aws:fsx:region:account-id:backup/backup-*`	`backup/backup-1a20e49137e31d9e0`
Punto di ripristino per macchina virtuale	`arn:aws:backup:region:account-id:recovery-point:*`	`1801234a-5b6b-7dc8-8032-836f7ffc623b`
Punto di ripristino per il backup continuo di Amazon S3	`arn:aws:backup:region:account-id:recovery-point:*`	`my-bucket -5ec207d0`
Punto di ripristino per il backup periodico S3	`arn:aws:backup:region:account-id:recovery-point:*`	`my-bucket -20211231900000-5ec207d0`
Punto di ripristino per Amazon DocumentDB	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Punto di ripristino per Neptune	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Punto di ripristino per Amazon Redshift	`arn:aws:redshift:region:account-id:snapshot:resource/awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`

Tipo di risorsa	Formato ARN	Esempio di ID univoco
Punto di ripristino per Amazon Timestream	`arn:aws:backup:` *`region`*`:`*`account-id`*` :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta`
Punto di ripristino per il modello AWS CloudFormation	`arn:aws:backup:` *`region`*`:`*`account-id`*` :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`
Punto di ripristino per il database SAP HANA sull'istanza Amazon EC2	`arn:aws:backup:` *`region`*`:`*`account-id`*` :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`

Le risorse che supportano la AWS Backup gestione completa dispongono tutte di punti di ripristino in questo formato, il che semplifica l'applicazione delle politiche di autorizzazione per proteggere tali punti di ripristino`arn:aws:backup:`*`region`*`:`*`account-id:`*`:recovery-point:*`. Per vedere quali risorse supportano la AWS Backup gestione completa, consulta la sezione corrispondente della Disponibilità delle funzionalità per risorsa tabella.

AWS Backup fornisce una serie di operazioni per l'utilizzo delle AWS Backup risorse. Per un elenco di operazioni disponibili, consulta la sezione AWS Backup Azioni.

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'utente Account AWS 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 tue credenziali utente Account AWS root Account AWS per creare un archivio di backup, sei il Account AWS proprietario del vault.
- Se crei un utente IAM nel tuo account Account AWS e concedi le autorizzazioni per creare un archivio di backup a quell'utente, l'utente può creare un archivio di backup. Tieni presente, tuttavia, che l' AWS a cui appartiene l'utente è il proprietario della risorsa vault di backup.

- Se crei un ruolo IAM in tuo Account AWS possesso delle autorizzazioni necessarie per creare un vault di backup, chiunque possa assumere il ruolo può creare un vault. Il tuo Account AWS, a cui appartiene il ruolo, possiede la risorsa del vault di backup.

Specificare elementi delle policy: azioni, effetti e principali

Per ogni AWS Backup risorsa (vediRisorse e operazioni), il servizio definisce un insieme di operazioni API (vediAzioni). Per concedere le autorizzazioni per queste operazioni API, AWS Backup definisce una serie di azioni che è possibile specificare in una politica. L'esecuzione di un'operazione API può richiedere le autorizzazioni per più di un'operazione.

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.
- Operazione: utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare.
- Effetto: l'effetto prodotto quando l'utente richiede l'operazione specifica, ovvero un'autorizzazione o un rifiuto. USe 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.
- Principale - Nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse).

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consulta Riferimento alle policy JSON IAM nella Guida per l'utente di IAM.

Per una tabella che mostra tutte le azioni dell' AWS Backup API, consultaAutorizzazioni API: riferimenti a operazioni, 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.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

AWS Backup definisce il proprio set di chiavi di condizione. Per visualizzare un elenco di chiavi di AWS Backup condizione, vedere Condition keys for AWS Backup nel Service Authorization Reference.

Autorizzazioni API: riferimenti a operazioni, risorse e condizioni

Quando configuri il Controllo accessi 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. L' include ogni operazione AWS Backup API, le azioni corrispondenti per le quali è possibile concedere le autorizzazioni per eseguire l'azione e 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`. Se il campo `Resource` è vuoto, puoi usare il carattere jolly (*) per includere tutte le risorse.

Puoi utilizzare i tasti AWS-wide condition nelle tue AWS Backup politiche per esprimere condizioni. Per un elenco completo delle chiavi AWS-wide, consulta Available Keys nella IAM User Guide.

[1] Utilizza la politica di accesso al vault esistente.

[2] Per informazioni sugli ARN AWS Backup ARN di risorse dei punti di ripristino specifici per le risorse, vedere.

[3] `StartRestoreJob` deve avere la coppia chiave-valore nei metadati della risorsa. Per ottenere i metadati della risorsa, richiamare l'API `GetRecoveryPointRestoreMetadata`.

[4] Alcuni tipi di risorse richiedono che il ruolo che esegue il backup disponga di un'autorizzazione specifica per l'etichettatura `backup:TagResource` se si prevede di includere i tag delle risorse originali nel backup o di aggiungere tag aggiuntivi a un backup. Qualsiasi backup con un ARN che inizia `arn:aws:backup:`*`region`*`:`*`account-id`*`:recovery-point:` con o un backup continuo richiede questa autorizzazione. `backup:TagResource`l'autorizzazione deve essere applicata a `"`*`resourcetype`*`": "arn:aws:backup:`*`region`*`:`*`account-id:`*`recovery-point:*"`

Per ulteriori informazioni, consulta Operazioni, risorse e chiavi di condizione per AWS Backup nella Documentiazione di riferimento per l'autorizzazione al servizio.

Autorizzazioni di copia di tag

Quando AWS Backup esegue un processo di backup o copia, tenta di copiare i tag dalla risorsa di origine (o dal punto di ripristino in caso di copia) al punto di ripristino.

> **Note**
>
> AWS Backup non copia nativamente i tag durante i processi di ripristino. Per un'architettura basata sugli eventi che copierà i tag durante i processi di ripristino, vedi Come conservare i tag delle risorse nei AWS Backup processi di ripristino.

Durante un processo di backup o copia, AWS Backup aggrega i tag specificati nel piano di backup (o piano di copia o backup su richiesta) con i tag della risorsa di origine. Tuttavia, AWS impone un limite di 50 tag per risorsa, che AWS Backup non può essere superato. Quando un processo di backup o copia aggrega i tag dal piano e dalla risorsa di origine, potrebbe rilevare più di 50 tag in totale. In questo caso non sarà in grado di completare il processo ed esso fallirà. Ciò è coerente con le migliori pratiche AWS di etichettatura a livello globale. Per ulteriori informazioni, consulta Limiti dei tag nella Guida di riferimento generale di AWS .

- La tua risorsa ha più di 50 tag dopo aver aggregato i tag dei job di backup con i tag delle risorse di origine. AWS supporta fino a 50 tag per risorsa. Per ulteriori informazioni, consulta la pagina relativa ai Limiti dei tag.
- Il ruolo IAM a cui fornisci AWS Backup non dispone delle autorizzazioni per leggere i tag di origine o impostare i tag di destinazione. Per ulteriori informazioni e esempi di policy relative ai ruoli IAM, consulta Policy gestite.

Puoi utilizzare il tuo piano di backup per creare tag che contraddicano i tag delle risorse di origine. Quando i due sono in conflitto, i tag del piano di backup hanno la precedenza. Utilizza questa tecnica se preferisci non copiare il valore di un tag dalla risorsa di origine. Specificate la stessa chiave di tag, ma un valore diverso o vuoto, utilizzando il piano di backup.

Autorizzazioni necessarie per assegnare tag ai backup

Tipo di risorsa	Autorizzazione richiesta
File system Amazon EFS	`elasticfilesystem:DescribeTags`

Tipo di risorsa	Autorizzazione richiesta
File system Amazon FSx	`fsx:ListTagsForResource`
Database Amazon RDS for MySQL e cluster Amazon Aurora	`rds:AddTagsToResource` `rds:ListTagsForResource`
Volume Storage Gateway	`storagegateway:ListTagsForResource`
Istanza Amazon EC2 e volume EBS	`EC2:CreateTags` `EC2:DescribeTags`

DynamoDB non supporta l'assegnazione di tag ai backup a meno che non venga prima abilitato Backup di DynamoDB avanzato.

Quando un backup Amazon EC2 crea un Image Recovery Point e un set di snapshot, AWS Backup copia i tag nell'AMI risultante. AWS Backup copia inoltre i tag dai volumi associati all'istanza Amazon EC2 negli snapshot risultanti.

Policy di accesso

La policy delle autorizzazioni descrive chi ha accesso a cosa. Le policy collegate a un'identità IAM vengono definite policy basate su identità (policy IAM). Le politiche associate a una risorsa vengono chiamate politiche basate sulle risorse. AWS Backup supporta sia politiche basate sull'identità che politiche basate sulle risorse.

> **Note**
>
> Questa sezione illustra l'utilizzo di IAM nel contesto di. AWS Backup 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 JSON IAM nella Guida per l'utente di IAM.

Policy basate su identità (policy IAM)

Le policy basate su identità sono policy che si possono collegare a identità IAM, come utenti o ruoli. Ad esempio, è possibile definire una policy che consenta a un utente di visualizzare ed eseguire il backup AWS delle risorse, ma che impedisca loro di ripristinare i backup.

Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consulta Identità (utenti, gruppi e ruoli) nella Guida per l'utente di IAM.

Per ulteriori informazioni su come utilizzare le policy IAM per controllare l'accesso ai backup, consulta Politiche gestite per AWS Backup.

Policy basate su risorse

AWS Backup supporta politiche di accesso basate sulle risorse per gli archivi di backup. Questo permette di definire una policy di accesso che possa controllare di quali tipi di accesso a uno qualsiasi dei backup organizzati in un vault di backup dispongono gli utenti. Le policy di accesso basate su risorse per i vault di backup offrono un modo semplice per controllare l'accesso ai backup.

Le policy di accesso di Backup Vault controllano l'accesso degli utenti quando si utilizzano le AWS Backup API. È possibile accedere ad alcuni tipi di backup, ad esempio gli snapshot di Amazon Elastic Block Store (Amazon EBS) e Amazon Relational Database Service (Amazon RDS), utilizzando le API di tali servizi. È possibile creare policy di accesso separate in IAM che controllano l'accesso alle API per avere il controllo completo dell'accesso ai backup.

Per informazioni su come creare una policy di accesso per i vault di backup, consulta Imposta le policy di accesso ai vault di backup.

Ruoli di servizio IAM

Un ruolo AWS Identity and Access Management (IAM) è simile a quello di un utente, in quanto è un' AWS identità con politiche di autorizzazione che determinano ciò che l'identità può e non può fare. AWS Tuttavia, invece di essere associato in modo univoco a una persona, un ruolo è destinato a essere assunto da chiunque. Un ruolo di servizio è un ruolo che un AWS servizio assume per eseguire azioni per conto dell'utente. In quanto servizio che esegue le operazioni di backup per tuo conto, è necessario trasferire a AWS Backup un ruolo da assumere durante l'esecuzione di operazioni di backup per tuo conto. Per ulteriori informazioni sui ruoli IAM, consulta Ruoli IAM nella Guida per l'utente di IAM.

Il ruolo a cui passi AWS Backup deve disporre di una policy IAM con le autorizzazioni che consentano di eseguire azioni associate AWS Backup alle operazioni di backup, come la creazione,

il ripristino o la scadenza dei backup. Sono necessarie autorizzazioni diverse per ciascuno dei servizi supportati. AWS AWS Backup Il ruolo deve inoltre essere AWS Backup elencato come entità attendibile, che consente di AWS Backup assumere il ruolo.

Quando si assegnano risorse a un piano di backup o se si esegue un backup, una copia o un ripristino su richiesta, è necessario assegnare un ruolo di servizio che abbia accesso all'esecuzione delle operazioni sottostanti sulle risorse specificate. AWS Backup utilizza questo ruolo per creare, etichettare ed eliminare risorse nel tuo account.

Utilizzo AWS dei ruoli per controllare l'accesso ai backup

È possibile utilizzare i ruoli per controllare l'accesso ai backup definendo i ruoli con ambito limitato e specificando chi può trasferire il ruolo a AWS Backup. Ad esempio, puoi creare un ruolo che conceda solo le autorizzazioni per il backup dei database Amazon Relational Database Service (Amazon RDS) e concedere solo ai proprietari di database Amazon RDS l'autorizzazione a passare quel ruolo. AWS Backup AWS Backup fornisce diverse politiche gestite predefinite per ciascuno dei servizi supportati. È possibile collegare queste policy gestite ai ruoli creati. Ciò semplifica la creazione di ruoli specifici del servizio con le autorizzazioni corrette necessarie. AWS Backup

Per ulteriori informazioni sulle politiche AWS gestite per AWS Backup, vedere. Politiche gestite per AWS Backup

Ruolo di servizio predefinito per AWS Backup

Quando si utilizza la AWS Backup console per la prima volta, è possibile scegliere di AWS Backup creare automaticamente un ruolo di servizio predefinito. Questo ruolo dispone delle autorizzazioni AWS Backup necessarie per creare e ripristinare i backup per tuo conto.

> **Note**
>
> Il ruolo predefinito viene creato automaticamente quando si utilizza la AWS Management Console. È possibile creare il ruolo predefinito utilizzando AWS Command Line Interface (AWS CLI), ma deve essere eseguito manualmente.

Se preferisci utilizzare ruoli personalizzati, come ruoli separati per diversi tipi di risorse, puoi anche farlo e passare i tuoi ruoli personalizzati a AWS Backup. Per visualizzare esempi di ruoli che abilitano il backup e il ripristino per singoli tipi di risorse, consulta la tabella Policy gestite dal cliente.

Il ruolo di servizio predefinito è denominato`AWSBackupDefaultServiceRole`. Questo ruolo di servizio contiene due politiche gestite AWSBackupServiceRolePolicyForBackupe AWSBackupServiceRolePolicyForRestores.

`AWSBackupServiceRolePolicyForBackup`include una policy IAM che concede AWS Backup le autorizzazioni per descrivere la risorsa di cui viene eseguito il backup, la possibilità di creare, eliminare, descrivere o aggiungere tag a un backup indipendentemente dalla AWS KMS chiave con cui è crittografato.

`AWSBackupServiceRolePolicyForRestores`include una policy IAM che concede AWS Backup le autorizzazioni per creare, eliminare o descrivere la nuova risorsa creata da un backup, indipendentemente dalla AWS KMS chiave con cui è crittografata. Include anche le autorizzazioni necessarie per applicare tag alla risorsa appena creata.

Per ripristinare un'istanza Amazon EC2, è necessario avviare una nuova istanza.

Creazione del ruolo di servizio predefinito nella console

Le azioni specifiche eseguite nella AWS Backup console creano il ruolo di servizio AWS Backup predefinito.

Per creare il ruolo di servizio AWS Backup predefinito nel tuo AWS account

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Per creare il ruolo per il tuo account, assegna le risorse a un piano di backup o crea un backup su richiesta.

    a. Creare un piano di backup e assegnare risorse al backup. Consulta Creazione di un backup pianificato.

    b. In alternativa, è possibile creare un backup su richiesta. Consulta Creazione di un backup su richiesta.
3. Verifica di aver creato `AWSBackupDefaultServiceRole` nel tuo account seguendo questi passaggi:

    a. Attendi alcuni minuti. Per ulteriori informazioni, consulta Le modifiche che apporto non sono sempre immediatamente visibili nella Guida per l'utente di AWS Identity and Access Management.

    b. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

c. Nel menu di navigazione a sinistra, scegliere Ruoli.

d. Nella casella di ricerca, digitare `AWSBackupDefaultServiceRole`. Se questa selezione esiste, hai creato il ruolo AWS Backup predefinito e completato questa procedura.

e. Se `AWSBackupDefaultServiceRole` ancora non viene visualizzato, aggiungi le seguenti autorizzazioni all'utente IAM o al ruolo IAM che utilizzi per accedere alla console.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource":"arn:aws:iam::*:role/service-role/AWSBackupDefaultServiceRole"
    },
    {
      "Effect":"Allow",
      "Action":[
        "iam:ListRoles"
      ],
      "Resource":"*"
    }
  ]
}
```

Per le regioni cinesi, sostituisci *aws* con *aws-cn*. Per AWS GovCloud (US) le regioni, sostituisci *aws* con *aws-us-gov*.

f. Se non riesci ad aggiungere autorizzazioni al tuo utente IAM o al tuo ruolo IAM, chiedi all'amministratore di creare manualmente un ruolo con un nome diverso da `AWSBackupDefaultServiceRole` e associarlo a queste policy gestite:

- `AWSBackupServiceRolePolicyForBackup`
- `AWSBackupServiceRolePolicyForRestores`

Politiche gestite per AWS Backup

Le politiche gestite sono politiche autonome basate sull'identità che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Quando si allega una policy a un'entità principale, è necessario fornire all'entità le autorizzazioni definite nella policy.

AWS le politiche gestite vengono create e amministrate da. AWS Non è possibile modificare le autorizzazioni definite nelle politiche AWS gestite. Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica.

Le policy gestite dai clienti offrono controlli granulari per impostare l'accesso ai backup. AWS Backup Ad esempio, puoi utilizzarle per consentire all'amministratore di backup del database di accedere ai backup di Amazon RDS ma non a quelli di Amazon EFS.

Per ulteriori informazioni, consulta Managed policy nella IAM User Guide.

AWS politiche gestite

AWS Backup fornisce le seguenti politiche AWS gestite per casi d'uso comuni. Queste policy consentono di definire le autorizzazioni appropriate e di controllare l'accesso ai backup. Sono disponibili due tipi i policy gestite. Un tipo è stato progettato per essere assegnato agli utenti per controllare il proprio accesso a AWS Backup. L'altro tipo di policy gestita è stato progettato per essere collegato ai ruoli che vengono passati a AWS Backup. La tabella seguente elenca tutte le policy gestite che AWS Backup offre e spiega come vengono definite. Puoi trovare queste policy gestite nella sezione Policy della console IAM.

Policy

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest

- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

Questa politica concede agli utenti le autorizzazioni per creare controlli e framework che definiscono le loro aspettative in termini di AWS Backup risorse e attività e per controllare AWS Backup risorse e attività rispetto ai controlli e ai framework definiti. Questa politica concede autorizzazioni AWS Config e servizi simili per descrivere le aspettative degli utenti, eseguire gli audit.

Questa policy concede inoltre le autorizzazioni per fornire report di audit ad Amazon S3 e a servizi simili e consente agli utenti di trovare e aprire i propri report di controllo.

Per visualizzare le autorizzazioni relative a questa politica, consulta il Managed Policy AWSBackupAuditAccessReference.AWS

AWSBackupDataTransferAccess

Questa policy fornisce le autorizzazioni per le API di trasferimento dei dati del piano di AWS Backup archiviazione, permettendo all'agente AWS Backint di completare il trasferimento dei dati di backup con il piano di storage. AWS Backup Puoi collegare questa policy ai ruoli assunti dalle istanze Amazon EC2 che eseguono SAP HANA con l'agente Backint.

Per visualizzare le autorizzazioni per questa politica, consulta AWSBackupDataTransferAccessil Managed Policy Reference.AWS

AWSBackupFullAccess

L'amministratore di backup ha pieno accesso alle AWS Backup operazioni, tra cui la creazione o la modifica dei piani di backup, l'assegnazione di AWS risorse ai piani di backup e il ripristino dei backup. Gli amministratori di backup sono responsabili di stabilire e di applicare la conformità dei backup definendo piani di backup che soddisfino i requisiti normativi e aziendali dell'organizzazione. Gli amministratori di Backup assicurano inoltre che AWS le risorse della propria organizzazione siano assegnate al piano appropriato.

Per visualizzare le autorizzazioni relative a questa policy, consulta AWSBackupFullAccessil AWS Managed Policy Reference.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Per visualizzare le autorizzazioni per questa politica, consulta il AWS Managed Policy Reference.

AWSBackupOperatorAccess

Gli operatori di backup sono utenti che hanno la responsabilità di garantire il backup delle risorse di cui sono responsabili venga eseguito correttamente. Gli operatori di backup dispongono delle autorizzazioni per assegnare AWS risorse ai piani di backup creati dall'amministratore di backup. Dispongono inoltre delle autorizzazioni per creare backup su richiesta delle proprie AWS risorse e per configurare il periodo di conservazione dei backup su richiesta. Non dispongono invece delle autorizzazioni per creare o modificare i piani di backup o per eliminare i backup pianificati dopo che sono stati creati. Gli operatori di backup possono ripristinare i backup. È possibile limitare i tipi di risorse che un operatore di backup può assegnare a un piano di backup o ripristinare da un backup. A tale scopo, è possibile passare solo determinati ruoli di servizio a cui sono consentite le autorizzazioni per AWS Backup un determinato tipo di risorsa.

Per visualizzare le autorizzazioni per questa politica, consulta AWSBackupOperatorAccessil AWS Managed Policy Reference.

AWSBackupOrganizationAdminAccess

L'amministratore dell'organizzazione ha pieno accesso alle AWS Organizations operazioni, tra cui la creazione, la modifica o l'eliminazione delle politiche di backup, l'assegnazione delle politiche di backup agli account e alle unità organizzative e il monitoraggio delle attività di backup all'interno dell'organizzazione. Gli amministratori dell'organizzazione sono responsabili della protezione degli account nell'organizzazione mediante la definizione e l'assegnazione di policy di backup che soddisfino i requisiti aziendali e normativi dell'organizzazione.

Per visualizzare le autorizzazioni relative a questa politica, consulta il AWS Managed Policy AWSBackupOrganizationAdminAccessReference.

AWSBackupRestoreAccessForSAPHANA

Questa policy consente di AWS Backup ripristinare un backup di SAP HANA su Amazon EC2.

Per visualizzare le autorizzazioni per questa politica, consulta il Managed Policy AWSBackupRestoreAccessForSAPHANAReference.AWS

AWSBackupServiceLinkedRolePolicyForBackup

Questa policy è associata al ruolo collegato al servizio denominato AWSServiceRoleforBackup per consentire di chiamare AWS i servizi AWS Backup per conto dell'utente per gestire i backup. Per ulteriori informazioni, consulta the section called “Backup e copia”.

Per visualizzare le autorizzazioni relative a questa policy, consulta il Managed Policy AWSBackupServiceLinkedRolePolicyforBackupReference.AWS

AWSBackupServiceLinkedRolePolicyForBackupTest

Per visualizzare le autorizzazioni per questa politica, consulta AWSBackupServiceLinkedRolePolicyForBackupTestil AWS Managed Policy Reference.

AWSBackupServiceRolePolicyForBackup

Fornisce AWS Backup le autorizzazioni per creare backup di tutti i tipi di risorse supportati per tuo conto.

Per visualizzare le autorizzazioni per questa politica, consulta il AWS Managed Policy AWSBackupServiceRolePolicyForBackupReference.

AWSBackupServiceRolePolicyForRestores

Fornisce AWS Backup le autorizzazioni per ripristinare i backup di tutti i tipi di risorse supportati per tuo conto.

Per visualizzare le autorizzazioni per questa politica, consulta il AWS Managed Policy AWSBackupServiceRolePolicyForRestoresReference.

Per il ripristino delle istanze EC2, devi includere anche le seguenti autorizzazioni per avviare l'istanza EC2:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
```

```
    ]
}
```

AWSBackupServiceRolePolicyForS3Backup

Questa policy contiene le autorizzazioni necessarie per eseguire il backup AWS Backup di qualsiasi bucket S3. Ciò include l'accesso a tutti gli oggetti in un bucket e a qualsiasi chiave associata. AWS KMS

Per visualizzare le autorizzazioni per questa politica, consulta AWSBackupServiceRolePolicyForS3Backupil AWS Managed Policy Reference.

AWSBackupServiceRolePolicyForS3Restore

Questa policy contiene le autorizzazioni necessarie per AWS Backup ripristinare un backup S3 in un bucket. Ciò include le autorizzazioni di lettura e scrittura per i bucket e l'utilizzo di qualsiasi AWS KMS chiave per quanto riguarda le operazioni S3.

Per visualizzare le autorizzazioni per questa politica, consulta il Managed Policy AWSBackupServiceRolePolicyForS3RestoreReference.AWS

AWSServiceRolePolicyForBackupReports

AWS Backup utilizza questa politica per il ruolo collegato al AWSServiceRoleForBackupReportsservizio. Questo ruolo collegato al servizio fornisce AWS Backup le autorizzazioni per monitorare e generare report sulla conformità delle impostazioni, dei job e delle risorse di backup con i framework.

Per visualizzare le autorizzazioni per questa politica, consulta AWSServiceRolePolicyForBackupReportsil Managed Policy Reference.AWS

AWSServiceRolePolicyForBackupRestoreTesting

Per visualizzare le autorizzazioni per questa politica, consulta AWSServiceRolePolicyForBackupRestoreTestingil AWS Managed Policy Reference.

Policy gestite dal cliente

Le sezioni seguenti descrivono le autorizzazioni di backup e ripristino consigliate per l'applicazione Servizi AWS e per quelle di terze parti supportate da. AWS BackupÈ possibile utilizzare le politiche

AWS gestite esistenti come modello durante la creazione di documenti di policy personalizzati e quindi personalizzarli per limitare ulteriormente l'accesso alle AWS risorse.

Amazon Aurora

Backup

Inizia con le seguenti affermazioni tratte da AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Ripristino

Inizia con la `RDSPermissions` dichiarazione di AWSBackupServiceRolePolicyForRestores.

Amazon DynamoDB

Backup

Inizia con le seguenti dichiarazioni di AWSBackupServiceRolePolicyForBackup:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Ripristino

Inizia con le seguenti affermazioni di AWSBackupServiceRolePolicyForRestores:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamoDBRestorePermissions`
- `KMSPermissions`

Amazon EBS

Backup

Inizia con le seguenti affermazioni di AWSBackupServiceRolePolicyForBackup:

- `EBSResourcePermissions`
- `EBSTagAndDeletePermissions`
- `EBSCopyPermissions`
- `EBSSnapshotTierPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Ripristino

Inizia con la `EBSPermissions` dichiarazione di AWSBackupServiceRolePolicyForRestores.

Aggiungi l'istruzione seguente.

```
{
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
},
```

Amazon EC2

Backup

Inizia con le seguenti dichiarazioni di AWSBackupServiceRolePolicyForBackup:

- `EBSCopyPermissions`
- `EC2CopyPermissions`
- `EC2Permissions`
- `EC2TagPermissions`

- `EC2ModifyPermissions`
- `EBSResourcePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Ripristino

Inizia con le seguenti affermazioni di AWSBackupServiceRolePolicyForRestores:

- `EBSPermissions`
- `EC2DescribePermissions`
- `EC2RunInstancesPermissions`
- `EC2TerminateInstancesPermissions`
- `EC2CreateTagsPermissions`

Aggiungi l'istruzione seguente.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Amazon EFS

Backup

Inizia con le seguenti affermazioni di AWSBackupServiceRolePolicyForBackup:

- `EFSPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Ripristino

Inizia con la `EFSPermissions` dichiarazione di AWSBackupServiceRolePolicyForRestores.

Amazon FSx

Backup

Inizia con le seguenti dichiarazioni di AWSBackupServiceRolePolicyForBackup:

- `FsxBackupPermissions`
- `FsxCreateBackupPermissions`
- `FsxPermissions`
- `FsxVolumePermissions`
- `FsxListTagsPermissions`
- `FsxDeletePermissions`
- `FsxResourcePermissions`
- `KMSPermissions`

Ripristino

Inizia con le seguenti affermazioni di AWSBackupServiceRolePolicyForRestores:

- `FsxPermissions`
- `FsxTagPermissions`
- `FsxBackupPermissions`
- `FsxDeletePermissions`
- `FsxDescribePermissions`
- `FsxVolumeTagPermissions`
- `FsxBackupTagPermissions`
- `FsxVolumePermissions`
- `DSPermissions`
- `KMSDescribePermissions`

Amazon RDS

Backup

Inizia con le seguenti affermazioni di AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Ripristino

Inizia con la `RDSPermissions` dichiarazione di AWSBackupServiceRolePolicyForRestores.

Amazon S3

Backup

Inizia consultando AWSBackupServiceRolePolicyForS3Backup.

Aggiungi gli `BackupVaultCopyPermissions` estratti conto `BackupVaultPermissions` e se devi copiare i backup su un altro account.

Ripristino

Inizia consultando AWSBackupServiceRolePolicyForS3Restore.

AWS Storage Gateway

Backup

Inizia con le seguenti dichiarazioni di AWSBackupServiceRolePolicyForBackup:

- `StorageGatewayPermissions`
- `EBSTagAndDeletePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Aggiungi l'istruzione seguente.

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
},
```

Ripristino

Inizia con le seguenti affermazioni di AWSBackupServiceRolePolicyForRestores:

- `StorageGatewayVolumePermissions`
- `StorageGatewayGatewayPermissions`
- `StorageGatewayListPermissions`

Macchina virtuale

Backup

Inizia con la `BackupGatewayBackupPermissions` dichiarazione di AWSBackupServiceRolePolicyForBackup.

Ripristino

Inizia con la `GatewayRestorePermissions` dichiarazione di AWSBackupServiceRolePolicyForRestores.

Backup crittografato

Per ripristinare un backup crittografato, puoi procedere in uno dei seguenti modi:

- Aggiungi il tuo ruolo alla lista consentita per la politica AWS KMS chiave
- Aggiungi le seguenti istruzioni da AWSBackupServiceRolePolicyForRestoresal tuo ruolo IAM per i ripristini:
  - `KMSDescribePermissions`
  - `KMSPermissions`
  - `KMSCreateGrantPermissions`

Aggiornamenti delle policy per AWS Backup

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Backup da quando questo servizio ha iniziato a tenere traccia di queste modifiche.

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	AWS Backup ha aggiunto l'autorizzazione `backup:TagResource` a questa politica. L'autorizzazione è necessaria per ottenere le autorizzazioni di etichettatura durante la creazione di un punto di ripristino.	17 maggio 2024
AWSBackupServiceRolePolicyForS3Backup: aggiornamento a una policy esistente	AWS Backup ha aggiunto l'autorizzazione `backup:TagResource` a questa politica. L'autorizzazione è necessaria per ottenere le autorizzazioni di etichettatura durante la creazione di un punto di ripristino.	17 maggio 2024
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	AWS Backup ha aggiunto l'autorizzazione `backup:TagResource` a questa politica. L'autorizzazione è necessaria per ottenere le autorizzazioni di etichettatura durante	17 maggio 2024

Modifica	Descrizione	Data
	la creazione di un punto di ripristino.	
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	È stata aggiunta l'autorizzazione `rds:DeleteDBInstanceAutomatedBackups` . Questa autorizzazione è necessaria per AWS Backup supportare il backup continuo e point-in-time-restore delle istanze Amazon RDS.	1 maggio 2024
AWSBackupFullAccess: aggiornamento a una policy esistente	AWS Backup ha aggiornato l'Amazon Resource Name (ARN) nell'autorizzazione `storagegateway:ListVolumes` da `arn:aws:storagegateway:*:*:gateway/*` a per `*` adattarsi a una modifica del modello API Storage Gateway.	1 maggio 2024
AWSBackupOperatorAccess: aggiornamento a una policy esistente	AWS Backup ha aggiornato l'Amazon Resource Name (ARN) nell'autorizzazione `storagegateway:ListVolumes` da `arn:aws:storagegateway:*:*:gateway/*` a per `*` adattarsi a una modifica del modello API Storage Gateway.	1 maggio 2024

Modifica	Descrizione	Data
AWSServiceRolePolicyForBackupRestoreTesting: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per descrivere ed elencare i punti di ripristino e le risorse protette al fine di condurre piani di test di ripristino:`backup:DescribeRecoveryPoint` , `backup:DescribeProtectedResource` `backup:ListProtectedResources` , e. `backup:ListRecoveryPointsByResource` È stata aggiunta l'autorizzazione `ec2:DescribeSnapshotTierStatus` a supportare lo storage a livello di archivio di Amazon EBS. È stata aggiunta l'autorizzazione `rds:DescribeDBClusterAutomatedBackups` a supportare i backup continui di Amazon Aurora. Sono state aggiunte le seguenti autorizzazioni per supportare i test di ripristino dei backup `redshift:DescribeClusters` di Amazon Redshift: e.	14 febbraio 2024

Modifica	Descrizione	Data
	`redshift:DeleteCluster` È stata aggiunta l'autorizzazione `timestream:DeleteTable` a supportare i test di ripristino dei backup di Amazon Timestream.	
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Aggiunte le autorizzazioni `ec2:DescribeSnapshotTierStatus` e. `ec2:RestoreSnapshotTier` Queste autorizzazioni sono necessarie per consentire agli utenti di ripristinare le risorse Amazon EBS archiviate AWS Backup dallo storage di archivio. Per il ripristino delle istanze EC2, devi includere anche le autorizzazioni come mostrato nella seguente istruzione di policy per avviare l'istanza EC2:	27 novembre 2023

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le autorizzazioni `ec2:DescribeSnapshotTierStatus` e `ec2:ModifySnapshotTier` il supporto di un'opzione di storage aggiuntiva per la transizione delle risorse di backup di Amazon EBS al livello di storage di archiviazione. Queste autorizzazioni sono necessarie affinché gli utenti abbiano la possibilità di trasferire le risorse Amazon EBS archiviate AWS Backup allo storage di archivio.	27 novembre 2023

Modifica	Descrizione	Data
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le autorizzazioni `ec2:DescribeSnapshotTierStatus` e `ec2:ModifySnapshotTier` il supporto di un'opzione di storage aggiuntiva per la transizione delle risorse di backup di Amazon EBS al livello di storage di archiviazione. Queste autorizzazioni sono necessarie affinché gli utenti abbiano la possibilità di trasferire le risorse Amazon EBS archiviate AWS Backup allo storage di archivio. Sono state aggiunte le autorizzazioni `rds:DescribeDBClusterSnapshots` `erds:RestoreDBClusterToPointInTime` , necessarie per PITR (point-in-time ripristini) dei cluster Aurora.	

Modifica	Descrizione	Data
AWSServiceRolePolicyForBackupRestoreTesting: nuova policy	Fornisce le autorizzazioni necessarie per eseguire i test di ripristino. Le autorizzazioni includono le azioni `list, read, and write` per i seguenti servizi da includere nei test di ripristino: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx for Lustre, FSx for Windows File Server, FSx for ONTAP, FSx for OpenZFS, Amazon Neptune, Amazon RDS e Amazon S3.	27 novembre 2023
AWSBackupFullAccess: aggiornamento a una policy esistente	Aggiunto `restore-testing.backup.amazonaws.com` a `IamPassRolePermissions` e `IamCreateServiceLinkedRolePermissions`. Questa aggiunta è necessaria per AWS Backup eseguire test di ripristino per conto dei clienti.	27 novembre 2023
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Sono state aggiunte le autorizzazioni `rds:DescribeDBClusterSnapshots` `erds:RestoreDBClusterToPointInTime`, necessarie per PITR (point-in-time ripristini) dei cluster Aurora.	6 settembre 2023

Modifica	Descrizione	Data
AWSBackupFullAccess: aggiornamento a una policy esistente	È stata aggiunta l'autorizzazione `rds:DescribeDBClusterAutomatedBackups`, necessaria per il backup e il point-in-time ripristino continui dei cluster Aurora.	6 settembre 2023
AWSBackupOperatorAccess: aggiornamento a una policy esistente	È stata aggiunta l'autorizzazione `rds:DescribeDBClusterAutomatedBackups`, necessaria per il backup e il point-in-time ripristino continui dei cluster Aurora.	6 settembre 2023

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	È stata aggiunta l'autorizzazione. `rds:DescribeDBClusterAutomatedBackups` Questa autorizzazione è necessaria per il AWS Backup supporto del backup e del point-in-time ripristino continui dei cluster Aurora. È stata aggiunta l'autorizzazione `rds:DeleteDBClusterAutomatedBackups` per consentire a AWS Backup Lifecycle di eliminare e dissociare i punti di ripristino continui di Amazon Aurora al termine di un periodo di conservazione. Questa autorizzazione è necessaria affinché il punto di ripristino Aurora eviti la transizione verso uno stato `EXIPIRED`. Aggiunta l'autorizzazione `rds:ModifyDBCluster` che consente di AWS Backup interagire con i cluster Aurora. Questa aggiunta consente agli utenti di abilitare o disabilitare i backup continui in base alle configurazioni desiderate.	6 settembre 2023

Modifica	Descrizione	Data
AWSBackupFullAccess: aggiornamento a una policy esistente	È stata aggiunta l'azione `ram:GetResourceShareAssociations` per concedere all'utente l'autorizzazione a ottenere associazioni di condivisione delle risorse per un nuovo tipo di archivio.	8 agosto 2023
AWSBackupOperatorAccess: aggiornamento a una policy esistente	È stata aggiunta l'azione `ram:GetResourceShareAssociations` per concedere all'utente l'autorizzazione a ottenere associazioni di condivisione delle risorse per un nuovo tipo di archivio.	8 agosto 2023
AWSBackupServiceRolePolicyForS3Backup: aggiornamento a una policy esistente	È stata aggiunta l'autorizzazione `s3:PutInventoryConfiguration` a migliorare la velocità delle prestazioni di backup utilizzando un bucket inventory.	1° agosto 2023

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per aggiungere tag `ec2:CreateTags` per ripristinare le risorse: `storagegateway:AddTagsToResource elasticfilesystem:TagResource` ,, solo `ec2:CreateAction` ciò include `RunInstances` o `CreateVolume fsx:TagResource` , e. `cloudformation:TagResource`	22 maggio 2023
AWSBackupAuditAccess: aggiornamento a una policy esistente	Ha sostituito la selezione delle risorse all'interno dell'API `config:DescribeCompliancebyConfigRule` con una risorsa wildcard per facilitare la selezione delle risorse da parte di un utente.	11 aprile 2023
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	È stata aggiunta la seguente autorizzazione per ripristinare Amazon EFS utilizzando una chiave gestita dal cliente:`kms:GenerateDataKeyWithoutPlaintext` . Questo aiuta a garantire che gli utenti dispongano delle autorizzazioni necessarie per ripristinare le risorse Amazon EFS.	27 marzo 2023

Modifica	Descrizione	Data
AWSServiceRolePolicyForBackupReports: aggiornamento a una policy esistente	Sono state aggiornate le `config:DescribeConfigRuleEvaluationStatus` azioni `config:DescribeConfigRules` and per consentire a AWS Backup Audit Manager di accedere alle regole gestite AWS Config da AWS Backup Audit Manager.	9 marzo 2023
AWSBackupServiceRolePolicyForS3Restore: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni: `kms:Decrypt` `s3:PutBucketOwnershipControls` , e `s3:GetBucketOwnershipControls` alla policy. `AWSBackupServiceRolePolicyForS3Restore` Queste autorizzazioni sono necessarie per supportare il ripristino degli oggetti quando la crittografia KMS viene utilizzata nel backup originale e per il ripristino degli oggetti quando la proprietà degli oggetti è configurata sul bucket originale anziché su ACL.	13 febbraio 2023

Modifica	Descrizione	Data
AWSBackupFullAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per pianificare i backup utilizzando i tag VMware delle macchine virtuali e per supportare la limitazione della larghezza di banda basata sulla pianificazione:,,,,, e. `backup-gateway:GetHypervisorPropertyMappings backup-gateway:GetVirtualMachine backup-gateway:PutHypervisorPropertyMappings backup-gateway:GetHypervisor backup-gateway:StartVirtualMachinesMetadataSync backup-gateway:GetBandwidthRateLimitSchedule backup-gateway:PutBandwidthRateLimitSchedule`	15 dicembre 2022

Modifica	Descrizione	Data
AWSBackupOperatorAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per pianificare i backup utilizzando i tag VMware delle macchine virtuali e per supportare la limitazione della larghezza di banda basata sulla pianificazione:,, e. `backup-gateway:GetHypervisorPropertyMappings` `backup-gateway:GetVirtualMachine` `backup-gateway:GetHypervisor` `backup-gateway:GetBandwidthRateLimitSchedule`	15 dicembre 2022
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync: nuova policy	Fornisce le autorizzazioni a AWS Backup Gateway per sincronizzare i metadati delle macchine virtuali nelle reti locali con Backup Gateway.	15 dicembre 2022

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare i processi di backup di Timestream:`timestream:StartAwsBackupJob` ,,,,,`timestream:GetAwsBackupStatus` , `timestream:ListTables` e. `timestream:ListDatabases` `timestream:ListTagsForResource` `timestream:DescribeTable` `timestream:DescribeDatabase` `timestream:DescribeEndpoints`	13 dicembre 2022

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare i processi di ripristino di Timestream:`timestream:StartAwsRestoreJob` ,,,,,`timestream:GetAwsRestoreStatus` , `timestream:ListTables` `timestream:ListTagsForResource` , `timestream:ListDatabases` e. `timestream:DescribeTable` `timestream:DescribeDatabase` `s3:GetBucketAcl` `timestream:DescribeEndpoints`	13 dicembre 2022
AWSBackupFullAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare le risorse Timestream:,, e. `timestream:ListTables` `timestream:ListDatabases` `s3:ListAllMyBuckets` `timestream:DescribeEndpoints`	13 dicembre 2022

Modifica	Descrizione	Data
AWSBackupOperatorAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare le risorse Timestream:,,, e. `timestream:ListDatabases timestream:ListTables s3:ListAllMyBuckets timestream:DescribeEndpoints`	13 dicembre 2022
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare le risorse Timestream:`timestream:ListDatabases` ,,,,, `timestream:ListTables timestream:ListTagsForResource` , `timestream:DescribeDatabase` e. `timestream:DescribeTable timestream:GetAwsBackupStatus timestream:GetAwsRestoreStatus timestream:DescribeEndpoints`	13 dicembre 2022

Modifica	Descrizione	Data
AWSBackupFullAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare le risorse Amazon Redshift`redshift:DescribeClusters` :`redshift:DescribeClusterSubnetGroups` ,,`redshift:DescribeNodeConfigurationOptions` ,`redshift:DescribeOrderableClusterOptions` ,`redshift:DescribeClusterParameterGroups` , `redshift:DescribeClusterTracks` `redshift:DescribeSnapshotSchedules` , e. `ec2:DescribeAddresses`	27 novembre 2022

Modifica	Descrizione	Data
AWSBackupOperatorAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare le risorse Amazon Redshift`redshift:DescribeClusters` :`redshift:DescribeClusterSubnetGroups` ,,,, `redshift:DescribeNodeConfigurationOptions` `redshift:DescribeOrderableClusterOptions` ,`redshift:DescribeClusterParameterGroups`, . `redshift:DescribeClusterTracks` `redshift:DescribeSnapshotSchedules` , e. `ec2:DescribeAddresses`	27 novembre 2022

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare i processi di ripristino di Amazon Redshift`redshift:RestoreFromClusterSnapshot`:`redshift:RestoreTableFromClusterSnapshot` ,`redshift:DescribeClusters` , e. `redshift:DescribeTableRestoreStatus`	27 novembre 2022
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare i processi di backup di Amazon Redshift`redshift:CreateClusterSnapshot` :`redshift:DescribeClusterSnapshots` ,,`redshift:DescribeTags` , `redshift:DeleteClusterSnapshot` `redshift:DescribeClusters` , e. `redshift:CreateTags`	27 novembre 2022
AWSBackupFullAccess: aggiornamento a una policy esistente	È stata aggiunta la seguente autorizzazione alle CloudFormation risorse di supporto:. `cloudformation:ListStacks`	27 novembre 2022

Modifica	Descrizione	Data
AWSBackupOperatorAccess: aggiornamento a una policy esistente	È stata aggiunta la seguente autorizzazione per supportare CloudFormation le risorse:`cloudformation:ListStacks` .	27 novembre 2022
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare CloudFormation le risorse:`redshift:DescribeClusterSnapshots` , `redshift:DescribeTags` `redshift:DeleteClusterSnapshot` , `eredshift:DescribeClusters` .	27 novembre 2022
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare i processi di backup dello stack di AWS CloudFormation applicazioni:`cloudformation:GetTemplate` , `ecloudformation:DescribeStacks` . `cloudformation:ListStackResources`	16 novembre 2022

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare i job di backup dello stack di AWS CloudFormation applicazioni: e `cloudformation:CreateChangeSet` `cloudformation:DescribeChangeSet`	16 novembre 2022
AWSBackupOrganizationAdminAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni a questa politica per consentire agli amministratori dell'organizzazione di utilizzare la funzionalità Amministratore delegato:,, e `organizations:ListDelegatedAdministrator` `organizations:RegisterDelegatedAdministrator` `organizations:DeregisterDelegatedAdministrator`	27 novembre 2022

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare SAP HANA su istanze Amazon EC2:`ssm-sap:GetOperation` ,,,, `ssm-sap:ListDatabases` e. `ssm-sap:BackupDatabase` `ssm-sap:UpdateHanaBackupSettings` `ssm-sap:GetDatabase` `ssm-sap:ListTagsForResource`	20 novembre 2022
AWSBackupFullAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare SAP HANA su istanze Amazon EC2:,, e. `ssm-sap:GetOperation` `ssm-sap:ListDatabases` `ssm-sap:GetDatabase` `ssm-sap:ListTagsForResource`	20 novembre 2022
AWSBackupOperatorAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare SAP HANA su istanze Amazon EC2:,, e. `ssm-sap:GetOperation` `ssm-sap:ListDatabases` `ssm-sap:GetDatabase` `ssm-sap:ListTagsForResource`	20 novembre 2022

Modifica	Descrizione	Data
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	È stata aggiunta la seguente autorizzazione per supportare SAP HANA su istanze Amazon EC2:. `ssm-sap:GetOperation`	20 novembre 2022
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	È stata aggiunta la seguente autorizzazione per supportare i processi di ripristino del gateway di Backup su un'istanza EC2:`ec2:CreateTags` .	20 novembre 2022
AWSBackupDataTransferAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per supportare il trasferimento sicuro dei dati di storage per SAP HANA sulle risorse Amazon EC2:`backup-storage:StartObject` ,,,, `backup-storage:PutChunk` `backup-storage:GetChunk` , `backup-storage:ListChunks` e. `backup-storage:ListObjects` `backup-storage:GetObjectMetadata` `backup-storage:NotifyObjectComplete`	20 novembre 2022

Modifica	Descrizione	Data
AWSBackupRestoreAccessForSAPHANA: aggiornamento a una policy esistente	Sono state aggiunte le seguenti autorizzazioni per consentire ai proprietari delle risorse di eseguire il ripristino di SAP HANA sulle risorse Amazon EC2:`backup:Get* ,,backup:List* ,backup:Describe* ,backup:StartBackupJob ,backup:StartRestoreJob ,ssm-sap:GetOperation , ssm-sap:ListDatabases ssm-sap:BackupDatabase , ssm-sap:RestoreDatabase e. ssm-sap:UpdateHanaBackupSettings ssm-sap:GetDatabase ssm-sap:ListTagsForResource`	20 novembre 2022
AWSBackupServiceRolePolicyForS3Backup: aggiornamento a una policy esistente	È stata aggiunta l'autorizzazione `s3:GetBucketAcl` a supportare le operazioni di backup AWS Backup di Amazon S3.	24 agosto 2022

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Sono state aggiunte le seguenti azioni per concedere l'accesso alla creazione di un'istanza di database per supportare la funzionalità Multi-Availability Zone (Multi-AZ):. `rds:CreateDBInstance`	20 luglio 2022
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	È stata aggiunta l'`s3:GetBucketTagging` autorizzazione a concedere all'utente l'autorizzazione a selezionare i bucket di cui eseguire il backup con una jolly di risorse. Senza questa autorizzazione, gli utenti che selezionano i bucket di cui eseguire il backup con una risorsa wildcard non hanno successo.	6 maggio 2022
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte risorse di volume nell'ambito delle azioni esistenti `fsx:CreateBackup` e sono state aggiunte nuove `fsx:ListTagsForResource` azioni `fsx:DescribeVolumes` per supportare i backup a livello di volume FSx for ONTAP.	27 aprile 2022

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Sono state aggiunte le seguenti azioni per concedere agli utenti le autorizzazioni per ripristinare i `fsx:DescribeVolumes` volumi FSx for ONTAP`fsx:CreateVolumeFromBackup` ,, `fsx:DeleteVolume` e. `fsx:UntagResource`	27 aprile 2022
AWSBackupServiceRolePolicyForS3Backup: aggiornamento a una policy esistente	Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per ricevere notifiche di modifiche ai propri bucket Amazon S3 durante le operazioni di backup: e. `s3:GetBucketNotification` `s3:PutBucketNotification`	25 febbraio 2022

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForS3Backup: nuova policy	Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per eseguire il backup dei propri bucket Amazon S3s3:GetInventoryConfiguration :s3:PutInventoryConfiguration ,,s3:ListBucketVersions ,s3:ListBucket ,, s3:GetBucketTagging s3:GetBucketVersioning , e s3:GetBucketNotification s3:GetBucketLocation s3:ListAllMyBuckets Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per il backup dei propri oggetti Amazon S3s3:GetObject :s3GetObjectAcl ,,s3:GetObjectVersionTagging , s3:GetObjectVersionAcl s3:GetObjectTagging , e. s3:GetObjectVersion Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per il backup dei dati kms:Decry	17 febbraio 2022

Modifica	Descrizione	Data
	pt crittografati di Amazon S3: e. kms:DescribeKey Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per eseguire backup incrementali dei dati Amazon S3 utilizzando le regole di EventBridge Amazonevents:DescribeRule :events:EnableRule ,,,events:PutRule ,events:DeleteRule ,, events:PutTargets events:RemoveTargets events:ListTargetsByRule , events:DisableRule e. cloudwatch:GetMetricData events:ListRules	

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForS3Restore: nuova policy	Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per ripristinare i propri bucket Amazon S3 `s3:CreateBucket` :`s3:ListBucketVersions` ,,, `s3:ListBucket` `s3:GetBucketVersioning` , `s3:GetBucketLocation` e. `s3:PutBucketVersioning` Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per ripristinare i propri bucket Amazon S3 `s3:GetObject` :`s3:GetObjectVersion` ,`s3:DeleteObject` ,`s3:PutObjectVersionAcl` ,`s3:GetObjectVersionAcl` ,`s3:GetObjectTagging` ,, `s3:PutObjectTagging` `s3:GetObjectAcl` `s3:PutObjectAcl` , `s3:PutObject` e. `s3:ListMultipartUploadParts` Sono state aggiunte le seguenti azioni per concedere	17 febbraio 2022

Modifica	Descrizione	Data
	all'utente le autorizzazioni per crittografare i dati Amazon S3 ripristinati`kms:Decrypt` :`kms:DescribeKey` , e. `kms:GenerateDataKey`	
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	`s3:ListAllMyBuckets` Aggiunto per concedere all'utente le autorizzazioni per visualizzare un elenco dei propri bucket e scegliere quali assegnare a un piano di backup.	14 febbraio 2022
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	`backup-gateway:ListVirtualMachines` Aggiunto per concedere all'utente le autorizzazioni per visualizzare un elenco delle proprie macchine virtuali e scegliere quali assegnare a un piano di backup. `backup-gateway:ListTagsForResource` Aggiunto per concedere all'utente le autorizzazioni per elencare i tag per le proprie macchine virtuali.	30 novembre 2021

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	Aggiunto `backup-gateway:Backup` per concedere all'utente le autorizzazioni per ripristinare i backup delle macchine virtuali. AWS Backup aggiunto anche `backup-gateway:ListTagsForResource` per concedere all'utente le autorizzazioni per elencare i tag assegnati ai backup delle macchine virtuali.	30 novembre 2021
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Aggiunto `backup-gateway:Restore` per concedere all'utente le autorizzazioni per ripristinare i backup delle macchine virtuali.	30 novembre 2021

Modifica	Descrizione	Data
AWSBackupFullAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti azioni per concedere agli utenti le autorizzazioni necessarie per utilizzare AWS Backup Gateway per il backup, il ripristino e la gestione delle proprie macchine virtuali: `backup-gateway:AssociateGatewayToServer backup-gateway:CreateGateway backup-gateway:DeleteGateway backup-gateway:DeleteHypervisor ,backup-gateway:DisassociateGatewayFromServer ,backup-gateway:ImportHypervisorConfiguration ,backup-gateway:ListGateways ,,backup-gateway:ListHypervisors ,backup-gateway:ListTagsForResource ,backup-gateway:ListVirtualMachines ,backup-gateway:PutMaintenanceStartTime ,backup-gateway:TagResource , backup-gateway:TestHypervisorConfiguration backup-ga`	30 novembre 2021

Modifica	Descrizione	Data
	`teway:UntagResourc e` , `backup-gateway:Upd ateGatewayInformat ion` e. `backup-ga teway:UpdateHyperv isor`	
AWSBackupOperatorAccess: aggiornamento a una policy esistente	Sono state aggiunte le seguenti azioni per concedere all'utente le autorizzazioni per il backup delle proprie macchine virtuali:`backup-ga teway:ListGateways` , `backup-gateway:Lis tHypervisors` `backup-gateway:ListTagsForR esource` , e. `backup-ga teway:ListVirtualM achines`	30 novembre 2021
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	`dynamodb:ListTags0 fResource` Aggiunto per concedere all'utente le autorizzazioni per elencare i tag delle tabelle DynamoDB di cui eseguire il backup utilizzando le funzionalità di backup avanzate AWS Backup di DynamoDB.	23 novembre 2021

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	`dynamodb:StartAwsBackupJob` Aggiunto per concedere all'utente le autorizzazioni per eseguire il backup delle tabelle DynamoDB utilizzando funzionalità di backup avanzate. `dynamodb:ListTagsOfResource` Aggiunto per concedere all'utente le autorizzazioni per copiare i tag dalle tabelle DynamoDB di origine ai propri backup.	23 novembre 2021
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	`dynamodb:RestoreTableFromAwsBackup` Aggiunto per concedere all'utente le autorizzazioni per ripristinare le tabelle DynamoDB di cui è stato eseguito il backup utilizzando le funzionalità di backup avanzate AWS Backup di DynamoDB.	23 novembre 2021

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	`dynamodb:RestoreTableFromAwsBackup` Aggiunto per concedere all'utente le autorizzazioni per ripristinare le tabelle DynamoDB di cui è stato eseguito il backup utilizzando le funzionalità di backup avanzate AWS Backup di DynamoDB.	23 novembre 2021
AWSBackupOperatorAccess: aggiornamento a una policy esistente	Le azioni sono state rimosse perché erano `backup:GetRecoveryPointRestoreMetadata` ridondanti. `rds:DescribeDBSnapshots` AWS Backup non aveva bisogno di entrambi `backup:GetRecoveryPointRestoreMetadata` e `backup:Get*` come parte di. `AWSBackupOperatorAccess` Inoltre, AWS Backup non aveva bisogno di entrambi `rds:DescribeDBSnapshots` e `rds:describeDBSnapshots` come parte di`AWSBackupOperatorAccess` .	23 novembre 2021

Modifica	Descrizione	Data
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	Sono state aggiunte le nuove azioni `elasticfilesystem:DescribeFileSystems` `dynamodb:ListTables` ,`storagegateway:ListVolumes` ,`ec2:DescribeVolumes` ,`ec2:DescribeInstances` , `rds:DescribeDBInstances` `rds:DescribeDBClusters` , e `fsx:DescribeFileSystems` per consentire ai clienti di visualizzare e scegliere da un elenco delle risorse AWS Backup supportate al momento di selezionare le risorse da assegnare a un piano di backup.	10 novembre 2021
AWSBackupAuditAccess: nuova policy	Aggiunto `AWSBackupAuditAccess` per concedere all'utente le autorizzazioni per utilizzare AWS Backup Audit Manager. Le autorizzazioni includono la possibilità di configurare i framework di conformità e generare report.	24 agosto 2021

Modifica	Descrizione	Data
AWSServiceRolePolicyForBackupReports: nuova policy	`AWSServiceRolePolicyForBackupReports` Aggiunto per concedere le autorizzazioni per un ruolo collegato al servizio per automatizzare il monitoraggio delle impostazioni, dei processi e delle risorse di backup per la conformità con i framework configurati dall'utente.	24 agosto 2021
AWSBackupFullAccess: aggiornamento a una policy esistente	`iam:CreateServiceLinkedRole` Aggiunto per creare un ruolo collegato ai servizi (nel migliore dei modi) per automatizzare l'eliminazione dei punti di ripristino scaduti per te. Senza questo ruolo collegato ai servizi, AWS Backup non è possibile eliminare i punti di ripristino scaduti dopo che i clienti hanno eliminato il ruolo IAM originale utilizzato per creare i punti di ripristino.	5 luglio 2021

Modifica	Descrizione	Data
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	È stata aggiunta la nuova azione `dynamodb:DeleteBackup` per concedere l'`DeleteRecoveryPoint` autorizzazione per automatizzare l'eliminazione dei punti di ripristino DynamoDB scaduti in base alle impostazioni del ciclo di vita del piano di backup.	5 luglio 2021
AWSBackupOperatorAccess: aggiornamento a una policy esistente	Sono state rimosse le azioni perché erano ridondant `ibackup:GetRecoveryPointRestoreMetadata` . `rds:DescribeDBSnapshots` AWS Backup non aveva bisogno di entrambi `backup:GetRecoveryPointRestoreMetadata` e `backup:Get*` come parte di AlsoAWSBackup `OperatorAccess` , non AWS Backup aveva bisogno di entrambi `rds:DescribeDBSnapshots` e `rds:describeDBSnapshots` come parte di `AWSBackupOperatorAccess`	25 maggio 2021

Modifica	Descrizione	Data
AWSBackupOperatorAccess: aggiornamento a una policy esistente	Ho rimosso `backup:GetRecoveryPointRestoreMetadata` le azioni `rds:DescribeDBSnapshots` perché erano ridondanti. AWS Backup non aveva bisogno di entrambi `backup:GetRecoveryPointRestoreMetadata` e `backup:Get*` come parte di. `AWSBackupOperatorAccess` Inoltre, AWS Backup non aveva bisogno di entrambi `rds:DescribeDBSnapshots` e `rds:describeDBSnapshots` come parte di`AWSBackupOperatorAccess` .	25 maggio 2021
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	È stata aggiunta la nuova azione `fsx:TagResource` per concedere `StartRestoreJob` l'autorizzazione per consentire di applicare tag ai file system Amazon FSx durante il processo di ripristino.	24 maggio 2021

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForRestores: aggiornamento a una policy esistente	Sono state aggiunte le nuove azioni `ec2:DescribeImages` e `ec2:DescribeInstances` la concessione `StartRestoreJob` dell'autorizzazione per consentire il ripristino delle istanze Amazon EC2 dai punti di ripristino.	24 maggio 2021
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	È stata aggiunta la nuova azione `fsx:CopyBackup` per concedere `StartCopyJob` l'autorizzazione per consentire di copiare i punti di ripristino Amazon FSx tra regioni e account.	12 Aprile 2021
AWSBackupServiceLinkedRolePolicyForBackup: aggiornamento a una policy esistente	È stata aggiunta la nuova azione `fsx:CopyBackup` per concedere `StartCopyJob` l'autorizzazione per consentire di copiare i punti di ripristino Amazon FSx tra regioni e account.	12 Aprile 2021

Modifica	Descrizione	Data
AWSBackupServiceRolePolicyForBackup: aggiornamento a una policy esistente	Aggiornato per soddisfare i seguenti requisiti: AWS Backup Per creare un backup di una tabella DynamoDB crittografata, è necessario aggiungere `kms:Decrypt` e le autorizzazioni `kms:GenerateDataKey` e il ruolo IAM utilizzato per il backup.	10 marzo 2021

Modifica	Descrizione	Data
AWSBackupFullAccess: aggiornamento a una policy esistente	Aggiornato per soddisfare i seguenti requisiti: AWS Backup Per configurare backup continui per il tuo database Amazon RDS, verifica che l'autorizzazione API `rds:ModifyDBInstance` esista nel ruolo IAM definito dalla configurazione del tuo piano di backup. Per ripristinare i backup continui di Amazon RDS, devi aggiungere l'autorizzazione `rds:RestoreDBInstanceToPointInTime` al ruolo IAM inviato per il processo di ripristino. Nella AWS Backup console, per descrivere l'intervallo di tempo disponibile per il point-in-time ripristino, devi includere l'autorizzazione `rds:DescribeDBInstanceAutomatedBackups` API nella tua policy gestita da IAM.	10 marzo 2021
AWS Backup ha iniziato a tenere traccia delle modifiche	AWS Backup ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	10 marzo 2021

Utilizzo di ruoli collegati ai servizi per AWS Backup

AWS Backup utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Backup I ruoli collegati ai servizi sono predefiniti AWS Backup e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Argomenti

Utilizzo dei ruoli per il backup e la copia

AWS Backup utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Backup I ruoli collegati ai servizi sono predefiniti AWS Backup e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione AWS Backup perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Backup definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Backup Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi AWS Backup le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per AWS Backup

AWS Backup utilizza il ruolo collegato al servizio denominato AWSServiceRoleForBackup: fornisce le AWS Backup autorizzazioni per elencare le risorse di cui è possibile eseguire il backup e per copiare i backup.

AWS Backup utilizza inoltre il ruolo per eliminare tutti i backup per tutti i tipi di risorse ad eccezione di Amazon EC2.

Il ruolo AWSServiceRoleForBackup collegato ai servizi si affida ai seguenti servizi per l'assunzione del ruolo:

- `backup.amazonaws.com`

Per visualizzare le autorizzazioni per questa politica, consulta il Managed Policy AWSBackupServiceLinkedRolePolicyforBackupReference.AWS

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS Backup

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando elenchi le risorse di cui eseguire il backup, configuri il backup su più account o esegui backup nell'API AWS Management Console, l'o l' AWS API AWS CLI, AWS Backup crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato ai servizi può apparire nell'account se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate dal ruolo. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando elenchi le risorse di cui eseguire il backup, configuri il backup su più account o esegui backup, viene nuovamente AWS Backup creato il ruolo collegato al servizio.

Modifica di un ruolo collegato ai servizi per AWS Backup

AWS Backup non consente di modificare il ruolo collegato al servizio. AWSServiceRoleForBackup Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS Backup

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo. Innanzitutto, devi eliminare tutti i punti di ripristino. Quindi, devi eliminare tutti i vault di backup.

> **Note**
>
> Se il AWS Backup servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti, quindi ripeti l'operazione.

Per eliminare AWS Backup le risorse utilizzate dalla AWSServiceRoleForBackup (console)

1. Per eliminare tutti i punti di ripristino e i vault di backup (tranne il vault predefinito), segui la procedura in Eliminazione di un vault di backup.
2. Per eliminare il vault predefinito, utilizza il seguente comando in AWS CLI:

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

Per eliminare AWS Backup le risorse utilizzate da AWSServiceRoleForBackup (AWS CLI)

1. Per eliminare tutti i punti di ripristino, usa delete-recovery-point.
2. Per eliminare tutti i vault di backup, utilizza `delete-backup-vault`.

Per eliminare AWS Backup le risorse utilizzate dall' AWSServiceRoleForBackup (API)

1. Per eliminare tutti i punti di ripristino, utilizza `DeleteRecoveryPoint`.
2. Per eliminare tutti i vault di backup, utilizza `DeleteBackupVault`.

Eliminazione manuale del ruolo collegato ai servizi

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSServiceRoleForBackup collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS Backup

AWS Backup supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Disponibilità delle funzionalitàAWS Backup tramite Regione.

Utilizzo dei ruoli per AWS Backup Audit Manager

AWS Backup utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Backup I ruoli collegati ai servizi sono predefiniti AWS Backup e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione AWS Backup perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Backup definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Backup Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi AWS Backup le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per AWS Backup

AWS Backup utilizza il ruolo collegato al servizio denominato AWSServiceRoleForBackupReports: fornisce AWS Backup l'autorizzazione per creare controlli, framework e report.

Il ruolo AWSServiceRoleForBackupReports collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `backup.amazonaws.com`

Per visualizzare le autorizzazioni per questa politica, consulta il Managed Policy AWSServiceRolePolicyForBackupReportsReference.AWS

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS Backup

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un framework o un piano di report in AWS Management Console, the AWS CLI o nell' AWS API, AWS Backup crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato ai servizi può apparire nell'account se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate dal ruolo. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un framework o un piano di report, AWS Backup crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per AWS Backup

AWS Backup non consente di modificare il ruolo collegato al AWSServiceRoleForBackupReports servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS Backup

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo. Devi eliminare tutti i framework e i piani di report.

> **Note**
>
> Se il AWS Backup servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti, quindi ripeti l'operazione.

Per eliminare AWS Backup le risorse utilizzate dalla AWSServiceRoleForBackupReports (console)

1. Per eliminare tutti i framework, consulta Eliminazione dei framework.
2. Per eliminare tutti i piani di report, consulta Eliminazione dei piani di report.

Per eliminare AWS Backup le risorse utilizzate da AWSServiceRoleForBackupReports (AWS CLI)

1. Per eliminare tutti i framework, usa delete-framework.
2. Per eliminare tutti i piani di report, utilizzare delete-report-plan.

Per eliminare AWS Backup le risorse utilizzate dall' AWSServiceRoleForBackupReports (API)

1. Per eliminare tutti i framework, utilizza DeleteFramework.
2. Per eliminare tutti i piani di report, usa DeleteReportPlan.

Eliminazione manuale del ruolo collegato ai servizi

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSServiceRoleForBackupReports collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS Backup

AWS Backup supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Disponibilità delle funzionalitàAWS Backup tramite Regione.

Utilizzo dei ruoli per i test di ripristino

AWS Backup utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Backup I ruoli collegati ai servizi sono predefiniti AWS Backup e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione AWS Backup perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Backup definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Backup Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi AWS Backup le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per AWS Backup

AWS Backup utilizza il ruolo collegato al servizio denominato AWSServiceRolePolicyForBackupRestoreTesting: fornisce le autorizzazioni di backup per eseguire test di ripristino.

Il ruolo AWSServiceRolePolicyForBackupRestoreTesting collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `backup.amazonaws.com`

Per visualizzare le autorizzazioni per questa politica, consulta il Managed Policy AWSServiceRolePolicyForBackupRestoreTestingReference.AWS

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS Backup

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando esegui i test di ripristino nell'API AWS Management Console AWS CLI, nella o nell' AWS API, AWS Backup crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato ai servizi può apparire nell'account se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate dal ruolo. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando esegui il test di ripristino, AWS Backup crea nuovamente il ruolo collegato al servizio.

Modifica di un ruolo collegato ai servizi per AWS Backup

AWS Backup non consente di modificare il ruolo collegato al AWSServiceRolePolicyForBackupRestoreTesting servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS Backup

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo. È necessario eliminare tutti i piani di test di ripristino.

> **Note**
>
> Se il AWS Backup servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti, quindi ripeti l'operazione.

Per eliminare AWS Backup le risorse utilizzate dalla AWSServiceRolePolicyForBackupRestoreTesting (console)

- Per eliminare tutti i piani di test di ripristino, consulta Test di ripristino.

Per eliminare AWS Backup le risorse utilizzate da AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI)

- Per eliminare i piani di test di ripristino, usa `delete-restore-testing-plan`.

Per eliminare AWS Backup le risorse utilizzate dall' AWSServiceRolePolicyForBackupRestoreTesting (API)

- Per eliminare i piani di test di ripristino, usa `DeleteRestoreTestingPlan`.

Eliminazione manuale del ruolo collegato ai servizi

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSServiceRolePolicyForBackupRestoreTesting collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS Backup

AWS Backup supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Disponibilità delle funzionalitàAWS Backup tramite Regione.

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. In AWS, la rappresentazione cross-service può comportare il problema

confused deputy. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Ti consigliamo di utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` nelle policy delle risorse per limitare le autorizzazioni con cui AWS Backup fornisce un altro servizio alla risorsa. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account nella stessa istruzione di policy.

Il valore di `aws:SourceArn` deve essere un vault AWS Backup quando si utilizza AWS Backup per pubblicare argomenti di Amazon SNS a nome dell'utente.

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

Sicurezza dell'infrastruttura in AWS Backup

In quanto servizio gestito, AWS Backup è protetto dalla sicurezza di rete AWS globale. Per ulteriori informazioni sui servizi di AWS 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 Protezione dell'infrastruttura in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS Backup attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.2 o versioni successive. I client devono inoltre supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Diffie-Hellman Ephemeral (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.

Integrità dei dati in AWS Backup

AWS Backup obiettivo di integrità dei dati

AWS Backup cerca di mantenere l'integrità durante la trasmissione, l'archiviazione e l'elaborazione dei dati. AWS Backup tratta i dati delle risorse archiviate come informazioni critiche indipendenti dal contenuto, in quanto offriamo lo stesso elevato livello di sicurezza ai clienti, indipendentemente dal tipo di dati archiviati. Siamo attenti alla sicurezza dei nostri clienti e abbiamo implementato sofisticate misure tecniche e fisiche contro l'accesso non autorizzato. Il cliente mantiene il controllo completo sulla classificazione dei dati, sulle regioni in cui vengono archiviati e sulle modalità di controllo, archiviazione e protezione dalla divulgazione dei dati.

AWS Backup implementazione dell'integrità dei dati

AWS Backup collabora con altri servizi AWS e con Amazon per mantenere l'integrità dei dati archiviati e con cui interagisce. Gli strumenti utilizzati possono variare e possono includere (a solo titolo di esempio):

- Convalida continua degli oggetti in base al relativo checksum per prevenirne il danneggiamento
- Checksum interni per confermare l'integrità dei dati in transito e inattivi
- Checksum calcolati sui dati nei backup creati dall'archivio principale
- Tentativo automatico di ripristinare i normali livelli di ridondanza dello storage degli oggetti in caso di danneggiamento del disco o rilevamento di un guasto del dispositivo
- Archiviazione ridondante dei dati su più postazioni fisiche
- Miglioramento della durabilità degli oggetti su più zone di disponibilità durante la scrittura iniziale, combinato con un'ulteriore replica in caso di indisponibilità del dispositivo o rilevamento di bit-rot
- Checksum su tutto il traffico di rete per rilevare il danneggiamento dei pacchetti di dati durante l'archiviazione o il recupero dei dati

AWS Backup archivia nativamente i dati per Amazon DynamoDB con funzionalità avanzate, Amazon EFS, Amazon S3, Amazon Timestream e macchine virtuali in esecuzione con VMware connesse tramite gateway di Backup. AWS Backup facilita i backup dei dati archiviati con altri servizi, tra cui Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon FSx per Windows File Server, Amazon FSx for Lustre, Amazon FSx per OpenZFS, Amazon FSx per ONTAP, Amazon Neptune, Amazon RDS e Amazon Redshift. NetApp

Conferma e controllo oggettivi dell'integrità dei dati di AWS Backup

I dati archiviati direttamente da AWS Backup e i dati archiviati in collaborazione con altri AWS servizi con cui AWS Backup interagisce sono soggetti al rigoroso processo di Amazon Simple Storage Service (Amazon S3) alla base di tale integrità dei dati. Tale integrità è confermata da un revisore indipendente e terzo attraverso un rapporto di audit SOC annuale disponibile attraverso AWS Artifact nella AWS Management Console.

Conservazioni legali e AWS Backup

Un blocco a fini legali è uno strumento amministrativo che impedisce l'eliminazione dei backup mentre sono bloccati. Finché il blocco è in vigore, i backup bloccati non possono essere eliminati e le policy del ciclo di vita che potrebbero alterare lo stato del backup (ad esempio la transizione allo stato `Deleted`) vengono rimandate finché il blocco a fini legali non viene rimosso. Un backup può essere oggetto di molteplici blocchi a fini legali.

I blocchi legali possono essere applicati a uno o più backup (noti anche come punti di ripristino) creati AWS Backup se il loro ciclo di vita lo consente. Un tipo di backup denominato backup continuo prevede un ciclo di vita massimo di 35 giorni. Le conservazioni legali non prolungano il ciclo di vita continuo dei backup.

Quando viene creato un blocco a fini legali, questo può tenere conto di criteri di filtro specifici, come i tipi di risorse e gli ID delle risorse. Inoltre, è possibile definire l'intervallo di date di creazione dei backup che si desidera includere in un blocco a fini legali. i blocchi a fini legali e i backup si trovano in una relazione molti-a-molti, il che significa che un backup può avere più di un blocco a fini legali e un blocco a fini legali può includere più di un backup. Ogni account può avere un massimo di 50 blocchi a fini legali attivi contemporaneamente.

I blocchi a fini legali si applicano solo al backup originale su cui sono imposti. Quando un backup viene copiato tra regioni o account diversi (se la risorsa lo supporta), tali copie non conservano né portano con sé il blocco a fini legali. A un blocco a fini legali, come a ogni altra risorsa, è associato un Amazon Resource Name (ARN) univoco. Solo i punti di ripristino creati da AWS Backup possono far parte di una custodia legale.

Tieni presente che mentre Vault Lock di AWS Backup fornisce protezione e immutabilità aggiuntive a un vault, un blocco a fini legali fornisce una protezione aggiuntiva contro l'eliminazione di singoli backup (punti di ripristino). La conservazione legale non scade e conserva i dati all'interno del backup a tempo indeterminato. Il blocco rimane attivo fino a quando non viene rilasciato da un utente con autorizzazioni sufficienti.

Creazione di un blocco a fini legali

Quando viene creato un blocco a fini legali, questo contiene solo i punti di ripristino che sono già stati creati. I backup (punti di ripristino) con stato impostato a `EXPIRED` o `DELETING` non verranno inclusi nel blocco a fini legali. I punti di ripristino (backup) con lo stato impostato a `CREATING` potrebbero non essere inclusi nel blocco a fini legali, in base al momento del completamento.

I blocchi legali possono essere aggiunti dagli utenti che dispongono delle autorizzazioni IAM richieste.

Creazione di un blocco a fini legali utilizzando la console di

Per creare una conservazione legale

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel pannello di controllo a sinistra della console, trovare la sezione Il mio account. Scegli Sospensioni legali.
3. Scegli Aggiungi blocco legale.
4. Vengono visualizzati tre pannelli: Dettagli sulla conservazione a fini legali, Ambito di conservazione a fini legali e tag di conservazione a fini legali.

    a. In Dettagli sul blocco a fini legali, inserire un titolo e una descrizione del blocco a fini legali nelle caselle di testo fornite.

    b. Nel pannello Ambito del blocco a fini legali, scegliere in che modo selezionare la risorsa da includere nel blocco. Quando si crea un blocco, si sceglie il metodo utilizzato per selezionare le risorse che rientrano nel blocco legale. È possibile scegliere una delle seguenti opzioni:

        - ID e tipi di risorse specifici
        - Seleziona gli archivi di backup
        - Tutti i tipi di risorse o tutti gli archivi di backup all'interno del tuo account

    c. Indicazione dell'intervallo di date del blocco a fini legali. Inserire le date nel formato YYYY:MM:DD (gli estremi sono inclusi).

    d. Facoltativamente, puoi aggiungere tag per il blocco nella sezione Tag di conservazione legale. I tag possono aiutare a classificare il blocco per riferimenti e organizzazioni futuri. È possibile aggiungere fino a 50 tag in totale.
5. Quando sei soddisfatto della configurazione del nuovo blocco a fini legali, fai clic sul pulsante Aggiungi nuovo blocco.

Crea un blocco a fini legali utilizzando il AWS CLI

È possibile creare un blocco legale utilizzando il create-legal-holdcomando.

```
aws backup create-legal-hold --title "my title" \
    --description "my description" \
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

Visualizzazione dei blocchi a fini legali

È possibile visualizzare i dettagli relativi alla conservazione a fini legali nella AWS Backup console o a livello di programmazione.

Visualizza i blocchi legali utilizzando la console

Per visualizzare tutti i blocchi a fini legali all'interno di un account utilizzando la console di Backup,

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nella parte sinistra del pannello di controllo, nella sezione Il mio account, fare clic su Blocchi a fini legali.
3. La tabella dei blocchi a fini legali mostra il titolo, lo stato, la descrizione, l'ID e la data di creazione dei blocchi esistenti. Fare clic sulla freccia rivolta verso il basso accanto all'intestazione della tabella per filtrare la tabella in base alla colonna selezionata.

Visualizzazione dei blocchi a fini legali a livello di codice

Per visualizzare tutte le riserve legali a livello di codice, puoi utilizzare le seguenti chiamate API: ListLegalHoldse. GetLegalHold

È possibile utilizzare il seguente modello JSON per. `GetLegalHold`

```
GET /legal-holds/{legalHoldId} HTTP/1.1

Request

empty body

Response
```

```
{
    Title: string,
    Status: LegalHoldStatus,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,

   ResourceSelection: {
        VaultArns: [ string ]
        Resources: [ string ]
   },
   ResourceFilters: {
        DateRange: {
          FromDate: number,
          ToDate: number
        }
   }
}
```

È possibile utilizzare il seguente modello JSON per. `ListLegalHolds`

```
GET /legal-holds/
  &maxResults=MaxResults
  &nextToken=NextToken


Request

empty body
url params:
  MaxResults: number  // optional,
  NextToken: string  // optional

status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING
maxResults: 1-1000



Response
```

```
{
  NextToken: token,
  LegalHolds: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,
  ]

}
```

Di seguito sono riportati i possibili valori di stato.

Stato	Descrizione
CREAZIONE IN CORSO	I punti di ripristino richiesti sono in fase di attivazione del blocco e le richieste di eliminazione di tali punti di ripristino potrebbero avere esito positivo poiché il blocco non è ancora stato creato.
ACTIVE	Il blocco a fini legali è stato creato. Tutti i punti di ripristino elencati in tale blocco sono bloccati.
CANCELLING (ANNULLAMENTO IN CORSO)	I blocchi a fini legali sono in corso di rimozione e le richieste di eliminazione dei punti di ripristino oggetto del blocco potrebbero avere esito positivo.
CANCELED (ANNULLATO)	Il blocco a fini legali è stato completamente annullato e non ha più alcun effetto. I punti di ripristino possono essere eliminati.

Rilascio di un blocco a fini legali

I blocchi legali rimangono in vigore fino a quando non vengono rimossi da un utente con autorizzazioni sufficienti. La rimozione di un blocco a fini legali è nota anche come annullamento, eliminazione o rilascio di un blocco a fini legali. La rimozione di un blocco a fini legali lo elimina da tutti i backup a cui era collegato. Tutti i backup scaduti durante la conservazione legale vengono eliminati entro 24 ore dalla rimozione della conservazione legale.

Rilascio di un blocco a fini legali utilizzando la console di

Per rilasciare un blocco utilizzando la console

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Inserire la descrizione che si desidera associare al rilascio.
3. Controllare i dettagli, quindi fare clic su Rimuovi blocco.
4. Quando viene visualizzata la finestra di dialogo Rilascia blocco, confermare l'intenzione di annullare il blocco digitando `confirm` nella casella di testo.

    - Selezionare la casella che conferma l'intenzione di annullare il blocco.

Nella pagina Legal holds (Blocchi a fini legali) è possibile visualizzare tutti i propri blocchi a fini legali. Se il rilascio ha avuto esito positivo, lo stato di tale blocco verrà visualizzato come `Released`.

Rilascia un blocco legale a livello di codice

Per rimuovere un blocco a livello di codice, utilizza la chiamata API. CancelLegalHold

Utilizza il seguente modello JSON.

```
DELETE /legal-holds/{legalHoldId}


Request

{
   CancelDescription: String
   DeleteAfterDays: number // optional
}
```

```
DeleteAfterDays: optional.
  Defaults to 180 days. how long to keep legal hold record after canceled.
  This applies to the actual legal hold record only.
  Recovery points are unlocked as soon as cancelation processes and are not subject to
 this date.

Response

Empty body

200 if successful
other standard codes
```

AWS PrivateLink

AWS PrivateLink consente di stabilire una connessione privata tra il Virtual Private Cloud («VPC») e gli endpoint creando un AWS Backup endpoint VPC di interfaccia. Gli endpoint di interfaccia sono alimentati da AWS PrivateLink, una tecnologia che ti consente di accedere in modo privato alle AWS Backup API limitando tutto il traffico di rete tra il tuo VPC e AWS Backup la rete Amazon.

AWS PrivateLink ti consente di accedere in modo privato alle AWS Backup operazioni senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare AWS Backup con gli endpoint API. Inoltre, le istanze non hanno bisogno di indirizzi IP pubblici per utilizzare nessuna delle operazioni AWS Backup API e API del gateway di Backup disponibili. Il traffico tra il tuo VPC e AWS Backup non esce dalla rete Amazon.

Per ulteriori informazioni sugli endpoint dei VPC, consulta Endpoint VPC di interfaccia (AWS PrivateLink) nella Guida per l'utente di Amazon VPC.

Considerazioni sugli endpoint VPC di Amazon

Prima di configurare un endpoint VPC di interfaccia per AWS Backup gli endpoint, consulta le proprietà e le limitazioni degli endpoint dell'interfaccia nella Amazon VPC User Guide.

Tutte le AWS Backup operazioni relative alla gestione delle risorse di Amazon Backup sono disponibili dal tuo VPC utilizzando. AWS PrivateLink

Le policy degli endpoint VPC sono supportate per gli endpoint di Backup. Per impostazione predefinita, attraverso l'endpoint è consentito l'accesso completo alle operazioni di Backup. Per

ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Creazione di un AWS Backup endpoint VPC

Puoi creare un endpoint VPC per AWS Backup utilizzare la console Amazon VPC o (CLI). AWS Command Line Interface AWS Per ulteriori informazioni, consulta Creazione di un endpoint di interfaccia nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC per AWS Backup utilizzare il nome del servizio. `com.amazonaws.region.backup`

Nelle regioni Cina (Pechino) e Cina (Ningxia), il nome del servizio deve essere `cn.com.amazonaws.region.backup`.

Per gli endpoint del gateway di Backup, utilizzare `com.amazonaws.region.backup-gateway`.

Durante la creazione di un endpoint VPC per il gateway di backup, nel gruppo di sicurezza devono essere incluse le seguenti porte TCP :

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Protocollo	Porta	Direzione	Origine	Destinazione	Utilizzo
TCP	443 (HTTPS)	In uscita	Backup Gateway	AWS	Per la comunicazione dal Backup Gateway all'endpoint del AWS servizio

Utilizzo di un endpoint VPC

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API all' AWS Backup endpoint VPC utilizzando il nome DNS predefinito per la regione, ad esempio. AWS `backup.us-east-1.amazonaws.com`

Tuttavia, per la regione Cina (Pechino) e la regione Cina (Ningxia) Regioni AWS, le richieste API devono essere effettuate con l'endpoint VPC utilizzando e, rispettivamente. `backup.cn-north-1.amazonaws.com.cn` `backup.cn-northwest-1.amazonaws.com.cn`

Per ulteriori informazioni, consulta Accesso a un servizio tramite un endpoint di interfaccia nella Guida per l'utente di Amazon VPC.

Creazione di una policy degli endpoint VPC

Puoi allegare una policy di endpoint all'endpoint VPC che controlla l'accesso all'API di Amazon Backup. La policy specifica:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

> **Important**
>
> Quando viene applicata una policy non predefinita a un endpoint VPC di interfaccia AWS Backup per, alcune richieste API non riuscite, come quelle non `RequestLimitExceeded` riuscite, potrebbero non essere registrate su Amazon. AWS CloudTrail CloudWatch

Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Esempio: policy degli endpoint VPC per le azioni AWS Backup

Di seguito è riportato un esempio di policy sugli endpoint per. AWS Backup Se associata a un endpoint, questa policy garantisce l'accesso alle AWS Backup azioni elencate per tutti i principi su tutte le risorse.

```
{
```

```
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

Esempio: policy endpoint VPC che nega tutti gli accessi da un account AWS specificato

La seguente politica degli endpoint VPC nega all' AWS account `123456789012` tutti gli accessi alle risorse che utilizzano l'endpoint. La policy consente tutte le operazioni da altri account.

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

Per ulteriori dettagli sulle risposte API disponibili, consulta la Guida alle API.

La disponibilità AWS Backup attualmente supporta gli endpoint VPC nelle seguenti regioni: AWS

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)
- Regione Stati Uniti occidentali (Oregon)

- Regione Stati Uniti occidentali (California settentrionale)
- Regione Africa (Città del Capo)
- Regione Asia Pacifico (Hong Kong)
- Regione Asia Pacifico (Mumbai)
- Regione Asia Pacifico (Osaka-Locale)
- Regione Asia Pacifico (Seoul)
- Regione Asia Pacifico (Singapore)
- Regione Asia Pacifico (Sydney)
- Regione Asia Pacifico (Tokyo)
- Regione Canada (Centrale)
- Regione Europa (Francoforte)
- Regione Europa (Irlanda)
- Regione Europa (Londra)
- Regione Europa (Parigi)
- Regione Europa (Stoccolma)
- Regione Europa (Milano)
- Regione Medio Oriente (Bahrein)
- Regione Sud America (San Paolo)
- Regione Asia Pacifico (Giacarta)
- Regione Asia Pacifico (Osaka-Locale)
- Regione Cina (Pechino)
- Regione Cina (Ningxia)
- AWS GovCloud (Stati Uniti orientali)
- AWS GovCloud (Stati Uniti occidentali)

> **Note**
>
> AWS Backup per VMware non è disponibile nelle regioni della Cina (Cina (Pechino) e regione Cina (Ningxia)) o nella regione Asia Pacifico (Giacarta).

Resilienza in AWS Backup

AWS Backup prende molto sul serio la sua resilienza e la sicurezza dei tuoi dati.

AWS Backup archivia i backup con una resilienza e una durata almeno pari a quelle offerte dal AWS servizio originale della risorsa, se ne facessi il backup.

AWS Backup è progettato per utilizzare l'infrastruttura AWS globale per replicare i backup su più zone di disponibilità per una durabilità del 99,99999% (11 nove) in un dato anno, a condizione che venga rispettata la documentazione corrente. AWS Backup

AWS Backup crittografa i piani di backup inattivi e ne esegue il backup continuo. Puoi anche limitare l'accesso ai tuoi piani di backup utilizzando credenziali e policy AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta le sezioni Autenticazione, Controllo dell'accesso e Best practice di sicurezza in IAM.

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. AWS Backup archivia i backup tra le zone di disponibilità. 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, consulta l'Accordo sul livello di servizio (SLA) di AWS Backup.

Inoltre, AWS Backup consente di copiare i backup tra le regioni per una resilienza ancora maggiore. Per ulteriori informazioni sulla funzionalità di copia AWS Backup tra aree geografiche, vedere Creazione di una copia di backup.

Per ulteriori informazioni sulle zone Regioni AWS di disponibilità, vedere AWS Global Infrastructure.

AWS Backup quote

Le seguenti quote si applicano quando si lavora con. AWS Backup Molte AWS Backup quote sono regolabili se consentite dal servizio di tipo di risorsa. Per richiedere un adeguamento della quota, descrivi il tuo caso d'uso in AWS Support.

AWS Backup quote

Risorsa	Quota	Note
Numero di vault di backup per regione per account	300	Puoi richiedere una regolazione.
Numero di punti di ripristino per vault di backup	1.000.000	Puoi richiedere una regolazione.
Numero di piani di backup per regione per account	300	Puoi richiedere una regolazione.
Numero di versioni per piano di backup	2.000	Puoi richiedere una regolazione.
Numero di assegnazioni di risorse per piano di backup	100	Non regolabile
Numero di processi di backup attivi per account	Illimitato	
Numero di copie di backup simultanee per account verso una regione di destinazione	100	Puoi richiedere un adeguamento per determinate risorse (attualmente macchine virtuali, database Advanced DynamoDB, Timestream, Amazon EFS e SAP HANA su istanze Amazon EC2)
Numero di copie simultanee per vault di backup di destinazione nell'account dopo che	5	Non regolabile

Risorsa	Quota	Note
il limite (voce precedente) è stato raggiunto		
Numero di copie tra account simultanee che possono essere eseguite della stessa risorsa nella stessa regione di destinazione	30	Non regolabile.
Numero di processi di copia e di backup simultanei per risorsa	1	Non regolabile. Questa quota consente di mantenere le prestazioni dei carichi di lavoro.
Numero di tag di metadati per backup	50	Non è possibile richiedere un adeguamento. AWS impone questa quota a tutte le risorse. Consulta Limiti e requisiti per la denominazione dei tag nei Riferimenti generali di AWS .
Numero di tag per selezione di risorse in una politica di backup tra account	30	Non regolabile. È possibile includere tag aggiuntivi utilizzando più assegnazioni di risorse o piani di backup.
Numero di hypervisor	10	Non regolabile
Numero di blocchi a fini legali	50 per account	Non regolabile
Numero massimo di livelli di backup nidificati di stack di applicazioni	10	Non regolabile

AWS Backup delle quote di risorse di Amazon Timestream

Risorsa	Quota	Note
Numero di processi di backup Timestream simultanei per account	4	Puoi richiedere una regolazione.
Numero di processi di ripristino Timestream simultanei per account	1	Puoi richiedere una regolazione.

Esistono quote per una singola assegnazione delle risorse in un'unica regola di backup. Puoi creare un piano di backup con più regole di backup.

AWS Backup Quote Audit Manager

Risorsa	Quota	Note
Numero di framework personalizzati per account per regione	15	Puoi richiedere una regolazione.
Numero di controlli per account per regione	50	Puoi richiedere una regolazione.
Numero di piani di report per account	20	Puoi richiedere una regolazione.
Numero di framework per piano di report	1.000	Non regolabile
Numero massimo di account moltiplicato per regioni in un piano di report	300	Non regolabile

Quote del piano di test di ripristino

Risorsa	Quota	Note
Piani di test di ripristino	100	Non regolabile
Numero di tag in ogni piano	50	Non regolabile
Selezioni per piano	30	Non regolabile
ARN per selezione del test di ripristino	30	Non regolabile
Condizioni per selezione	30	Include quelle contenute in `StringEquals` e `StringNotEquals`
Selettori di vault per la selezione del test di ripristino	30	Non regolabile
Valore massimo (in giorni) della finestra di selezione	365 giorni	
Limiti di ore della finestra di avvio	Minimo: 1 ora; massimo: 168 ore	
Lunghezza massima dei caratteri del nome del piano di test di ripristino	50 caratteri	Caratteri alfanumerici e di sottolineatura, senza spazi
Lunghezza massima dei caratteri del nome della selezione del test di ripristino	50 caratteri	Caratteri alfanumerici e di sottolineatura, senza spazi

AWS Backup gateway quote

Risorsa	Quota	Note
Processi di backup o ripristino per gateway	4	Non puoi richiedere una regolazione. Invece, crea più

Risorsa	Quota	Note
		gateway e connettili al tuo hypervisor.

Quando gestisci i backup su più account utilizzando AWS Organizations, potresti riscontrare delle quote che impongono. AWS Organizations Per queste quote, consulta Quote per AWS Organizations nella Guida per l'utente di AWS Organizations .

È inoltre possibile che si verifichino delle quote imposte da un servizio supportato, tra cui AWS Backup:

- Amazon Elastic File System
- Amazon Elastic Block Store
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon DynamoDB
- Amazon FSx per Lustre
- Amazon FSx per Windows File Server
- Amazon DocumentDB
- Amazon Neptune
- Amazon Simple Storage Service
- Amazon Timestream

Monitoraggio

AWS Backup funziona con altri AWS strumenti per consentirti di monitorarne i carichi di lavoro. Questi strumenti includono i seguenti:

- AWS Backup dashboard della console
  - Il pannello di controllo dei processi offre il monitoraggio dell'integrità del processo, in cui è possibile visualizzare le metriche che mostrano gli esiti positivi e negativi dei processi, filtrati per motivo, account, regione e tipo di risorsa.
  - La dashboard dei lavori è disponibile nelle regioni in cui è supportato AWS Backup Audit Manager. Consulta Disponibilità delle funzionalità tramite Regione AWS per l'elenco delle regioni. Tutte le altre regioni potranno accedere a CloudWatch Dashboard.
- Amazon CloudWatch e Amazon EventBridge per monitorare AWS Backup i processi.
  - Puoi utilizzarlo CloudWatch per tenere traccia delle metriche, creare allarmi e visualizzare dashboard.
  - È possibile utilizzare EventBridge per visualizzare e monitorare gli eventi. AWS Backup

  Per ulteriori informazioni, consulta Monitoraggio AWS Backup degli eventi tramite Amazon EventBridge.
- AWS CloudTrailper monitorare le chiamate AWS Backup API. Puoi identificare ora, IP di origine, utenti e account che effettuano tali chiamate. Per ulteriori informazioni, consulta Registrazione delle chiamate API con AWS Backup CloudTrail.
- Amazon Simple Notification Service (Amazon SNS) per abbonarsi ad argomenti AWS Backup correlati come eventi di backup, ripristino e copia. Per ulteriori informazioni, consulta Opzioni di notifica con AWS Backup.

AWS Backup dashboard della console

> **Note**
>
> La dashboard dei lavori è disponibile in tutte le regioni in cui è supportato AWS Backup Audit Manager. Consulta Disponibilità delle funzionalità tramite Regione AWS per l'elenco delle regioni. Tutte le altre regioni potranno accedere a CloudWatch Dashboard.

Argomenti

Panoramica dei pannelli di controllo di Backup

AWS Backup fornisce una dashboard Jobs nella console per aiutarti a monitorare lo stato dei processi di backup, copia e ripristino. Gli stessi dati visualizzati visivamente nella console possono essere recuperati nella riga di comando tramite AWS CLI.

Il pannello di controllo dei processi può essere utilizzato per identificare problemi relativi ai processi di backup, copia e ripristino tramite il monitoraggio a livello di organizzazione o degli account membro. Con queste informazioni, puoi individuare e diagnosticare eventi e possibili problemi per garantire l'attendibilità delle tue attività.

Il pannello di controllo dei processi può visualizzare i dati di due intervalli di tempo. Per impostazione predefinita, vengono visualizzati i dati degli ultimi 14 giorni, ma è possibile modificare la visualizzazione per mostrare i dati degli ultimi 7 giorni. Se modifichi l'intervallo di tempo, i dati verranno aggiornati in base alla nuova impostazione.

Tieni presente che il pannello di controllo mostra gli ultimi dati fino alle 0:00 UTC, ovvero i dati del giorno corrente non sono inclusi. Il pannello di controllo si aggiorna ogni giorno tra le 1:30 e le 2:30 UTC circa.

Visualizzazione del pannello di controllo dei processi

Per visualizzare la dashboard dei lavori, accedi alla AWS Backup console e seleziona Jobs dashboard nella barra di navigazione a sinistra.

Nella pagina del pannello di controllo dei processi puoi selezionare i processi nella scheda dei processi di backup, copia o ripristino.

La panoramica del pannello di controllo dei processi mostra la vista aggregata relativa all'intervallo di tempo specificato per l'attività dei processi, inclusi i processi completati, completati con problemi, scaduti e non riusciti. Per impostazione predefinita, vengono visualizzati i dati degli ultimi 14 giorni, ma è possibile modificare la visualizzazione per mostrare i dati di 7 giorni.

> **Note**
>
> `Completed with issues` è lo stato di un processo visualizzato nella console indicante che è stato completato con un messaggio di stato.

Integrità del processo

Il grafico a linee mostra le percentuali di processi riusciti e non riusciti nel tempo. La linea della percentuale di processi riusciti mostra l'aggregazione dei processi completati e di quelli completati con problemi. La linea relativa alla percentuale di processi non riusciti mostra la somma dei processi non riusciti e scaduti in base all'intervallo di tempo specificato.

I processi nello stato non completato o diverso da non riuscito (processi con stato creato, in attesa, in esecuzione, interrotto, interruzione in corso o parziale) non sono inclusi e le percentuali totali potrebbero non essere uguali a 100%.

Stato del processo nel tempo

Puoi generare un grafico a barre personalizzato che mostra il numero di processi in ogni categoria (completato, completo con problemi, non riuscito e scaduto), distribuiti in base ai giorni.

Con i menu a discesa, scegli gli stati, i tipi di risorse e AWS le regioni che desideri visualizzare nel grafico. Se desideri approfondire la selezione, scegli Visualizza processi per vedere una visualizzazione prefiltrata della pagina di monitoraggio dei processi multi-account.

Puoi passare il mouse su una barra per visualizzare un popup che mostra i dati dettagliati del processo per la data selezionata.

Processi problematici

Un processo problematico ha lo stato non riuscito, scaduto o completato con problemi. Ogni grafico mostra la metrica corrispondente che contiene gli account, i tipi di risorse o i motivi principali relativi al maggior numero di processi problematici.

La visualizzazione predefinita dispone il widget del pannello di controllo in base alla metrica specificata in ordine decrescente, a partire dalla metrica con il maggior numero di processi problematici.

La visualizzazione dei principali account problematici è visibile solo negli account che dispongono dell'accesso tramite Organizations, come gli account amministrativi e gli account amministratore

delegato. Se visibile, puoi passare il mouse su un account per visualizzare il numero dei relativi processi problematici.

Puoi selezionare una barra all'interno del grafico per aprire una finestra popup in cui puoi scegliere lo stato di un processo per visualizzare una tabella di monitoraggio dei processi multi-account filtrata in base allo stato selezionato.

Motivi dei processi problematici

Il widget Principali motivi problematici mostra la categoria di codici a cui appartengono i messaggi di errore. Tuttavia, la categoria potrebbe non spiegare i problemi riscontrati da un processo. Espandi le seguenti categorie di codici di messaggio per visualizzare maggiori dettagli sui messaggi o sugli errori specifici che potrebbero verificarsi nei processi.

"VSS_ERROR"

- "Windows VSS Backup attempt failed because either Instance or SSM Agent has invalid state or insufficient privileges."
- "Windows VSS Backup attempt failed because of insufficient privileges to perform this operation."
- "Windows VSS Backup attempt failed because ec2-vss-agent.exe is not installed in the Instance."
- "Windows VSS Backup Job Error encountered, trying for regular backup."
- "Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation."
- "Windows VSS Backup attempt failed because of unsupported Windows Server version. Supported Versions are Windows Server 2012 or later."
- "Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation."

"LIMIT_EXCEEDED"

- "Subscriber limit exceeded: You have reached the maximum concurrent number of backups, which is 300. Wait until other jobs finish, and try again. Puoi anche contattarci AWS Support per richiedere un aumento della quota».
- "Maximum allowed in-progress snapshots for a single volume exceeded."
- "Maximum allowed active snapshot limit exceeded."
- "Cannot create more than 20 user snapshots."
- "The resultant tag set must not have more than 50 user tags."

- "You have reached the maximum supported backups for your account/database. See Quotas in the Timestream developer guide for additional information."
- "You have reached your quota of 50,000 for the number of public and private images allowed in this Region. Deregister unused images, or request an increase in your AMI quota."
- «Il backup è riuscito, ma non siamo riusciti a mantenere NetworkInterfaces i metadati perché le loro dimensioni superavano i nostri limiti interni».
- "REGEX#subscriber limit exceeded"
- "REGEX#More than 50 tags specified"
- "REGEX#can have at most"

"ACCESS_DENIED"

- "You are not authorized to perform this operation."
- «Accesso negato. Tentativo di chiamata al servizio» AWS Backup
- «Le immagini di Marketplace AWS non possono essere copiate su un altro AWS account».
- "Copy job failed because the destination Backup vault is encrypted with the default Backup service managed key. The contents of this vault cannot be copied. È possibile copiare solo il contenuto di un archivio di Backup crittografato da una AWS KMS chiave.
- Le istantanee crittografate con non Chiave gestita da AWS possono essere condivise. Specify another snapshot."
- "Encrypted snapshots with Amazon EBS default key cannot be shared."
- "Copy job failed. Both source and destination account must be a member of the same organization."
- "REGEX#access denied"
- "REGEX#not authorized to"
- «REGEX #cannot» deve essere assunto da AWS Backup
- "REGEX#does not have permission"
- "REGEX#missing permission"

"CONCURRENT_JOB"

- "Backup job failed because there was a running job for the same resource."

"FEATURE_NOT_ENABLED"

- "Copy job failed. Cross-account copy feature is not enabled for the current organization."

"JOB_EXPIRED"

- "Backup job expired before completion."

"INVALID_LIFECYCLE"

- "Copy job failed. The retention specified in the job is not within the range specified for the target Backup Vault."
- "REGEX#could not start because it is either inside or too close to the weekly maintenance window configured."
- "REGEX#could not start because it is either inside or too close to the automated backup window configured."

"INVALID_STATE"

- "REGEX#Instance is not in state"
- "REGEX#not in the available state"
- "REGEX#not in available state"
- "REGEX#Cannot snapshot volume"

"KMS_KEY_ERROR"

- "KMS key is either disabled or pending deletion or access to KMS key is denied"
- "Given key ID is not accessible"
- "AMI snapshot copy failed with error: Given key ID is not accessible. È necessario disporre DescribeKey delle autorizzazioni sulla CMK predefinita»
- "REGEX#kms key"

"ACCESS_KEY_ERROR"

- «L' AWS Access Key Id richiede un abbonamento per il servizio»

"HYPERVISOR_OFFLINE"

- "This operation is not valid for the specified hypervisor because it is not online"

"RESOURCE_NOT_FOUND"

- "The specified volume was not found."
- "The virtual machine is not found."
- "Given key ID does not exist"
- "REGEX#does not exist"
- "REGEX#Could not find resource"
- "REGEX#Could not find cryopod"
- "REGEX#Cannot find recovery point"
- "REGEX#resource not found"
- "REGEX#no longer available"
- "REGEX#is invalid"

"RESOURCE_NOT_SUPPORTED"

- "REGEX#unsupported resource type"
- "REGEX#Unsupported resource type"

"TAG_COPY_ERROR"

- "We are unable to copy resource tags to your backup because of the Internal Failure."
- "We are unable to copy resource tags to your backup because source or destination recovery point is unavailable."

"TOKEN_EXPIRED"

- "Token expired. Try again."

"UNSUPPORTED_OPERATION"

- «CreateSnapshot metodo non supportato sull'hypervisor durante la creazione di istantanee. Aborted backup job."
- «UnsupportedOperation : Le copie di backup di Storage Gateway richiedono un archivio di backup creato dall'utente e un CMK a destinazione.»
- "REGEX#Feature is not supported for provided resource type."

"FATAL_ERROR"

- "An internal error occurred."
- "Copy job encountered a fatal error. Contatta il AWS Support per ulteriore assistenza».
- "Copy job encountered a fatal error."
- "REGEX#Backup job encountered a fatal error"

Acquisizione dei dati del dashboard tramite AWS CLI

È possibile utilizzare la riga di comando per recuperare gli stessi dati visualizzati nella console. Utilizza uno dei seguenti comandi della CLI:

- `list-backup-job-summaries`
- `list-copy-job-summaries`
- `list-restore-job-summaries`

Sono disponibili parametri validi che puoi includere in ogni comando:

```
BackupJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

CopyJobSummaries (list)
```

```
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

RestoreJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
AggregationPeriod: (string),
NextToken (string)
```

Questo esempio mostra una richiesta in cui l'input dell'utente è `list-backup-job-summaries` e la richiesta chiede di restituire tutti gli account disponibili con lo stato `FAILED` nei 14 giorni precedenti:

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

Per ottenere il numero di processi con stato `completed with issues`, sottrai il numero totale di processi `COMPLETED` con `MessageCategory` pari a `SUCCESS` dal numero totale di processi `COMPLETED`.

Monitoraggio AWS Backup degli eventi tramite Amazon EventBridge

AWS Backup invia eventi ad Amazon EventBridge quando lo stato di un processo di backup o copia cambia. Puoi utilizzarlo EventBridge per monitorare AWS Backup gli eventi. Ad esempio, è possibile ricevere un allarme quando un processo di backup fallisce. AWS Backup emette eventi con la EventBridge massima diligenza ogni 5 minuti.

Per tenere traccia degli eventi utilizzando EventBridge, consulta quanto segue:

- Creazione di una regola che reagisce agli eventi (Amazon EventBridge User Guide)

- Amazon CloudWatch Events and Metrics per AWS Backup (blog: consulta Configurare AWS Backup gli eventi da inviare ad Amazon EventBridge)

Alcuni eventi segnalano `status: COMPLETED` mentre altri eventi segnalano `state: COMPLETED`. Ciò è coerente con l' AWS Backup API. Alcuni stati sono specifici della AWS Backup console: lo `Completed with issues` stato è una rappresentazione dei `Completed` lavori con messaggi di stato. Per monitorare gli eventi `Completed with issues`, controlla i processi `COMPLETED` che hanno un messaggio di stato.

In alternativa, puoi utilizzare l'API di AWS Backup notifica per tenere traccia AWS Backup degli eventi con Amazon Simple Notification Service (Amazon SNS). Tuttavia, EventBridge tiene traccia di più modifiche rispetto all'API di notifica, incluse le modifiche agli archivi di backup, allo stato del processo di copia, alle impostazioni regionali e al numero di punti di ripristino freddi o caldi.

Eventi

- Eventi Backup Job
- Eventi del piano di Backup
- Eventi Backup Vault
- Eventi Copy Job
- Eventi Recovery Point
- eventi Region Settings
- Eventi Restore Job

Eventi Backup Job

Di seguito sono riportati alcuni esempi di eventi.

Stato

- Stato: FALLITO
- Stato: COMPLETATO
- Stato: IN ESECUZIONE
- Stato: INTERROTTO
- Stato: SCADUTO
- Stato: IN SOSPESO

- Stato: CREATO

Stato: FALLITO


```
{
  "version": "0",
  "id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:15:26Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "34176239-e96d-4e1d-9fad-529dbb3c3556",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:13:07.392Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "FAILED",
    "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us-
west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86 does not exist.
\"",
    "startBy": "2020-07-30T04:13:07.392Z",
    "percentDone": 0,
    "retryCount": 3
  }
}
```


Stato: COMPLETATO


```
{
  "version": "0",
  "id": "dafac799-9b88-0134-26b7-fef4d54a134f",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:41:17Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:f1d966fe-a3bd-410b-
b292-99f442d13b56"
  ],
  "detail": {
    "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",
    "backupSizeInBytes": "36048",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "bytesTransferred": "36048",
    "creationDate": "2020-07-15T21:40:31.207Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T21:41:05.921Z",
    "startBy": "2020-07-16T05:40:31.207Z",
    "percentDone": 100,
    "retryCount": 3
  }
}
```

Stato: IN ESECUZIONE

```
{
  "version": "0",
  "id": "44946c39-b519-3505-44e6-ba74afeb2e30",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:39:13Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
    "backupSizeInBytes": "3221225472",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:38:31.152Z",
```

```
    "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-0b5ae24f2ee72d926",
    "resourceType": "EBS",
    "state": "RUNNING",
    "startBy": "2020-07-16T05:00:00Z",
    "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
    "percentDone": 99,
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    }
  }
}
```

Stato: INTERROTTO

```
{
  "version": "0",
  "id": "4c91ceb0-b798-da82-6818-c29b3dce7543",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:33:16Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "backupVaultName": "f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:33:00.803Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "ABORTED",
    "statusMessage": "\"Backup job was stopped by user.\"",
    "completionDate": "2020-07-15T21:33:01.621Z",
    "startBy": "2020-07-16T05:33:00.803Z",
    "percentDone": 0
```

```
  }
}
```

Stato: SCADUTO

```
{
  "version": "0",
  "id": "1d7bbc04-6120-1145-13b9-49b0af465328",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T13:04:57Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:aws/backup/
AutomatedBackupVaultDel2",
    "backupVaultName": "aws/backup/AutomatedBackupVaultDel2",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T05:10:20.077Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "EXPIRED",
    "statusMessage": "\"Backup job failed because there was a running job for the same
 resource.\"",
    "completionDate": "2020-07-29T13:02:15.234Z",
    "startBy": "2020-07-29T13:00:00Z",
    "percentDone": 0,
    "createdBy": {
      "backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:aws/
efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00NjhlLWIzMTEtNWRjOWY0YTNjN2Vj",
      "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11dc2"
    }
  }
}
```

Stato: IN SOSPESO

```
{
```

```
  "version": "0",
  "id": "64dd1897-f863-31a3-9ee5-b05e306d81ff",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:03:30Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "2cffdb68-d6ed-485f-9f9b-8b530749f1c2",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ed1f2661-5587-48bf-8a98-fadb977bf975",
    "backupVaultName": "ed1f2661-5587-48bf-8a98-fadb977bf975",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:01:06.224Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "PENDING",
    "statusMessage": "",
    "startBy": "2020-07-30T04:01:06.224Z",
    "percentDone": 0
  }
}
```


Stato: CREATO


```
{
  "version": "0",
  "id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T20:32:53Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
    "state": "CREATED",
    "creationDate": "2020-06-22T20:32:47.466Z"
  }
}
```

Eventi del piano di Backup

Di seguito sono riportati alcuni esempi di eventi.

Stato

- Stato: MODIFICATO
- Stato: ELIMINATO
- Stato: CREATO

Stato: MODIFICATO

```
{
  "version": "0",
  "id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "modifiedAt": "2020-06-24T23:18:19.168Z",
    "state": "MODIFIED"
  }
}
```

Stato: ELIMINATO

```
{
  "version": "0",
  "id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "deletionDate": "2020-06-24T23:18:19.411Z",
    "state": "DELETED"
  }
}
```

Stato: CREATO

```
{
  "version": "0",
  "id": "b64fb2d0-ae16-ff9a-faf6-0bdd0d4bfdef",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-
d3afa4c84f59"
  ],
  "detail": {
    "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",
    "versionId": "N2Q4OTczMzEtZmY1My00N2UwLWE3ODUtMjViYWYyOTUzZWY4",
    "creationDate": "2020-06-24T23:18:15.318Z",
    "state": "CREATED"
  }
}
```

Eventi Backup Vault

Di seguito sono riportati alcuni esempi di eventi.

Stato

- Stato: CREATO
- Stato: MODIFICATO

- Stato: ELIMINATO

Stato: CREATO

```
{
  "version": "0",
  "id": "d415609e-5f35-d9a2-76d1-613683e4e024",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:d8864642-155c-4283-a168-
a04f40e12c97"
  ],
  "detail": {
    "backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
    "state": "CREATED"
  }
}
```

Stato: MODIFICATO

```
{
  "version": "0",
  "id": "1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:nameOfTestBackup"
  ],
  "detail": {
    "backupVaultName": "vaultName",
    "state": "MODIFIED",
    "isLocked": "true"
  }
}
```

Stato: ELIMINATO

```
{
  "version": "0",
  "id": "344bccc1-6d2e-da93-3adf-b3f82460294d",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T02:42:37Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:e8189629-1f8e-4ed2-af7d-
b32415d04db1"
  ],
  "detail": {
    "backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
    "state": "DELETED"
  }
}
```

Eventi Copy Job

Di seguito sono riportati alcuni esempi di eventi.

Stato

- Stato: FALLITO
- Stato: IN ESECUZIONE
- Stato: COMPLETATO
- Stato: CREATO

Stato: FALLITO

```
{
  "version": "0",
  "id": "4660bc92-a44d-c939-4542-cda503f14855",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:37:34Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-00179b33a7a88cac5"
  ],
  "detail": {
    "copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
    "backupSizeInBytes": 22548578304,
    "creationDate": "2020-07-15T20:36:13.239Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "state": "FAILED",
    "statusMessage": "Access denied exception while trying to list tags",
    "completionDate": "2020-07-15T20:37:28.704Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "destinationRecoveryPointArn": {}
  }
}
```

Stato: IN ESECUZIONE

```
{
  "version": "0",
  "id": "d17480ae-7042-edb2-0ff5-8b94822c58e4",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:07:48Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
```

```
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "RUNNING",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": {},
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

Stato: COMPLETATO

```
{
  "version": "0",
  "id": "47deb974-6473-aef1-56c2-52c3eaedfceb",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:08:04Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T22:07:58.111Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
```

```
    "destinationRecoveryPointArn": "arn:aws:ec2:us-west-2::snapshot/
snap-0726fe70935586180",
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

Stato: CREATO

```
{
  "version": "0",
  "id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T21:06:32Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-0888b126e2170b98e"
  ],
  "detail": {
    "creationDate": "2020-06-22T21:06:25.754Z",
    "state": "CREATED",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17"
  }
}
```

Eventi Recovery Point

Di seguito sono riportati alcuni esempi di eventi.

Stato

- Stato: COMPLETATO
- Stato: ELIMINATO

- Stato: MODIFICATO

Stato: COMPLETATO


```
{
    "version": "0",
    "id": "ab32977c-378d-2122-e985-fgh4596f0709",
    "detail-type": "Recovery Point State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-07-15T21:39:07Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-
d60e-00c2-5c3b-49960142d03b"
    ],
    "detail": {
        "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "creationDate": "2020-07-15T21:38:31.152Z",
        "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
        "resourceType": "Aurora",
        "resourceArn": "arn:aws:rds:us-west-2:1112233445566:cluster:id",
        "status": "COMPLETED",
        "isEncrypted": "false",
        "storageClass": "WARM",
        "completionDate": "2020-07-15T21:39:05.689Z",
        "createdBy": {
            "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
            "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
        },
        "lifecycle": {
            "deleteAfterDays": 100
        },
        "calculatedLifeCycle": {
            "deleteAt": "2020-10-23T21:38:31.152Z"
        }
    }
```

```
}
```

Stato: ELIMINATO

```
{
  "version": "0",
  "id": "6089ee76-d856-0d7c-cee7-0a431cd43343",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T22:38:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:157f892e-
fe46-48da-9dbe-4154f91f8acc",
    "arn:aws:rds:us-west-2:1112233445566:snapshot:awsbackup:job-c1a6d40a-32d1-4d54-
bd70-bced933ef107"
  ],
  "detail": {
    "state": "DELETED",
    "lifecycle": {
      "deleteAfterDays": 300
    },
    "calculatedLifeCycle": {
      "deletedAt": "2021-05-25T22:29:02.452Z"
    }
  }
}
```

Stato: MODIFICATO

```
{
  "version": "0",
  "id": "14365bb1-adef-bc00-1ee3-8fac188d7996",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-02T23:33:57Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:helo12312",
    "arn:aws:dynamodb:us-west-2:1112233445566:table/test/
backup/01593730512469-033578ce"
```

```
  ],
  "detail": {
    "calculatedLifeCycle": {
      "toColdStorageAfterDays": "Fri Dec 04 22:55:11 UTC 2020"
    },
    "state": "MODIFIED"
  }
}
```

eventi Region Settings

Di seguito è riportato un esempio di evento.

```
{
  "version": "0",
  "id": "e7ed82ba-4955-4de5-10d6-dbafcfb68b4f",
  "detail-type": "Region Setting State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T22:55:03Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "modifiedAt": "2020-06-24T22:54:57.161Z",
    "ResourceTypeOptInPreference": {
      "Aurora": true
    },
    "state": "MODIFIED"
  }
}
```

Eventi Restore Job

Di seguito sono riportati alcuni esempi di eventi.

Stato

- Stato: FALLITO
- Stato: IN ESECUZIONE
- Stato: COMPLETATO
- Stato: IN SOSPESO

- Stato: CREATO

Stato: FALLITO


```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:19:29Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-12b3456dfb7f8cf90"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "22548578304",
    "creationDate": "2020-07-15T20:19:07.303Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/TestAWSBackupRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "FAILED",
    "statusMessage": "AWS Backup does not permit attaching a new instance profile to an
 EC2 instance. Please restore using the backed up instance profile."
  }
}
```


Stato: IN ESECUZIONE


```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:26:06Z",
  "region": "us-west-2",
```

```
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-0fe123ca456cfad7c"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "3221225472",
    "creationDate": "2020-07-29T20:26:00.098Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EBS",
    "status": "RUNNING"
  }
}
```

Stato: COMPLETATO

```
{
  "version":"0",
  "id":"ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type":"Restore Job State Change",
  "source":"aws.backup",
  "account":"1112233445566",
  "time":"2020-07-15T03:14:58Z",
  "region":"us-west-2",
  "resources":[
    "arn:aws:rds:us-
west-2:1112233445566:snapshot:awsbackup:job-1a2bcd34-567e-8901-23f4-5g6hijkl7890"
  ],
  "detail":{
    "restoreJobId":"AB123456-78C9-0123-456D-789012E34567",
    "backupSizeInBytes":"0",
    "creationDate":"2020-07-15T03:10:01.742Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn":"arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone":0,
    "resourceType":"RDS",
```

```
    "status":"COMPLETED",
    "createdResourceArn":"arn:aws:rds:us-
west-2:1112233445566:db:testinginstance1a2bcd34-567e-8901-23f4-5g6hijkl7890",
    "completionDate":"2020-07-15T03:14:53.128Z"
  }
}
```

Stato: IN SOSPESO

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:08:26Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-
b29f4edb47b1"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "backupSizeInBytes": "36048",
    "creationDate": "2020-07-29T20:08:21.083Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "PENDING"
  }
}
```

Stato: CREATO

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
```

```
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T18:50:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:a6560b33-3660-494c-8d47-
efgh939ij32k"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "creationDate": "2020-06-22T18:50:46.407Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "state": "CREATED"
  }
}
```

AWS Backup metriche con Amazon CloudWatch

Argomenti

- CloudWatch Dashboard
- Metriche con CloudWatch

CloudWatch Dashboard

> **Note**
>
> Il pannello di controllo della console dipende da quale regione si accede alla console. Consulta Disponibilità delle funzionalità tramite Regione AWS per vedere quali regioni hanno accesso al pannello di controllo dei processi. Le regioni non elencate potranno accedere alla CloudWatch dashboard.

La AWS Backup console include una dashboard per visualizzare le metriche relative ai processi di backup, copia e ripristino completati o non riusciti. All'interno di questo pannello di controllo, puoi visualizzare lo stato del processo per periodo di tempo, personalizzato in base all'intervallo di tempo desiderato.

PER ACCEDERE AL PANNELLO DI CONTROLLO

1. Apri la AWS Backup console all'indirizzo https://console.aws.amazon.com/backup.
2. Nel pannello di navigazione a sinistra, seleziona Pannello di controllo.

VISUALIZZARE E COMPRENDERE IL PANNELLO DI CONTROLLO

La CloudWatch dashboard mostra diversi widget. Ogni widget visualizza le metriche del processo in base al conteggio. Ogni widget visualizza diversi grafici a linee. Ogni riga corrisponde a una risorsa protetta (se una risorsa prevista non viene visualizzata, assicurati che la risorsa sia attivata in Impostazioni). Le visualizzazioni non mostrano i processi in corso.

L'asse y (valori verticali) visualizza il conteggio. L'asse x (valori orizzontali) visualizza momenti specifici. Se lo stato del processo selezionato non contiene punti dati da visualizzare, il valore verrà impostato su 0 con una linea orizzontale sull'asse x. La legenda che mostra le risorse sarà ancora visibile.

Le metriche visualizzano informazioni specifiche dell'account e della regione correlate all'accesso corrente. Per visualizzare altri account o regioni, devi accedere con l'account scelto.

PERSONALIZZAZIONE DEL PANNELLO DI CONTROLLO

Per impostazione predefinita, viene visualizzato un intervallo di tempo di una settimana. Nel menu in alto, sono disponibili opzioni per ridefinire l'intervallo di tempo visualizzato. Puoi scegliere tra 1 ora, 3 ore, 12 ore, 1 giorno, 3 giorni e 1 settimana. Inoltre, puoi selezionare Personalizzato per specificare un valore diverso. La personalizzazione modificherà temporaneamente la vista corrente in base alle specifiche dell'utente.

Puoi passare il mouse su un widget per visualizzare un pulsante Ingrandisci nell'angolo in alto a destra del widget. Fai clic su Ingrandisci per aprire il widget nella visualizzazione a schermo intero. In modalità a schermo intero, sono disponibili più opzioni per personalizzare la visualizzazione del grafico, come la modifica del periodo (il tempo tra tutti i punti dati). Le eventuali modifiche non verranno mantenute quando la visualizzazione a schermo intero viene chiusa.

Per visualizzare solo un tipo di risorsa alla volta, fai clic sul testo dell'etichetta del tipo di risorsa che desideri visualizzare nella legenda del grafico. Questa operazione deselezionerà tutti gli altri tipi di risorse. Per invertire questa operazione, fai clic sulla casella di colore del tipo di risorsa nella legenda. Per tornare alla visualizzazione predefinita di tutti i tipi di risorse con tutte le etichette selezionate, fai nuovamente clic sul testo dell'etichetta di qualsiasi tipo di risorsa selezionato.

Facendo clic sui tre punti verticali nell'angolo in alto a destra di un widget, viene visualizzato un menu a discesa con le opzioni per aggiornare, ingrandire, visualizzare nelle metriche e visualizzare nei log. «Visualizza nelle metriche» apre la metrica utilizzata nel widget nella console. CloudWatch Qui puoi apportare modifiche al widget e aggiungere il widget a una dashboard personalizzata nella CloudWatch dashboard. Qualsiasi modifica apportata nella CloudWatch dashboard non si rifletterà sulla dashboard in AWS Backup Console. «Visualizza come registri» apre la pagina di visualizzazione dei registri nella CloudWatch console.

Per aggiungere i widget visualizzati alla tua CloudWatch dashboard personalizzata, fai clic sul pulsante Aggiungi alla dashboard situato in alto a destra della dashboard. Si aprirà la CloudWatch console in cui potrai selezionare in quale dashboard personalizzata aggiungere tutti e sei i widget.

Per ulteriori informazioni, consulta Usare i CloudWatch parametri di Amazon.

Metriche con CloudWatch

È possibile utilizzare CloudWatch per monitorare le AWS Backup metriche. Il `AWS/Backup` namespace consente di tenere traccia delle seguenti metriche. AWS Backup emette metriche aggiornate ogni 5 minuti. CloudWatch

Lo scopo di questa pagina di documentazione è fornire i materiali di riferimento da utilizzare CloudWatch per il monitoraggio. AWS BackupPer scoprire come monitorare una metrica utilizzando CloudWatch, consulta il blog Amazon CloudWatch Events and Metrics for AWS Backup o Focus on Metrics and Alarms in a Single AWS Service nella Guida per l'utente. CloudWatch Per impostare gli allarmi, consulta Using Amazon CloudWatch Alarms nella Guida per l'CloudWatch utente.

Categoria	Parametri	Dimensioni di esempio	Esempio di caso d'uso
Processi	Numero di processi di backup, ripristino e copia in ogni stato, inclusi `CREATED`, `PENDING`, `RUNNING`, `ABORTED`, `COMPLETED` , `FAILED` e `EXPIRED`.	Tipo di risorsa, nome del vault. Il nome del vault di processi di copia è quello del relativo vault di destinazione.	Monitorare il numero di processi di backup non riusciti all'interno di uno o più vault di backup specifici. Se ci sono più di cinque processi non riusciti in un'ora, inviare un'e-mail o un SMS mediante Amazon

Categoria	Parametri	Dimensioni di esempio	Esempio di caso d'uso
	I diversi tipi di processi hanno diversi stati disponibili.		SNS o aprire un ticket al team di progettazione per analizzare la situazione. Criteri di segnalazione: è presente un valore diverso da zero
Punti di ripristino	Numero di punti di ripristino caldi e freddi in ogni stato: `MODIFIED`, `COMPLETED` , `PARTIAL`, `EXPIRED`, `DELETED`.	Tipo di risorsa, nome del vault.	Monitorare il numero di punti di ripristino eliminati per i volumi Amazon EBS e monitorare separatamente il numero di punti di ripristino caldi e freddi in ogni vault di backup. Criteri di segnalazione: è presente un valore diverso da zero

> **Note**
>
> Lo stato del lavoro di `Completed with issues` è specifico solo per la AWS Backup console; non può essere monitorato tramite. CloudWatch

Nelle seguenti tabelle vengono elencati le metriche disponibili per l'utente.

Parametro	Descrizione
`NumberOfBackupJobsCreated`	Il numero di job di backup AWS Backup creati.

Parametro	Descrizione
`NumberOfBackupJobsPending`	Il numero di processi di backup che verranno eseguiti in AWS Backup.
`NumberOfBackupJobsRunning`	Il numero di processi di backup attualmente in esecuzione AWS Backup.
`NumberOfBackupJobsAborted`	Il numero di processi di backup annullati dall'utente.
`NumberOfBackupJobsCompleted`	Il numero di processi di backup AWS Backup completati.
`NumberOfBackupJobsFailed`	Il numero di processi di backup con stato di `Failed`. Spesso causato dalla pianificazione di un processo di backup durante o 1 ora prima di una risorsa di database o 4 ore prima o durante una finestra di manutenzione di Amazon FSx o una finestra di backup automatizzato e non AWS Backup utilizzato per eseguire backup point-in-time continui per i ripristini. Consulta Point-in-Time Recovery per un elenco dei servizi supportati e istruzioni su come utilizzar li per eseguire backup continui o AWS Backup riprogrammare i processi di backup.
`NumberOfBackupJobsExpired`	Il numero di processi di backup con uno stato di. `EXPIRED` Un job di backup cambia dallo stato `CREATED` a `EXPIRED` se un backup non può iniziare entro la finestra di avvio.
`NumberOfCopyJobsCreated`	Il numero di processi di copia tra account e tra regioni creati da AWS Backup .

Parametro	Descrizione
NumberOfCopyJobsRunning	Il numero di processi di copia tra account e tra regioni attualmente in esecuzione in AWS Backup.
NumberOfCopyJobsCompleted	Il numero di processi di copia tra account e tra regioni terminati da AWS Backup .
NumberOfCopyJobsFailed	Il numero di operazioni di copia tra account e regioni diverse che sono state AWS Backup tentate ma non sono state completate.
NumberOfRestoreJobsPending	Il numero di processi di ripristino che verranno eseguiti in AWS Backup.
NumberOfRestoreJobsRunning	Il numero di processi di ripristino attualmente in esecuzione. AWS Backup
NumberOfRestoreJobsCompleted	Il numero di processi di ripristino AWS Backup completati.
NumberOfRestoreJobsFailed	Il numero di processi di ripristino che sono AWS Backup stati tentati ma non sono stati completat i.
NumberOfRecoveryPointsCompleted	Il numero di punti di ripristino AWS Backup creati.
NumberOfRecoveryPointsPartial	Il numero di punti di ripristino che sono AWS Backup stati creati ma che non sono stati completati. AWS riprova il processo in un secondo momento, ma poiché il nuovo tentativo viene eseguito in un secondo momento, mantiene il punto di ripristino parziale.

Parametro	Descrizione
`NumberOfRecoveryPointsExpired`	Il numero di punti di ripristino che AWS Backup hanno tentato di eliminare in base al ciclo di vita di conservazione dei backup, ma che non sono riusciti a eliminare. Il costo dello storage consumato dai backup scaduti viene addebitat o, pertanto è consigliabile eliminarli manualmen te.
`NumberOfRecoveryPointsDeleting`	Il numero di punti di ripristino da eliminare. AWS Backup
`NumberOfRecoveryPointsCold`	Il numero di punti di ripristino passati AWS Backup alla conservazione a freddo.

Sono disponibili altre dimensioni oltre a quelle elencate nella tabella. Per visualizzare tutte le dimensioni di una metrica, digita il nome di quella metrica nello spazio dei `AWS/Backup` nomi della sezione Metriche della console. CloudWatch

Registrazione delle chiamate API con AWS Backup CloudTrail

AWS Backup è integrato con AWS CloudTrailun servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un Servizio AWS servizio. CloudTrail acquisisce tutte le chiamate API AWS Backup come eventi. Le chiamate acquisite includono chiamate dalla AWS Backup console e chiamate di codice alle operazioni AWS Backup API. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata effettuata AWS Backup, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

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 le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente IAM Identity Center.
- 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 Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un percorso a regione singola o multiregione utilizzando. AWS CLI La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio account Regioni AWS . Se crei un percorso a regione singola, puoi visualizzare solo gli eventi registrati nel percorso. Regione AWS Per ulteriori informazioni sui percorsi, consulta Creazione di un percorso per te Account AWS e Creazione di un percorso per un'organizzazione nella Guida per l'AWS CloudTrail utente.

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di

conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

AWS Backup eventi in CloudTrail

AWS Backup genera questi CloudTrail eventi quando esegue backup, ripristini, copie o notifiche. Questi eventi non sono necessariamente generati dall'uso delle API AWS Backup pubbliche. Per ulteriori informazioni, consulta Servizio AWS gli eventi nella Guida per l'AWS CloudTrail utente.

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

Comprendere AWS Backup le voci dei file di registro

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 mostra `StartBackupJob` le `StartRestoreJob` `DeleteRecoveryPoint` azioni e anche l'`BackupJobCompleted`evento.

```
{
```

```
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:45:24Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartBackupJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-00a422a05b9c6asd3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": 60
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
    },
    "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
    "eventID": "fe8146a5-7812-4a95-90ad-074498be1234",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
```

```
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:49:50Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartRestoreJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",
        "metadata": {
            "volumeType": "gp2",
            "availabilityZone": "us-east-1b",
            "volumeSize": "100"
        },
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
        "resourceType": "EBS"
    },
    "responseElements": {
        "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
    },
    "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
    "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
```

```
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T14:52:42Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteRecoveryPoint",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
    },
    "responseElements": null,
    "requestID": "f1f1b33a-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "completionDate": {
```

```
            "seconds": 1547108091,
            "nanos": 906000000
        },
        "state": "COMPLETED",
        "percentDone": 100,
        "backupJobId": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
        "backupVaultName": "BackupVault",
        "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:BackupVault",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-06692095a6a421233",
        "creationDate": {
            "seconds": 1547101638,
            "nanos": 272000000
        },
        "backupSizeInBytes": 8589934592,
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "resourceType": "EBS"
    }
}
```

Registrazione degli eventi per la gestione di più account

Con AWS Backup, puoi gestire i backup in tutta la tua Account AWS AWS Organizationsstruttura. AWS Backup genera questi CloudTrail eventi quando crei, aggiorni o elimini una politica di AWS Organizations backup (che applica i piani di backup agli account dei membri) o quando esiste un piano di backup organizzativo non valido:

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationalBackupPlan`

Esempio: voci dei file di AWS Backup registro per la gestione di più account

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 illustra l'`CreateOrganizationalBackupPlan`azione.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"},
    "eventTime": "2020-06-02T00:34:00Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "CreateOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f2642255-af77-4203-8c37-7ca19d898e84",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "backupRules": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
\"name\":\"hourly\",\"description\":null,\"cryopodArn\":\"arn:aws:backup:ca-
central-1:123456789012:backup-vault:CryoControllerCAMTestBackupVault\",
\"scheduleExpression\":\"cron(0 0/1 ? * * *)\",\"startWindow\":\"PT1H\",
\"completionWindow\":\"PT2H\",\"lifecycle\":{\"moveToColdStorageAfterDays\":null,
\"deleteAfterDays\":\"7\"},\"tags\":null,\"copyActions\":[]}]",
        "backupSelections": "[{\"name\":\"selectiondatatype\",\"arn\":
\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-
a075ea715686\",\"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",
\"resources\":[],\"notResources\":[],\"conditions\":[{\"type\":\"STRINGEQUALS\",\"key
\":\"dataType\",\"value\":\"PII\"},{\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",
\"value\":\"RED\"}],\"creationDate\":\"2020-06-02T00:34:00.695Z\",\"creatorRequestId
\":null}]",
        "creationDate": {
```

```
            "seconds": 1591058040,
            "nanos": 695000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`DeleteOrganizationalBackupPlan`azione.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2020-06-02T00:34:25Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "deletionDate": {
            "seconds": 1591058065,
            "nanos": 519000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'evento`InvalidOrganizationBackupPlan`, che viene inviato quando AWS Backup riceve un piano di backup non valido da Organizations.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2022-06-11T13:29:23Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "InvalidOrganizationBackupPlan",
    "awsRegion": "Region",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "ab1de234-fg56-7890-h123-45ij678k9l01",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "987654321098",
    "serviceEventDetails": {
        "effectivePolicyVersion": 7,
        "effectivePolicyId": "12345678-a9b0-123c-45d6-78e901f23456",
        "lastUpdatedTimestamp": "Jun 11, 2022 1:29:22 PM",
        "policyType": "BACKUP_POLICY",
        "effectiveBackupPlan": {
            "logicalName": "logical-name",
            "regions": [
                "Region"
            ],
            "rules": [
                {
                    "name": "test-orgs",
                    "targetBackupVaultName": "vault-name",
                    "ruleLifecycle": {
                        "deleteAfterDays": 100
                    },
                    "copyActions": [],
                    "enableContinuousBackup": true
                }
```

```
            ],
            "selections": {
                "tagSelections": [
                    {
                        "selectionName": "selection-name",
                        "iamRoleArn": "arn:aws:iam::$account:role/role",
                        "targetedTags": [
                            {
                                "tagKey": "key",
                                "tagValue": "value"
                            }
                        ]
                    }
                ]
            },
            "backupPlanTags": {
                "key": "value"
            }
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    },
    "eventCategory": "Management"
}
```

Opzioni di notifica con AWS Backup

Esistono due modi per ricevere notifiche relative a AWS Backup:

- AWS Le notifiche utente possono inviare notifiche, tra cui CloudWatch allarmi Amazon e notifiche di altri servizi. AWS Support
- Amazon Simple Notification Service può avvisarti degli AWS Backup eventi.

AWS Notifiche utente e AWS Backup

AWS Backup supporta la gestione delle notifiche di backup dalla console AWS User Notifications. Con Notifiche utente AWS, puoi visualizzare lo stato di avanzamento dei processi di backup, copia e ripristino e le modifiche a policy di backup, vault, punti di ripristino e impostazioni dal Centro notifiche delle notifiche utente.

Amazon CloudWatch, gli EventBridge allarmi di Amazon e gli aggiornamenti dei AWS Support casi sono tra gli altri tipi di notifiche che puoi gestire dalla console. Inoltre, puoi configurare diverse opzioni di consegna, tra cui e-mail, AWS Chatbot notifiche e notifiche AWS Console Mobile Application push.

Amazon SNS ed eventi AWS Backup

AWS Backup sfrutta le solide notifiche fornite da Amazon Simple Notification Service (Amazon SNS). Puoi configurare Amazon SNS per ricevere notifiche AWS Backup sugli eventi dalla console Amazon SNS.

Limitazioni

- Sebbene il servizio Amazon SNS consenta notifiche tra più account, attualmente AWS Backup non supporta questa funzionalità. È necessario specificare l'ID AWS dell'account e l'ARN della risorsa dell'argomento.
- AWS Backup supporta gli argomenti standard per la deduplicazione SNS best-effort, ma attualmente AWS Backup non supporta gli argomenti SNS FIFO per la deduplicazione rigorosa.

Casi di utilizzo comune

- Imposta le notifiche per i processi di backup non riusciti seguendo la procedura descritta in Come posso ricevere notifiche per i processi non riusciti? AWS Backup da AWS Premium Support.
- Consulta JSON di notifica Amazon SNS di esempio per i processi di backup completati, non riusciti e scaduti nella tabella di esempi di eventi riportata di seguito.

Per ulteriori informazioni generali su Amazon SNS, consulta Nozioni di base su Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

AWS Backup API di notifica

Dopo aver creato i tuoi argomenti utilizzando la console Amazon SNS o AWS Command Line Interface (AWS CLI), puoi utilizzare le seguenti operazioni AWS Backup API per gestire le notifiche di backup.

- DeleteBackupVaultNotifications: elimina le notifiche eventi per il vault di backup specificato.
- GetBackupVaultNotifications: elenca tutte le notifiche eventi per il vault di backup specificato.
- PutBackupVaultNotifications: attiva le notifiche per l'argomento e gli eventi specificati.

AWS Backup supporta i seguenti eventi:

Tipo di processo	Evento
Processo di backup	`BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `CONTINUOUS_BACKUP_INTERRUPTED`
Processo di copia	`COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
Processo di ripristino	`RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED`
Punto di ripristino	`RECOVERY_POINT_MODIFIED`

AWS Backup per S3 supporta due eventi aggiuntivi:

- `S3_BACKUP_OBJECT_FAILED` invia all'utente una notifica relativa a tutti oggetti S3 di cui AWS Backup non è riuscito a eseguire il backup durante un processo di backup.
- `S3_RESTORE_OBJECT_FAILED` invia all'utente una notifica relativa a tutti gli oggetti S3 di cui AWS Backup non è riuscito a eseguire il ripristino durante un processo di ripristino.

Esempi di eventi

Example Esempio: processo di backup completato

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
```

```
            "Message": "An AWS Backup job was completed successfully. Recovery point
 ARN: arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012d. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"COMPLETED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

Example Esempio: processo di backup non riuscito

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed. Resource ARN : arn:aws:ec2:us-
west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-
f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"FAILED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
```

```
}
```

Example Esempio: il processo di backup non può essere completato durante la finestra di backup

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed to complete in time. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes" : {
              "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
              "State" : {"Type":"String","Value":"EXPIRED"},
              "AccountId" : {"Type":"String","Value":"123456789012"},
              "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
              "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

AWS Backup esempi di comandi di notifica

Puoi usare AWS CLI i comandi per iscriverti, elencare ed eliminare le notifiche di Amazon SNS per i tuoi AWS Backup eventi.

Esempio di notifica put del vault di backup

Il comando seguente effettua la sottoscrizione a un argomento Amazon SNS per il vault di backup specificato che notifica l'avvio o il completamento di un processo di ripristino o la modifica di un punto di ripristino.

```
aws backup put-backup-vault-notifications
```

```
    --backup-vault-name myBackupVault
    --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
    --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
 RECOVERY_POINT_MODIFIED
```

Esempio di notifica get del vault di backup

Il comando seguente elenca tutti gli eventi che hanno attualmente effettuato la sottoscrizione ad un argomento Amazon SNS per il vault di backup specificato.

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

Di seguito è riportato l'output di esempio:

```
{
    "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
    "BackupVaultEvents": [
        "RESTORE_JOB_STARTED",
        "RESTORE_JOB_COMPLETED",
        "RECOVERY_POINT_MODIFIED"
    ],
    "BackupVaultName": "myVault",
    "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

Esempio di notifica delete del vault di back

Il comando seguente annulla la sottoscrizione a un argomento Amazon SNS per il vault di backup specificato.

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

Specificazione AWS Backup come principale del servizio

> **Note**
>
> AWS Backup Per consentire la pubblicazione di argomenti SNS per conto dell'utente, è necessario specificare AWS Backup come responsabile del servizio.

Includi il seguente codice JSON nella politica di accesso dell'argomento Amazon SNS che utilizzi per tenere AWS Backup traccia degli eventi. È necessario specificare l'Amazon Resource Name (ARN) di risorsa del tuo argomento.

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Per ulteriori informazioni sulla specificazione di un servizio principale in una policy di accesso di Amazon SNS, consulta Allowing AWS Any Resource to Publish to a Topic nella Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Se il tuo argomento è crittografato, devi includere autorizzazioni aggiuntive nella tua policy per AWS Backup consentirne la pubblicazione. Per ulteriori informazioni su come abilitare i servizi alla pubblicazione su argomenti crittografati, consulta Enable Compatibility between Event Sources from AWS Services and Encrypted Topics nella Amazon Simple Notification Service Developer Guide.

Risoluzione dei problemi AWS Backup

Quando si utilizza AWS Backup, è possibile che si verifichino problemi. Le sezioni seguenti offrono un valido aiuto per risolvere alcuni dei problemi più comuni che potrebbero verificarsi.

Per domande generali sull'argomento AWS Backup, consulta le AWS Backup domande frequenti. È possibile anche cercare risposte e pubblicare domande nei forum di AWS Backup.

Argomenti

Risoluzione dei problemi generali

Quando si esegue il backup e il ripristino delle risorse, è necessario disporre dell'autorizzazione all'uso AWS Backup e all'accesso alle risorse che si desidera proteggere. Il modo più semplice per disporre delle autorizzazioni appropriate consiste nello scegliere il ruolo predefinito quando si assegnano risorse a un piano di backup. Per ulteriori informazioni sul controllo degli accessi tramite AWS Identity and Access Management (IAM) con AWS Backup, consultaControllo accessi.

Se si `AccessDenied` verifica un errore durante il tentativo di accedere a una AWS Backup risorsa, ad esempio un archivio di backup, la risorsa non esiste o non si dispone delle autorizzazioni per accedere alla risorsa.

Se si verificano problemi relativi al backup e al ripristino di un particolare tipo di risorsa, può essere utile esaminare l'argomento relativo alla risoluzione dei problemi di backup e ripristino per tale risorsa. Per ulteriori informazioni, consulta i collegamenti nella sezione Come AWS Backup funziona con i servizi supportati. AWS

Se AWS Backup non riesci a creare o eliminare una risorsa, puoi saperne di più sul problema utilizzando AWS CloudTrail per visualizzare i messaggi di errore o i registri. Per ulteriori informazioni sull'utilizzo CloudTrail con AWS Backup, consultaRegistrazione delle chiamate API con AWS Backup CloudTrail.

Risoluzione dei problemi relativi alla creazione di risorse

Le seguenti informazioni consentono di risolvere i problemi relativi alla creazione di backup.

- In generale, i servizi di AWS database non possono avviare i backup 1 ora prima o durante la finestra di manutenzione o la finestra di backup automatico. Amazon FSx non può avviare i backup 4 ore prima o durante la finestra di manutenzione o la finestra di backup automatico (Amazon Aurora è esente da questa limitazione della finestra di manutenzione). I backup di snapshot pianificati in questi orari non andranno a buon fine. Un'eccezione: quando scegli di utilizzare AWS Backup sia i backup istantanei che quelli continui per un servizio supportato, non devi più preoccuparti di quelle finestre perché le AWS Backup pianificheremo automaticamente. Consulta Point-in-Time Recovery per un elenco dei servizi supportati e istruzioni su come utilizzarli per AWS Backup eseguire backup continui.
- La creazione di backup per le tabelle DynamoDB non riesce durante la creazione delle tabelle. Per creare una tabella DynamoDB in genere sono necessari un paio di minuti.
- Il backup dei file system Amazon EFS può richiedere fino a 7 giorni, se i file system sono molto grandi. È possibile accodare un solo backup simultaneo alla volta per un file system Amazon EFS. Se viene accodato un backup successivo mentre quello precedente è ancora in corso, è possibile che la finestra di backup scada e non venga creato alcun backup.
- Amazon EBS ha una quota standard di 100.000 backup Regione AWS per account e i backup aggiuntivi falliscono quando viene raggiunta questa quota. Se si raggiunge questa quota, è possibile eliminare i backup in eccesso o richiedere un aumento della quota. Per ulteriori informazioni sulla richiesta di un aumento delle quote, consulta Quote del servizio AWS.
- Quando crei backup Amazon Relational Database Service (RDS), considera quanto segue:
  - Se non AWS Backup gestisci sia gli snapshot di Amazon RDS che i backup continui con point-in-time ripristino, i backup avranno esito negativo se avviati se pianificati o eseguiti su richiesta durante la finestra di backup giornaliera di 30 minuti configurabile dall'utente. Per ulteriori informazioni sui backup automatici Amazon RDS, consulta Utilizzo dei backup nella Guida per l'utente di Amazon RDS. Puoi evitare questa limitazione utilizzando AWS Backup per gestire sia gli snapshot di Amazon RDS che i backup continui con ripristino. point-in-time
  - Se si avvia un processo di backup dalla console di Amazon RDS, questo può generare un conflitto con un processo di backup dei cluster Aurora, causando l'errore `Backup job expired before completion.`. Se ciò si verifica, configura una finestra di backup più lunga in AWS Backup.

- AWS Backup attualmente non trasmette il gruppo di opzioni TDE quando viene creato un processo di copia. Se si intende utilizzare questo gruppo di opzioni per la creazione di processi di copia, è opportuno utilizzare la console Amazon RDS o l'API Amazon RDS anziché gli strumenti AWS Backup . Per ulteriori informazioni, consulta Copia di un gruppo di opzioni nella Guida per l'utente di Amazon Relational Database Service.
- ERRORE: i backup on demand vengono completati ma i backup pianificati hanno esito negativo con l'errore "The source snapshot KMS key does not exist, is not enabled or you do not have permissions to access it". Il processo on demand viene completato perché utilizza la chiamata API `CopyDBSnapshot`, che non richiede l'accesso KMS.

  RIMEDIO: aggiungi il ruolo IAM alla chiave KMS. Questo può essere fatto consentendo il ruolo nella policy della chiave KMS.

  Per modificare la policy:

  1. Apri la console KMS.
  2. Nella barra di navigazione a sinistra, seleziona Chiavi gestite dal cliente.
  3. Fai clic sulla chiave gestita dal cliente da modificare.
  4. In Policy della chiave, fai clic su Passa alla visualizzazione della policy.
  5. Fare clic su Edit (Modifica).
  6. Aggiungi il ruolo.

Risoluzione dei problemi relativi all'eliminazione delle risorse

I punti di ripristino creati da AWS Backup non possono essere eliminati nella finestra della console della risorsa protetta. È possibile eliminarli sulla AWS Backup console selezionandoli nell'archivio in cui sono archiviati e quindi scegliendo Elimina.

Per eliminare un punto di ripristino o un vault di backup, sono necessarie le autorizzazioni appropriate. Per ulteriori informazioni sul controllo degli accessi tramite IAM with AWS Backup, consultaControllo accessi.

Risoluzione dei problemi relativi al ripristino delle risorse

Ripristino tramite API

Per ripristinare un backup in modo programmatico, utilizza l'operazione API StartRestoreJob.

Per ottenere i metadati di configurazione con cui è stato creato il backup, puoi chiamare GetRecoveryPointRestoreMetadata.

Per ulteriori informazioni, consulta Ripristino di un backup.

Ripristino mediante la console

- Ripristino dei dati Amazon S3
- Ripristino di una macchina virtuale
- Ripristino di un file system Amazon FSx
- Ripristino di un volume Amazon EBS
- Ripristino di un file system Amazon EFS
- Ripristino di una tabella Amazon DynamoDB
- Ripristino di un database Amazon RDS
- Ripristino di un cluster Aurora
- Ripristino di un'istanza Amazon EC2
- Ripristino di un volume Storage Gateway
- Ripristino di un cluster Amazon DocumentDB
- Ripristino di un cluster Neptune

Risoluzione degli errori di formattazione

Quando viene incluso un carattere jolly (*) per il valore di un parametro, il carattere jolly viene elaborato per includere valori diversi dagli spazi bianchi. I valori in una coppia chiave-valore che contengono spazi bianchi non verranno inclusi come parte del carattere jolly.

API AWS Backup

Oltre a usare la console, puoi usare le azioni e i tipi di dati API di AWS Backup per configurare e gestire AWS Backup a livello di programmazione e le relative risorse. In questa sezione vengono descritte le azioni e tipi di dati di AWS Backup. Contiene il riferimento API per AWS Backup.

API AWS Backup

- Operazioni AWS Backup
- AWS Backup Tipi di dati

Azioni

Le seguenti azioni sono supportate da AWS Backup:

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework
- DeleteRecoveryPoint

- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection
- GetSupportedResourceTypes

- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob
- StartCopyJob

- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

Le seguenti azioni sono supportate da AWS Backup gateway:

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines

- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AWS Backup

Le seguenti azioni sono supportate da AWS Backup:

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework

- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection

- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob

- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

CancelLegalHold

Servizio: AWS Backup

Rimuove il blocco legale specificato su un punto di ripristino. Questa azione può essere eseguita solo da un utente con autorizzazioni sufficienti.

Sintassi della richiesta

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

CancelDescription

Una stringa che descrive il motivo della rimozione del blocco a fini legali.

Campo obbligatorio: sì

legalHoldId

L'ID del blocco a fini legali.

Campo obbligatorio: sì

RetainRecordInDays

L'importo intero, in giorni, dopo il quale rimuovere la conservazione legale.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 201
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 201 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidResourceStateException

AWS Backup sta già eseguendo un'azione su questo punto di ripristino. Non può eseguire l'azione richiesta fino al termine della prima azione. Riprova più tardi.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++

- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateBackupPlan

Servizio: AWS Backup

Crea un piano di backup utilizzando il nome del piano di backup e le regole di backup. Un piano di backup è un documento che contiene informazioni che vengono AWS Backup utilizzate per pianificare attività che creano punti di ripristino per le risorse.

Se chiami `CreateBackupPlan` con un piano già esistente, ricevi un'eccezione `AlreadyExistsException`.

Sintassi della richiesta

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
```

```
                "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
                "string" : "string"
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
        }
    ]
  },
  "BackupPlanTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupPlan

Il corpo di un piano di backup. Include un `BackupPlanName` e uno o più set di `Rules`.

Tipo: oggetto BackupPlanInput

Campo obbligatorio: sì

BackupPlanTags

I tag da assegnare al piano di backup.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

CreatorRequestId

Identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Se la richiesta include un `CreatorRequestId` che corrisponde a un piano di backup esistente, tale piano viene restituito. Questo parametro è facoltativo.

Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

- Tipo: stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AdvancedBackupSettings

Le impostazioni per un tipo di risorsa. Questa opzione è disponibile solo per i processi di backup di Windows Volume Shadow Copy Service (VSS).

Tipo: matrice di oggetti AdvancedBackupSetting

BackupPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

- Tipo: stringa

BackupPlanId

L'ID del piano di backup.

- Tipo: stringa

CreationDate

La data e l'ora di creazione di un piano di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

VersionId

Stringhe con codifica UTF-8 Unicode univoche generate casualmente con lunghezza massimo di 1.024 byte. e non possono essere modificati.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateBackupSelection

Servizio: AWS Backup

Crea un documento JSON che specifica un set di risorse da assegnare a un piano di backup. Per esempi, consulta Assegnazione di risorse a livello di codice.

Sintassi della richiesta

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
Content-type: application/json

{
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
```

```
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreatorRequestId": "string"
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

L'ID del piano di backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupSelection

Il corpo di una richiesta di assegnazione di un set di risorse a un piano di backup.

Tipo: oggetto BackupSelection

Campo obbligatorio: sì

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Questo parametro è facoltativo.

Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

-Tipo: stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlanId

L'ID del piano di backup.

- Tipo: stringa

CreationDate

La data e l'ora di creazione di una selezione di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

SelectionId

Identifica in modo univoco il corpo di una richiesta per assegnare un set di risorse a un piano di backup.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateBackupVault

Servizio: AWS Backup

Crea un container logico in cui vengono archiviati i backup. Una richiesta `CreateBackupVault` include un nome, facoltativamente uno o più tag delle risorse, una chiave di crittografia e un ID della richiesta.

> **Note**
>
> Non includere i dati riservati, ad esempio i numeri di passaporto, nel nome di un vault di backup.

Sintassi della richiesta

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati. Consistono in lettere, numeri e trattini.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupVaultTags

I tag da assegnare al vault di backup.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Questo parametro è facoltativo.

Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

-Tipo: stringa

Campo obbligatorio: no

EncryptionKeyArn

La chiave di crittografia lato server utilizzata per proteggere i backup, ad esempio `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

-Tipo: stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione in cui sono stati creati. Consistono di minuscole, numeri e trattini.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

La data e l'ora di creazione di un vault di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateFramework

Servizio: AWS Backup

Crea un framework con uno o più controlli. Un framework è una raccolta di controlli che è possibile utilizzare per valutare le procedure di backup. Utilizzando controlli personalizzabili predefiniti per definire le policy, è possibile valutare se le procedure di backup sono conformi alle policy e quali risorse non sono ancora conformi.

Sintassi della richiesta

```
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkTags": {
      "string" : "string"
   },
   "IdempotencyToken": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

FrameworkControls

I controlli che compongono il framework. Ogni controllo nell'elenco dispone di nome, parametri di input e ambito.

Tipo: matrice di oggetti FrameworkControl

Campo obbligatorio: sì

FrameworkDescription

Una descrizione facoltativa del framework, con un massimo di 1.024 caratteri.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `.*\S.*`

Campo obbligatorio: no

FrameworkName

Il nome univoco del framework. Il nome deve essere compreso tra 1 e 256 caratteri, deve iniziare con una lettera ed essere costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

FrameworkTags

I tag da assegnare al framework.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `CreateFrameworkInput`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

- Tipo: stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

FrameworkArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

FrameworkName

Il nome univoco del framework. Il nome deve essere compreso tra 1 e 256 caratteri, deve iniziare con una lettera ed essere costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLegalHold

Servizio: AWS Backup

Crea un blocco legale su un punto di ripristino (backup). Un blocco a fini legali è una limitazione alla modifica o eliminazione di un backup fino a quando un utente autorizzato non annulla il blocco a fini legali. Qualsiasi azione volta a eliminare o dissociare un punto di ripristino non andrà a buon fine e genererà un errore se sul punto di ripristino sono presenti uno o più blocchi a fini legali attivi.

Sintassi della richiesta

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
   "Description": "string",
   "IdempotencyToken": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Tags": {
      "string" : "string"
   },
   "Title": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Description

La descrizione della conservazione legale.

Tipo: stringa

Campo obbligatorio: sì

IdempotencyToken

Questa è una stringa scelta dall'utente utilizzata per distinguere tra chiamate altrimenti identiche. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

-Tipo: stringa

Campo obbligatorio: no

RecoveryPointSelection

I criteri per assegnare un insieme di risorse, ad esempio i tipi di risorse o gli archivi di backup.

Tipo: oggetto RecoveryPointSelection

Campo obbligatorio: no

Tags

Tag opzionali da includere. Un tag è una coppia chiave-valore che puoi utilizzare per gestire, filtrare e cercare le risorse. I caratteri consentiti includono lettere UTF-8, numeri, spazi e i caratteri seguenti: + - = . _ : /.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

Title

Il titolo della custodia legale.

Tipo: stringa

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Status": "string",
   "Title": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationDate

L'ora in cui è stata creata la custodia legale.

Tipo: Timestamp

Description

La descrizione del blocco legale.

- Tipo: stringa

LegalHoldArn

L'Amazon Resource Name (ARN) della custodia legale.

- Tipo: stringa

LegalHoldId

L'ID del blocco a fini legali.

- Tipo: stringa

RecoveryPointSelection

I criteri da assegnare a un insieme di risorse, ad esempio i tipi di risorse o gli archivi di backup.

Tipo: oggetto RecoveryPointSelection

Status

Lo stato della custodia legale.

- Tipo: stringa

Valori validi: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

Il titolo della custodia legale.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateLogicallyAirGappedBackupVault

Servizio: AWS Backup

Crea un contenitore logico in cui è possibile copiare i backup.

Questa richiesta include un nome, la regione, il numero massimo di giorni di conservazione, il numero minimo di giorni di conservazione e, facoltativamente, può includere tag e un ID richiesta dell'autore.

> **Note**
>
> Non includere i dati riservati, ad esempio i numeri di passaporto, nel nome di un vault di backup.

Sintassi della richiesta

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup con isolamento logico air gap sono identificati da nomi univoci per l'account utilizzato per crearli e per la regione in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupVaultTags

I tag da assegnare al vault.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

CreatorRequestId

L'ID della richiesta di creazione.

Questo parametro è facoltativo. Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

-Tipo: stringa

Campo obbligatorio: no

MaxRetentionDays

Il periodo di conservazione massimo durante il quale il vault conserva i propri punti di ripristino. Se questo parametro non è specificato, AWS Backup non applica un periodo di conservazione massimo sui punti di ripristino nel vault (consentendo lo storage a tempo indeterminato).

Se specificato, qualsiasi processo di backup o copia nel vault deve avere una policy del ciclo di vita con un periodo di conservazione uguale o inferiore al periodo di conservazione massimo. Se il periodo di conservazione del processo è più lungo del periodo di conservazione massimo, allora il processo di backup o di copia del vault non riesce ed è necessario modificare le impostazioni del ciclo di vita o utilizzare un vault diverso.

Tipo: long

Campo obbligatorio: sì

MinRetentionDays

Questa impostazione specifica il periodo di conservazione minimo durante il quale il vault mantiene i punti di ripristino. Se questo parametro non è specificato, non viene applicato alcun periodo di conservazione minimo.

Se specificato, qualsiasi processo di backup o copia nel vault deve avere una policy del ciclo di vita con un periodo di conservazione uguale o superiore al periodo di conservazione minimo. Se il periodo di conservazione del processo è più breve del periodo di conservazione minimo, allora il processo di backup o di copia del vault non riesce ed è necessario modificare le impostazioni del ciclo di vita o utilizzare un vault diverso.

Tipo: long

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupVaultArn

L'ARN (Amazon Resource Name) del vault.

- Tipo: stringa

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup con isolamento logico air gap sono identificati da nomi univoci per l'account utilizzato per crearli e per la regione in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

La data e l'ora di creazione del vault.

Questo valore è in formato Unix, ora Coordinated Universal Time (UTC) ed è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

VaultState

Lo stato attuale del vault.

-Tipo: stringa

Valori validi: `CREATING | AVAILABLE | FAILED`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateReportPlan

Servizio: AWS Backup

Crea un piano di report. Un piano di segnalazione è un documento che contiene informazioni sul contenuto del rapporto e su dove AWS Backup verrà consegnato.

Se chiami `CreateReportPlan` con un piano già esistente, ricevi un'eccezione `AlreadyExistsException`.

Sintassi della richiesta

```
POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `CreateReportPlanInput`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

- Tipo: stringa

Campo obbligatorio: no

ReportDeliveryChannel

Una struttura contenente informazioni su dove e come consegnare i report, in particolare il nome del bucket Amazon S3, il prefisso della chiave S3 e i formati dei report.

Tipo: oggetto ReportDeliveryChannel

Campo obbligatorio: sì

ReportPlanDescription

Una descrizione facoltativa del piano di report, con un massimo di 1.024 caratteri.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `.*\S.*`

Campo obbligatorio: no

ReportPlanName

Il nome univoco del piano di report. Il nome deve essere compreso tra 1 e 256 caratteri, deve iniziare con una lettera ed essere costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

ReportPlanTags

I tag da assegnare al piano di report.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

ReportSetting

Identifica il modello di report per il report. I report vengono creati utilizzando un modello di report. I modelli di report sono:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Se il modello di report è `RESOURCE_COMPLIANCE_REPORT` o`CONTROL_COMPLIANCE_REPORT`, questa risorsa API descrive anche la copertura del report Regioni AWS e i framework.

Tipo: oggetto ReportSetting

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

La data e l'ora di creazione di un vault di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

ReportPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

ReportPlanName

Il nome univoco del piano di report.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateRestoreTestingPlan

Servizio: AWS Backup

Crea un piano di test di ripristino.

Il primo dei due passaggi per creare un piano di test di ripristino. Dopo che questa richiesta è andata a buon fine, completa la procedura utilizzando CreateRestoreTestingSelection.

Sintassi della richiesta

```
PUT /restore-testing/plans HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "RestoreTestingPlanName": "string",
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   },
   "Tags": {
      "string" : "string"
   }
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Questo parametro è facoltativo. Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

-Tipo: stringa

Campo obbligatorio: no

RestoreTestingPlan

Un piano di test di ripristino deve contenere una stringa `RestoreTestingPlanName` univoca creata dall'utente e un cron `ScheduleExpression`. Facoltativamente, puoi includere un numero intero per `StartWindowHours` e una stringa `CreatorRequestId`.

`RestoreTestingPlanName` è una stringa univoca che identifica il nome del piano di test di ripristino. Non può essere modificato dopo la creazione e deve essere composto solo da caratteri alfanumerici e caratteri di sottolineatura.

Tipo: oggetto RestoreTestingPlanForCreate

Campo obbligatorio: sì

Tags

I tag da assegnare al piano di test di ripristino.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 201.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

La data e l'ora di creazione di un piano di test di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 12:11:30.087.

Tipo: Timestamp

RestoreTestingPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco il piano di test di ripristino creato.

- Tipo: stringa

RestoreTestingPlanName

Questa stringa univoca costituisce il nome del piano di test di ripristino.

Il nome non può essere modificato dopo la creazione. Il nome può contenere solo caratteri alfanumerici e caratteri di sottolineatura. La lunghezza massima è 50 caratteri.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

ConflictException

AWS Backup non può eseguire l'azione richiesta finché non termina l'esecuzione di un'azione precedente. Riprova più tardi.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python

- AWS SDK per Ruby V3

CreateRestoreTestingSelection

Servizio: AWS Backup

Questa richiesta può essere inviata dopo che la CreateRestoreTestingPlan richiesta è stata restituita correttamente. È la seconda parte della creazione di un piano di test delle risorse e deve essere completata in sequenza.

Consiste in `RestoreTestingSelectionName`, `ProtectedResourceType` e uno dei seguenti parametri:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Ogni tipo di risorsa protetta può avere un solo valore.

Una selezione di test di ripristino può includere un valore jolly ("*") per `ProtectedResourceArns` insieme a `ProtectedResourceConditions`. In alternativa, puoi includere fino a 30 ARN di risorse protette specifiche in `ProtectedResourceArns`.

Non è possibile selezionare i tipi di risorse protette e gli ARN specifici. Se entrambi sono inclusi, la richiesta avrà esito negativo.

Sintassi della richiesta

```
PUT /restore-testing/plans/RestoreTestingPlanName/selections HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
```

```
                "Key": "string",
                "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

RestoreTestingPlanName

Inserisci il nome del piano di test di ripristino che è stato restituito dalla CreateRestoreTestingPlan richiesta correlata.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

CreatorRequestId

Una stringa univoca facoltativa che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

- Tipo: stringa

Campo obbligatorio: no

RestoreTestingSelection

Consiste in `RestoreTestingSelectionName`, `ProtectedResourceType` e uno dei seguenti parametri:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Ogni tipo di risorsa protetta può avere un solo valore.

Una selezione di test di ripristino può includere un valore jolly ("*") per `ProtectedResourceArns` insieme a `ProtectedResourceConditions`. In alternativa, puoi includere fino a 30 ARN di risorse protette specifiche in `ProtectedResourceArns`.

Tipo: oggetto RestoreTestingSelectionForCreate

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 201.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

L'ora in cui è stata creata la selezione per il test delle risorse.

Tipo: Timestamp

RestoreTestingPlanArn

L'ARN del piano di test di ripristino a cui è associata la selezione del test di ripristino.

Tipo: stringa

RestoreTestingPlanName

Il nome del piano di test di ripristino.

Il nome non può essere modificato dopo la creazione. Il nome può contenere solo caratteri alfanumerici e caratteri di sottolineatura. La lunghezza massima è 50 caratteri.

- Tipo: stringa

RestoreTestingSelectionName

Il nome della selezione del test di ripristino per il relativo piano di test di ripristino.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteBackupPlan

Servizio: AWS Backup

Elimina un piano di backup. È possibile eliminare un piano di backup solo dopo che tutte le selezioni di risorse associate sono state eliminate. L'eliminazione di un piano di backup elimina la versione corrente del piano. Le versioni precedenti, se presenti, continueranno a esistere.

Sintassi della richiesta

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

Identifica in modo univoco un piano di backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

- Tipo: stringa

BackupPlanId

Identifica in modo univoco un piano di backup.

- Tipo: stringa

DeletionDate

La data e l'ora di eliminazione di un piano di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `DeletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

VersionId

Stringhe con codifica UTF-8 Unicode univoche generate casualmente con lunghezza massimo di 1.024 byte. Gli ID versione non possono essere modificati.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteBackupSelection

Servizio: AWS Backup

Elimina la selezione delle risorse associate a un piano di backup specificato da `SelectionId`.

Sintassi della richiesta

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

Identifica in modo univoco un piano di backup.

Campo obbligatorio: sì

selectionId

Identifica in modo univoco il corpo di una richiesta per assegnare un set di risorse a un piano di backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteBackupVault

Servizio: AWS Backup

Elimina il vault di backup identificato dal relativo nome. Un vault può essere eliminato solo se è vuoto.

Sintassi della richiesta

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteBackupVaultAccessPolicy

Servizio: AWS Backup

Elimina il documento di policy che gestisce le autorizzazioni su un vault di backup.

Sintassi della richiesta

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati. Consistono di minuscole, numeri e trattini.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteBackupVaultLockConfiguration

Servizio: AWS Backup

Elimina AWS Backup Vault Lock da un archivio di backup specificato dal nome di un archivio di backup.

Se la configurazione di Vault Lock è immutabile, non è possibile eliminare Vault Lock utilizzando le operazioni API; in caso contrario, si riceverà un `InvalidRequestException`. Per ulteriori informazioni, consulta Vault Lock nella Guida per gli sviluppatori. AWS Backup

Sintassi della richiesta

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome del vault di backup da cui eliminare AWS Backup Vault Lock.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteBackupVaultNotifications

Servizio: AWS Backup

Elimina le notifiche degli eventi per il vault di backup specificato.

Sintassi della richiesta

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteFramework

Servizio: AWS Backup

Elimina il framework specificato da un nome framework.

Sintassi della richiesta

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

frameworkName

Il nome univoco di un framework.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

AWS Backup non può eseguire l'azione richiesta finché non completa l'esecuzione di un'azione precedente. Riprova più tardi.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteRecoveryPoint

Servizio: AWS Backup

Elimina il punto di ripristino specificato da un ID del punto di ripristino.

Se l'ID del punto di ripristino appartiene a un backup continuo, la chiamata di questo endpoint elimina il backup continuo esistente e interrompe backup continui futuri.

Quando le autorizzazioni di un ruolo IAM non sono sufficienti per chiamare questa API, il servizio restituisce una risposta HTTP 200 con un corpo HTTP vuoto, ma il punto di ripristino non viene eliminato. Al contrario, viene attivato uno stato `EXPIRED`.

I punti di ripristino `EXPIRED` possono essere eliminati con questa API quando il ruolo IAM dispone dell'azione `iam:CreateServiceLinkedRole`. Per ulteriori informazioni sull'aggiunta di questo ruolo, consulta Risoluzione dei problemi relativi alle eliminazioni manuali.

Se l'utente o il ruolo viene eliminato o l'autorizzazione all'interno del ruolo viene rimossa, l'eliminazione non andrà a buon fine e verrà attivato uno stato `EXPIRED`.

Sintassi della richiesta

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

recoveryPointArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

InvalidResourceStateException

AWS Backup sta già eseguendo un'azione su questo punto di ripristino. Non può eseguire l'azione richiesta fino al termine della prima azione. Riprova più tardi.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteReportPlan

Servizio: AWS Backup

Elimina il piano di report specificato dal nome di un piano di report.

Sintassi della richiesta

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

reportPlanName

Il nome univoco di un piano di report.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

AWS Backup non può eseguire l'azione richiesta finché non completa l'esecuzione di un'azione precedente. Riprova più tardi.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteRestoreTestingPlan

Servizio: AWS Backup

Questa richiesta elimina il piano di test di ripristino specificato.

L'eliminazione può essere completata solo se vengono eliminate prima tutte le selezioni associate al test di ripristino.

Sintassi della richiesta

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

RestoreTestingPlanName

Nome univoco richiesto del piano di test di ripristino che si desidera eliminare.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 204
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteRestoreTestingSelection

Servizio: AWS Backup

Inserisci il nome del piano di test di ripristino e il nome della selezione per il test di ripristino.

Tutte le selezioni di test associate a un piano di test di ripristino devono essere eliminate prima di poter eliminare il piano di test di ripristino.

Sintassi della richiesta

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

RestoreTestingPlanName

Nome univoco obbligatorio del piano di test di ripristino che contiene la selezione per il test di ripristino che si desidera eliminare.

Campo obbligatorio: sì

RestoreTestingSelectionName

Nome univoco obbligatorio della selezione per il test di ripristino che si desidera eliminare.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 204
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeBackupJob

Servizio: AWS Backup

Restituisce i dettagli del processo di backup per il `BackupJobId` specificato.

Sintassi della richiesta

```
GET /backup-jobs/backupJobId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupJobId

Identifica in modo univoco una richiesta di backup AWS Backup di una risorsa.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupJobId": "string",
   "BackupOptions": {
      "string" : "string"
   },
   "BackupSizeInBytes": number,
   "BackupType": "string",
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "BytesTransferred": number,
   "ChildJobsInState": {
      "string" : number
   },
```

```
   "CompletionDate": number,
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "ExpectedCompletionDate": number,
   "IamRoleArn": "string",
   "InitiationDate": number,
   "IsParent": boolean,
   "MessageCategory": "string",
   "NumberOfChildJobs": number,
   "ParentJobId": "string",
   "PercentDone": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "StartBy": number,
   "State": "string",
   "StatusMessage": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AccountId

Restituisce l'ID account proprietario del processo di backup.

Tipo: stringa

Modello: `^[0-9]{12}$`

BackupJobId

Identifica in modo univoco una richiesta di backup AWS Backup di una risorsa.

Tipo: stringa

BackupOptions

Rappresenta le opzioni specificate come parte del piano di backup o del processo di backup on demand.

Tipo: mappatura stringa a stringa

Modello di chiave:`^[a-zA-Z0-9\-\_\.]{1,50}$`

Modello di valore: `^[a-zA-Z0-9\-\_\.]{1,50}$`

BackupSizeInBytes

La dimensione, in byte, di un backup.

Tipo: long

BackupType

Rappresenta il tipo di backup effettivo selezionato per un processo di backup. Ad esempio, se è stato eseguito correttamente un backup di Windows VSS (Volume Shadow Copy Service), `BackupType` restituisce `"WindowsVSS"`. Se `BackupType` è vuoto, significa che il tipo di backup è stato un backup normale.

-Tipo: stringa

BackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

-Tipo: stringa

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

BytesTransferred

La dimensione in byte trasferiti in un vault di backup nel momento in cui è stata richiesta la verifica dello stato del processo.

Tipo: long

ChildJobsInState

Ciò restituisce le statistiche dei processi di backup figlio (nidificati) inclusi.

Tipo: mappatura stringa a intero lungo

Chiavi valide: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

CompletionDate

La data e l'ora di complemento di un processo di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

CreatedBy

Contiene informazioni di identificazione sulla creazione di un processo di backup, tra cui `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` e `BackupRuleId` del piano backup utilizzato per crearlo.

Tipo: oggetto RecoveryPointCreator

CreationDate

La data e l'ora di creazione di un processo di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

ExpectedCompletionDate

La data e l'ora prevista di complemento di un processo di backup delle risorse, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `ExpectedCompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione; ad esempio, `arn:aws:iam::123456789012:role/S3Access`.

- Tipo: stringa

InitiationDate

La data di avvio di un processo di backup.

Tipo: Timestamp

IsParent

Ciò restituisce il valore booleano di cui un processo di backup è un processo principale (composito).

Tipo: Booleano

MessageCategory

Il numero di lavori per la categoria di messaggi specificata.

Stringhe di esempio possono essere `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `INVALIDPARAMETERS`. Visualizza Monitoraggio per un elenco di MessageCategory stringhe accettate.

- Tipo: stringa

NumberOfChildJobs

Ciò restituisce il numero di processi di backup figlio (nidificati).

Tipo: long

ParentJobId

Ciò restituisce l'ID del processo di backup della risorsa principale (composito).

- Tipo: stringa

PercentDone

Contiene una percentuale stimata di completamento di un processo nel momento in cui è stato richiesto lo stato del processo.

- Tipo: stringa

RecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

ResourceArn

Un ARN identifica in modo univoco una risorsa salvata. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

ResourceName

Il nome non univoco della risorsa che appartiene al backup specificato.

- Tipo: stringa

ResourceType

Il tipo di AWS risorsa di cui eseguire il backup; ad esempio, un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS).

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

Specifica l'ora in formato Unix e UTC (Coordinated Universal Time) in cui è necessario avviare un processo di backup prima che venga annullato. Il valore viene calcolato aggiungendo la finestra di avvio all'ora pianificata. Pertanto, se l'ora pianificata era le 18:00 e la finestra di avvia è di 2 ore, l'ora `StartBy` sarebbe le 20:00 della data specificata. Il valore di `StartBy` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

State

Lo stato corrente di un processo di backup.

- Tipo: stringa

Valori validi: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

Un messaggio dettagliato che spiega lo stato del processo di backup di una risorsa.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

DependencyFailureException

Un AWS servizio o una risorsa dipendente ha restituito un errore al AWS Backup servizio e l'azione non può essere completata.

Codice di stato HTTP: 500

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeBackupVault

Servizio: AWS Backup

Restituisce i metadati relativi a un vault di backup specificato in base al nome.

Sintassi della richiesta

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

BackupVaultAccountId

L'ID dell'account del vault di backup specificato.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string",
   "LockDate": number,
   "Locked": boolean,
   "MaxRetentionDays": number,
   "MinRetentionDays": number,
   "NumberOfRecoveryPoints": number,
```

```
   "VaultType": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione in cui sono stati creati.

- Tipo: stringa

CreationDate

La data e l'ora di creazione di un vault di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Questo parametro è facoltativo. Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

- Tipo: stringa

EncryptionKeyArn

La chiave di crittografia lato server utilizzata per proteggere i backup, ad esempio `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

- Tipo: stringa

LockDate

La data e l'ora in cui la configurazione di AWS Backup Vault Lock non può essere modificata o eliminata.

Se hai applicato Vault Lock al vault senza specificare una data di blocco, puoi modificare qualsiasi impostazione di Vault Lock o eliminare completamente Vault Lock dal vault, in qualsiasi momento.

Questo valore è in formato Unix, ora Coordinated Universal Time (UTC) ed è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Locked

Un valore booleano che indica se AWS Backup Vault Lock sta attualmente proteggendo l'archivio di backup. `True`significa che Vault Lock causa il fallimento delle operazioni di eliminazione o aggiornamento sui punti di ripristino archiviati nel vault.

Tipo: Booleano

MaxRetentionDays

L'impostazione AWS Backup Vault Lock che specifica il periodo di conservazione massimo durante il quale il vault conserva i propri punti di ripristino. Se questo parametro non è specificato, Vault Lock non applica un periodo di conservazione massimo sui punti di ripristino nel vault (consentendo lo storage a tempo indeterminato).

Se specificato, qualsiasi processo di backup o copia nel vault deve avere una policy del ciclo di vita con un periodo di conservazione uguale o inferiore al periodo di conservazione massimo. Se il periodo di conservazione del processo è più lungo del periodo di conservazione massimo, allora il processo di backup o di copia del vault non riesce ed è necessario modificare le impostazioni del ciclo di vita o utilizzare un vault diverso. I punti di ripristino già archiviati nel vault prima di Vault Lock non sono interessati.

Tipo: long

MinRetentionDays

L'impostazione AWS Backup Vault Lock che specifica il periodo di conservazione minimo durante il quale il vault conserva i propri punti di ripristino. Se questo parametro non è specificato, Vault Lock non applica un periodo di conservazione minimo.

Se specificato, qualsiasi processo di backup o copia nel vault deve avere una policy del ciclo di vita con un periodo di conservazione uguale o superiore al periodo di conservazione minimo. Se il periodo di conservazione del processo è più breve del periodo di conservazione minimo, allora il processo di backup o di copia del vault non riesce ed è necessario modificare le impostazioni del ciclo di vita o utilizzare un vault diverso. I punti di ripristino già archiviati nel vault prima di Vault Lock non sono interessati.

Tipo: long

NumberOfRecoveryPoints

Il numero di punti di ripristino archiviati in un vault di backup.

Tipo: long

VaultType

Il tipo di deposito descritto.

-Tipo: stringa

Valori validi: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeCopyJob

Servizio: AWS Backup

Restituisce i metadati associati alla creazione di una copia di una risorsa.

Sintassi della richiesta

```
GET /copy-jobs/copyJobId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

copyJobId

Identifica in modo univoco un processo di copia.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJob": {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "ChildJobsInState": {
         "string" : number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
      "CopyJobId": "string",
      "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
```

```
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
      },
      "CreationDate": number,
      "DestinationBackupVaultArn": "string",
      "DestinationRecoveryPointArn": "string",
      "IamRoleArn": "string",
      "IsParent": boolean,
      "MessageCategory": "string",
      "NumberOfChildJobs": number,
      "ParentJobId": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string",
      "SourceBackupVaultArn": "string",
      "SourceRecoveryPointArn": "string",
      "State": "string",
      "StatusMessage": "string"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CopyJob

Contiene informazioni dettagliate su un processo di copia.

Tipo: oggetto CopyJob

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeFramework

Servizio: AWS Backup

Restituisce i dettagli del framework per il `FrameworkName` specificato.

Sintassi della richiesta

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

frameworkName

Il nome univoco di un framework.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "DeploymentStatus": "string",
   "FrameworkArn": "string",
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
```

```
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkStatus": "string",
   "IdempotencyToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

La data e l'ora di creazione del framework, nella rappresentazione ISO 8601. Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, 2020-07-10T15:00:00.000-08:00 rappresenta il 10 luglio 2020 alle 15:00 8 ore indietro rispetto all'UTC.

Tipo: Timestamp

DeploymentStatus

Lo stato di implementazione di un framework. Gli stati sono:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

- Tipo: stringa

FrameworkArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

FrameworkControls

I controlli che compongono il framework. Ogni controllo nell'elenco dispone di nome, parametri di input e ambito.

Tipo: matrice di oggetti FrameworkControl

FrameworkDescription

Una descrizione facoltativa del framework.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `.*\S.*`

FrameworkName

Il nome univoco di un framework.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

Un framework consiste in uno o più controlli. Ogni controllo regola una risorsa, ad esempio piani di backup, selezioni di backup, vault di backup o punti di ripristino. È inoltre possibile attivare o disattivare la registrazione AWS Config per ciascuna risorsa. Gli stati sono:

- `ACTIVE` quando la registrazione è attivata per tutte le risorse amministrate dal framework.
- `PARTIALLY_ACTIVE` quando la registrazione è disattivata per almeno una risorsa amministrata dal framework.
- `INACTIVE` quando la registrazione è disattivata per tutte le risorse amministrate dal framework.
- `UNAVAILABLE`quando non AWS Backup è in grado di convalidare lo stato della registrazione in questo momento.

- Tipo: stringa

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `DescribeFrameworkOutput`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeGlobalSettings

Servizio: AWS Backup

Descrive se l' AWS account è abilitato al backup tra account. Restituisce un errore se l'account non è un membro di un'organizzazione Organizations. Esempio: `describe-global-settings --region us-west-2`

Sintassi della richiesta

```
GET /global-settings HTTP/1.1
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GlobalSettings

Lo stato del flag `isCrossAccountBackupEnabled`.

Tipo: mappatura stringa a stringa

LastUpdateTime

La data e l'ora dell'ultimo aggiornamento del flag `isCrossAccountBackupEnabled`. Questo aggiornamento è in formato Unix e nell'ora Coordinated Universal Time (UTC). Il valore di `LastUpdateTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python

- AWS SDK per Ruby V3

DescribeProtectedResource

Servizio: AWS Backup

Restituisce informazioni su una risorsa salvata, inclusa l'ultima volta in cui è stato eseguito il backup, il suo Amazon Resource Name (ARN) e il tipo di AWS servizio della risorsa salvata.

Sintassi della richiesta

```
GET /resources/resourceArn HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

resourceArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "LastBackupTime": number,
   "LastBackupVaultArn": "string",
   "LastRecoveryPointArn": "string",
   "LatestRestoreExecutionTimeMinutes": number,
   "LatestRestoreJobCreationDate": number,
   "LatestRestoreRecoveryPointCreationDate": number,
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LastBackupTime

La data e l'ora di esecuzione dell'ultimo backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `LastBackupTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

LastBackupVaultArn

L'ARN (Amazon Resource Name) dell'archivio di backup che contiene il punto di ripristino di backup più recente.

- Tipo: stringa

LastRecoveryPointArn

L'ARN (Amazon Resource Name) del punto di ripristino più recente.

- Tipo: stringa

LatestRestoreExecutionTimeMinutes

Il tempo, in minuti, impiegato per il completamento del processo di ripristino più recente.

Tipo: long

LatestRestoreJobCreationDate

La data di creazione del processo di ripristino più recente.

Tipo: Timestamp

LatestRestoreRecoveryPointCreationDate

La data di creazione del punto di ripristino più recente.

Tipo: Timestamp

ResourceArn

Un ARN che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

ResourceName

Il nome della risorsa che appartiene al backup specificato.

- Tipo: stringa

ResourceType

Il tipo di AWS risorsa salvata come punto di ripristino, ad esempio un volume Amazon EBS o un database Amazon RDS.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeRecoveryPoint

Servizio: AWS Backup

Restituisce i metadati associati a un punto di ripristino, inclusi ID, stato, crittografia e ciclo di vita.

Sintassi della richiesta

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

BackupVaultAccountId

L'ID dell'account del vault di backup specificato.

Modello: `^[0-9]{12}$`

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

recoveryPointArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupSizeInBytes": number,
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "CompletionDate": number,
   "CompositeMemberIdentifier": "string",
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "EncryptionKeyArn": "string",
   "IamRoleArn": "string",
   "IsEncrypted": boolean,
   "IsParent": boolean,
   "LastRestoreTime": number,
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "ParentRecoveryPointArn": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "SourceBackupVaultArn": "string",
   "Status": "string",
   "StatusMessage": "string",
   "StorageClass": "string",
   "VaultType": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupSizeInBytes

La dimensione, in byte, di un backup.

Tipo: long

BackupVaultArn

Un ARN che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

-Tipo: stringa

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

Un oggetto `CalculatedLifecycle` contenente i timestamp `DeleteAt` e `MoveToColdStorageAt`.

Tipo: oggetto CalculatedLifecycle

CompletionDate

La data e l'ora di completamento del processo di creazione di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

CompositeMemberIdentifier

L'identificatore di una risorsa all'interno di un gruppo composito, ad esempio un punto di ripristino annidato (figlio) appartenente a uno stack composito (principale). L'ID viene trasferito dall'ID logico all'interno di uno stack.

- Tipo: stringa

CreatedBy

Contiene informazioni di identificazione sulla creazione di un punto di ripristino, tra cui `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` e `BackupRuleId` del piano backup utilizzato per crearlo.

Tipo: oggetto RecoveryPointCreator

CreationDate

La data e l'ora di creazione di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

EncryptionKeyArn

La chiave di crittografia lato server utilizzata per proteggere i backup, ad esempio `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

- Tipo: stringa

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione; ad esempio, `arn:aws:iam::123456789012:role/S3Access`.

- Tipo: stringa

IsEncrypted

Un valore booleano che viene restituito come `TRUE` se il punto di ripristino specificato è crittografato o `FALSE` se il punto di ripristino non è crittografato.

Tipo: Booleano

IsParent

Ciò restituisce il valore booleano di cui un punto di ripristino è un processo padre (composito).

Tipo: Booleano

LastRestoreTime

La data e l'ora dell'ultimo ripristino di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `LastRestoreTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Lifecycle

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup esegue automaticamente le transizioni e le scadenze dei backup in base al ciclo di vita definito dall'utente.

I backup che vengono trasferiti allo storage dei dati inattivi devono essere archiviati nello storage per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Tipo: oggetto Lifecycle

ParentRecoveryPointArn

Questo è un ARN che identifica in modo univoco un punto di ripristino (composito) padre, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

RecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

ResourceArn

Un ARN identifica in modo univoco una risorsa salvata. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

ResourceName

Il nome della risorsa che appartiene al backup specificato.

- Tipo: stringa

ResourceType

Il tipo di AWS risorsa da salvare come punto di ripristino; ad esempio, un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS).

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

SourceBackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco il vault di origine in cui è stato originariamente eseguito il backup della risorsa, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`. Se il ripristino viene ripristinato nello stesso AWS account o nella stessa regione, questo valore sarà. `null`

- Tipo: stringa

Status

Un codice di stato che specifica lo stato del punto di ripristino.

`PARTIAL`lo stato indica che non è stato AWS Backup possibile creare il punto di ripristino prima della chiusura della finestra di backup. Per aumentare la finestra del piano di backup utilizzando l'API, vedi UpdateBackupPlan. Puoi anche aumentare la finestra del piano di backup utilizzando la console scegliendo e modificando il piano di backup.

`EXPIRED`lo stato indica che il punto di ripristino ha superato il periodo di conservazione, ma non AWS Backup dispone dell'autorizzazione o non è altrimenti in grado di eliminarlo. Per eliminare manualmente questi punti di ripristino, consulta Passaggio 3: Eliminare i punti di ripristino nella sezione Pulizia delle risorse di Nozioni di base.

Lo stato `STOPPED` si verifica in un backup continuo in cui un utente ha eseguito alcune azioni che causano la disabilitazione del backup continuo. Ciò può essere causato dalla rimozione delle autorizzazioni, dalla disattivazione del controllo delle versioni, dalla disattivazione degli eventi a

EventBridge cui vengono inviati o dalla disabilitazione delle EventBridge regole messe in atto da. AWS Backup

Per risolvere lo stato `STOPPED`, assicurati che tutte le autorizzazioni richieste siano in essere e che il controllo delle versioni sia abilitato sul bucket S3. Una volta soddisfatte queste condizioni, l'istanza successiva di una regola di backup in esecuzione comporterà la creazione di un nuovo punto di ripristino continuo. Non è necessario eliminare i punti di ripristino con stato STOPPED.

Per SAP HANA su Amazon EC2, lo stato `STOPPED` si verifica a causa dell'azione utente, della configurazione errata dell'applicazione o di un errore di backup. Per garantire il successo dei backup continui futuri, fai riferimento allo stato del punto di ripristino e controlla SAP HANA per i dettagli.

- Tipo: stringa

Valori validi: `COMPLETED | PARTIAL | DELETING | EXPIRED`

StatusMessage

Un messaggio di stato che spiega lo stato del punto di ripristino.

- Tipo: stringa

StorageClass

Specifica la classe di storage del punto di ripristino. I valori validi sono `WARM` e `COLD`.

- Tipo: stringa

Valori validi: `WARM | COLD | DELETED`

VaultType

Il tipo di archivio in cui è archiviato il punto di ripristino descritto.

- Tipo: stringa

Valori validi: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeRegionSettings

Servizio: AWS Backup

Restituisce le attuali impostazioni opt-in del servizio per la regione. Se l'opt-in del servizio è abilitato per un servizio, AWS Backup tenta di proteggere le risorse di quel servizio in questa regione, quando la risorsa è inclusa in un piano di backup su richiesta o pianificato. In caso contrario, AWS Backup non tenta di proteggere le risorse di tale servizio in questa regione.

Sintassi della richiesta

```
GET /account-settings HTTP/1.1
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ResourceTypeManagementPreference

Indica se gestisce AWS Backup completamente i backup per un tipo di risorsa.

Per i vantaggi della AWS Backup gestione completa, vedere AWS Backup Gestione completa.

Per un elenco dei tipi di risorse e per sapere se ciascuno supporta la AWS Backup gestione completa, consulta la tabella Disponibilità delle funzionalità per risorsa.

Se`"DynamoDB":false`, puoi abilitare la AWS Backup gestione completa del backup di DynamoDB abilitando le funzionalità di backup avanzate AWS Backup di DynamoDB.

Tipo: mappatura da stringa a matrice

Modello di chiave:`^[a-zA-Z0-9\-\_\.]{1,50}$`

ResourceTypeOptInPreference

I servizi insieme alle preferenze di attivazione nella regione.

Tipo: mappatura da stringa a matrice

Modello di chiave:`^[a-zA-Z0-9\-\_\.]{1,50}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2

- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeReportJob

Servizio: AWS Backup

Restituisce i dettagli associati alla creazione di un report come specificato da `ReportJobId`.

Sintassi della richiesta

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

reportJobId

L'identificatore del processo di report. Stringa con codifica UTF-8 Unicode univoca generata casualmente con lunghezza massima di 1.024 byte. L'ID processo report non può essere modificato.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJob": {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
         "S3BucketName": "string",
         "S3Keys": [ "string" ]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
```

```
        "StatusMessage": "string"
    }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ReportJob

Le informazioni su un processo di report, inclusi i tempi di completamento e creazione, la destinazione del report, l'ID univoco del processo di report, Amazon Resource Name (ARN), il modello di report, lo stato e il messaggio di stato.

Tipo: oggetto ReportJob

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeReportPlan

Servizio: AWS Backup

Restituisce un elenco di tutti i piani di report per un Account AWS and Regione AWS.

Sintassi della richiesta

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

reportPlanName

Il nome univoco di un piano di report.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
```

```
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "OrganizationUnits": [ "string" ],
         "Regions": [ "string" ],
         "ReportTemplate": "string"
      }
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ReportPlan

Restituisce i dettagli sul piano di report specificato in base al relativo nome. Questi dettagli includono il nome della risorsa Amazon (ARN) del piano di report, la descrizione, le impostazioni, il canale di distribuzione, lo stato di implementazione, l'ora di creazione e le ore ultimo tentativo ed esecuzione completata.

Tipo: oggetto ReportPlan

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeRestoreJob

Servizio: AWS Backup

Restituisce i metadati associati a un processo di ripristino specificato da un ID processo.

Sintassi della richiesta

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

restoreJobId

Identifica in modo univoco il processo che ripristina un punto di ripristino.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupSizeInBytes": number,
   "CompletionDate": number,
   "CreatedBy": {
      "RestoreTestingPlanArn": "string"
   },
   "CreatedResourceArn": "string",
   "CreationDate": number,
   "DeletionStatus": "string",
   "DeletionStatusMessage": "string",
   "ExpectedCompletionTimeMinutes": number,
   "IamRoleArn": "string",
   "PercentDone": "string",
```

```
    "RecoveryPointArn": "string",
    "RecoveryPointCreationDate": number,
    "ResourceType": "string",
    "RestoreJobId": "string",
    "Status": "string",
    "StatusMessage": "string",
    "ValidationStatus": "string",
    "ValidationStatusMessage": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AccountId

Restituisce l'ID account proprietario del processo di ripristino.

Tipo: stringa

Modello: `^[0-9]{12}$`

BackupSizeInBytes

La dimensione, in byte, della risorsa ripristinata.

Tipo: long

CompletionDate

La data e l'ora di completamento del processo di ripristino di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

CreatedBy

Contiene informazioni di identificazione sulla creazione di un processo di ripristino.

Tipo: oggetto RestoreJobCreator

CreatedResourceArn

L'Amazon Resource Name (ARN) della risorsa creata dal processo di ripristino.

Il formato dell'ARN dipende dal tipo della risorsa di cui si esegue il backup.

- Tipo: stringa

CreationDate

La data e l'ora in cui è stato creato il processo di ripristino, nel formato orario Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

DeletionStatus

Lo stato dei dati generati dal test di ripristino.

- Tipo: stringa

Valori validi: `DELETING | FAILED | SUCCESSFUL`

DeletionStatusMessage

Descrive lo stato di eliminazione del processo di ripristino.

- Tipo: stringa

ExpectedCompletionTimeMinutes

La quantità di tempo in minuti prevista per l'esecuzione del processo di ripristino di un punto di ripristino.

Tipo: long

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione; ad esempio, `arn:aws:iam::123456789012:role/S3Access`.

- Tipo: stringa

PercentDone

Contiene una percentuale stimata di completamento di un processo nel momento in cui è stato richiesto lo stato del processo.

- Tipo: stringa

RecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

RecoveryPointCreationDate

La data di creazione del punto di ripristino creato dal processo di ripristino specificato.

Tipo: Timestamp

ResourceType

Restituisce i metadati associati a un processo di ripristino elencati per tipo di risorsa.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

Identifica in modo univoco il processo che ripristina un punto di ripristino.

- Tipo: stringa

Status

Codice di stato che specifica lo stato del processo avviato da AWS Backup per ripristinare un punto di ripristino.

- Tipo: stringa

Valori validi: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

Un messaggio che mostra lo stato di un processo per ripristinare un punto di ripristino.

- Tipo: stringa

ValidationStatus

Lo stato di convalida eseguito sul processo di ripristino indicato.

- Tipo: stringa

Valori validi: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

Il messaggio sullo stato.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

DependencyFailureException

Un AWS servizio o una risorsa dipendente ha restituito un errore al AWS Backup servizio e l'azione non può essere completata.

Codice di stato HTTP: 500

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DisassociateRecoveryPoint

Servizio: AWS Backup

Elimina il punto di ripristino del backup continuo specificato AWS Backup e rilascia il controllo di tale backup continuo sul servizio di origine, ad esempio Amazon RDS. Il servizio di origine continuerà a creare e mantenere backup continui utilizzando il ciclo di vita specificato nel piano di backup originale.

Non supporta i punti di ripristino del backup snapshot.

Sintassi della richiesta

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome univoco di un AWS Backup vault.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

recoveryPointArn

Un Amazon Resource Name (ARN) che identifica in modo univoco un punto di ripristino. AWS Backup

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

InvalidResourceStateException

AWS Backup sta già eseguendo un'azione su questo punto di ripristino. Non può eseguire l'azione richiesta fino al termine della prima azione. Riprova più tardi.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DisassociateRecoveryPointFromParent

Servizio: AWS Backup

Questa azione su un punto di ripristino (nidificato) figlio specifico rimuove la relazione tra il punto di ripristino specificato e il relativo punto di ripristino (composito) padre.

Sintassi della richiesta

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un contenitore logico in cui è memorizzato il punto di ripristino secondario (annidato). Gli archivi di Backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la AWS regione in cui vengono creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

recoveryPointArn

L'Amazon Resource Name (ARN) che identifica in modo univoco il punto di ripristino secondario (annidato); ad esempio, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 204
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta AWS quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ExportBackupPlanTemplate

Servizio: AWS Backup

Restituisce il piano di backup specificato dall'ID del piano come un modello di backup.

Sintassi della richiesta

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

Identifica in modo univoco un piano di backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlanTemplateJson

Il corpo di un modello del piano di backup in formato JSON.

> **Note**
>
> Si tratta di un documento JSON firmato che non può essere modificato prima di essere passato a `GetBackupPlanFromJSON`.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetBackupPlan

Servizio: AWS Backup

Restituisce i dettagli `BackupPlan` per il `BackupPlanId` specificato. I dettagli sono il corpo di un piano di backup in formato JSON, in aggiunta ai metadati del piano.

Sintassi della richiesta

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

Identifica in modo univoco un piano di backup.

Campo obbligatorio: sì

VersionId

Stringhe con codifica UTF-8 Unicode univoche generate casualmente con lunghezza massimo di 1.024 byte. Gli ID versione non possono essere modificati.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
```

```
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   },
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
```

```
    "CreatorRequestId": "string",
    "DeletionDate": number,
    "LastExecutionDate": number,
    "VersionId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AdvancedBackupSettings

Contiene un elenco di `BackupOptions` per ogni tipo di risorsa. L'elenco viene compilato solo se l'opzione avanzata è impostata per il piano di backup.

Tipo: matrice di oggetti AdvancedBackupSetting

BackupPlan

Specifica il corpo di un piano di backup. Include un `BackupPlanName` e uno o più set di `Rules`.

Tipo: oggetto BackupPlan

BackupPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

- Tipo: stringa

BackupPlanId

Identifica in modo univoco un piano di backup.

- Tipo: stringa

CreationDate

La data e l'ora di creazione di un piano di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte.

- Tipo: stringa

DeletionDate

La data e ora di eliminazione di un piano di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `DeletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

LastExecutionDate

L'ultima volta che è stato eseguito questo piano di backup. Una data e ora, in formato UNIX e nell'ora Universal Coordinated Time (UTC). Il valore di `LastExecutionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

VersionId

Stringhe con codifica UTF-8 Unicode univoche generate casualmente con lunghezza massimo di 1.024 byte. Gli ID versione non possono essere modificati.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetBackupPlanFromJSON

Servizio: AWS Backup

Restituisce un documento JSON valido che specifica un piano di backup o un errore.

Sintassi della richiesta

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupPlanTemplateJson

Un documento del piano di backup fornito dal cliente in formato JSON.

Tipo: stringa

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
```

```
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlan

Specifica il corpo di un piano di backup. Include un `BackupPlanName` e uno o più set di `Rules`.

Tipo: oggetto BackupPlan

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetBackupPlanFromTemplate

Servizio: AWS Backup

Restituisce il modello specificato dal relativo `templateId` come un piano di backup.

Sintassi della richiesta

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

templateId

Identifica in modo univoco un modello di piano di backup archiviato.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanDocument": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
```

```
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlanDocument

Restituisce il corpo di un piano di backup basato sul modello di destinazione, inclusi il nome, le regole e il vault di backup del piano.

Tipo: oggetto BackupPlan

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python

- AWS SDK per Ruby V3

GetBackupSelection

Servizio: AWS Backup

Restituisce i metadati di selezione e un documento in formato JSON che specifica un elenco di risorse associate a un piano di backup.

Sintassi della richiesta

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

Identifica in modo univoco un piano di backup.

Campo obbligatorio: sì

selectionId

Identifica in modo univoco il corpo di una richiesta per assegnare un set di risorse a un piano di backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
```

```
                "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreationDate": number,
   "CreatorRequestId": "string",
   "SelectionId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlanId

Identifica in modo univoco un piano di backup.

- Tipo: stringa

BackupSelection

Specifica il corpo di una richiesta per assegnare un set di risorse a un piano di backup.

Tipo: oggetto BackupSelection

CreationDate

La data e l'ora di creazione di una selezione di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte.

- Tipo: stringa

SelectionId

Identifica in modo univoco il corpo di una richiesta per assegnare un set di risorse a un piano di backup.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetBackupVaultAccessPolicy

Servizio: AWS Backup

Restituisce il documento relativo alla policy di accesso associato al vault di backup denominato.

Sintassi della richiesta

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Policy

Il documento relativo alla policy di accesso del vault di backup in formato JSON.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetBackupVaultNotifications

Servizio: AWS Backup

Restituisce le notifiche degli eventi per il vault di backup specificato.

Sintassi della richiesta

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

BackupVaultEvents

Un array di eventi che indica lo stato dei processi per il backup delle per il vault di backup.

Tipo: matrice di stringhe

Valori validi: `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED`

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

SNSTopicArn

Un ARN che identifica in modo univoco un argomento Amazon Simple Notification Service (Amazon SNS); ad esempio, `arn:aws:sns:us-west-2:111122223333:MyTopic`.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetLegalHold

Servizio: AWS Backup

Questa azione restituisce i dettagli per un blocco ai fini legali specificato. I dettagli sono il corpo di un blocco ai fini legali in formato JSON, in aggiunta ai metadati.

Sintassi della richiesta

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

legalHoldId

L'ID del deposito legale.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CancelDescription": "string",
   "CancellationDate": number,
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
```

```
      "VaultNames": [ "string" ]
   },
   "RetainRecordUntil": number,
   "Status": "string",
   "Title": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CancelDescription

Il motivo per cui è stata rimossa la sospensione legale.

- Tipo: stringa

CancellationDate

L'ora in cui il blocco legale è stato annullato.

Tipo: Timestamp

CreationDate

L'ora in cui è stata creata la conservazione legale.

Tipo: Timestamp

Description

La descrizione della custodia legale.

- Tipo: stringa

LegalHoldArn

L'ARN del framework per la conservazione legale specificata. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

LegalHoldId

L'ID del deposito legale.

- Tipo: stringa

RecoveryPointSelection

I criteri per assegnare un set di risorse, ad esempio i tipi di risorse o gli archivi di backup.

Tipo: oggetto RecoveryPointSelection

RetainRecordUntil

La data e l'ora fino alle quali viene conservato il record di conservazione legale.

Tipo: Timestamp

Status

Lo stato della custodia legale.

- Tipo: stringa

Valori validi: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

Il titolo del deposito legale.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetRecoveryPointRestoreMetadata

Servizio: AWS Backup

Restituisce un set di coppie chiave-valore che sono state utilizzate per creare il backup.

Sintassi della richiesta

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

BackupVaultAccountId

L'ID dell'account del vault di backup specificato.

Modello: `^[0-9]{12}$`

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

recoveryPointArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupVaultArn

Un ARN che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

RecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

ResourceType

Il tipo di risorsa del punto di ripristino.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreMetadata

Il set di coppie chiave-valore dei metadati che descrivono la configurazione originale della risorsa di cui è stato eseguito il backup. Questi valori variano a seconda del servizio che viene ripristinato.

Tipo: mappatura stringa a stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python

- AWS SDK per Ruby V3

GetRestoreJobMetadata

Servizio: AWS Backup

Questa richiesta restituisce i metadati per il processo di ripristino specificato.

Sintassi della richiesta

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

restoreJobId

Si tratta di un identificatore univoco di un processo di ripristino all'interno AWS Backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Metadata

Contiene i metadati del processo di backup specificato.

Tipo: mappatura stringa a stringa

RestoreJobId

Si tratta di un identificatore univoco di un processo di ripristino all'interno di. AWS Backup

-Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetRestoreTestingInferredMetadata

Servizio: AWS Backup

Questa richiesta restituisce il set minimo di metadati necessario per avviare un processo di ripristino con impostazioni predefinite sicure. `BackupVaultName` e `RecoveryPointArn` sono parametri obbligatori. `BackupVaultAccountId` è un parametro facoltativo.

Sintassi della richiesta

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

BackupVaultAccountId

L'ID dell'account del vault di backup specificato.

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. Gli archivi di Backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la AWS regione in cui vengono creati. Consistono in lettere, numeri e trattini.

Campo obbligatorio: sì

RecoveryPointArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

InferredMetadata

Questa è una mappa di stringhe dei metadati dedotti dalla richiesta.

Tipo: mappatura stringa a stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetRestoreTestingPlan

Servizio: AWS Backup

Restituisce i dettagli `RestoreTestingPlan` per il `RestoreTestingPlanName` specificato. I dettagli sono il corpo di un piano di test di ripristino in formato JSON, in aggiunta ai metadati del piano.

Sintassi della richiesta

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

RestoreTestingPlanName

Il nome univoco richiesto del piano di test di ripristino.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingPlan": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "LastExecutionTime": number,
      "LastUpdateTime": number,
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
```

```
      },
      "RestoreTestingPlanArn": "string",
      "RestoreTestingPlanName": "string",
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

RestoreTestingPlan

Specifica il corpo di un piano di test di ripristino. Include `RestoreTestingPlanName`.

Tipo: oggetto RestoreTestingPlanForGet

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetRestoreTestingSelection

Servizio: AWS Backup

Restituisce RestoreTestingSelection, che mostra le risorse e gli elementi del piano di test di ripristino.

Sintassi della richiesta

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

RestoreTestingPlanName

Il nome univoco richiesto del piano di test di ripristino.

Campo obbligatorio: sì

RestoreTestingSelectionName

Il nome univoco richiesto della selezione del test di ripristino.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingSelection": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
```

```
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingPlanName": "string",
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

RestoreTestingSelection

Nome univoco della selezione del test di ripristino.

Tipo: oggetto RestoreTestingSelectionForGet

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetSupportedResourceTypes

Servizio: AWS Backup

Restituisce i tipi di AWS risorse supportati da AWS Backup.

Sintassi della richiesta

```
GET /supported-resource-types HTTP/1.1
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ResourceTypes

Contiene una stringa con i tipi di AWS risorse supportati:

- `Aurora` per Amazon Aurora
- `CloudFormation`per AWS CloudFormation
- `DocumentDB` per Amazon DocumentDB (compatibile con MongoDB)
- `DynamoDB` per Amazon DynamoDB
- `EBS` per Amazon Elastic Block Store

- `EC2` per Amazon Elastic Compute Cloud
- `EFS` per Amazon Elastic File System
- `FSX` per Amazon FSx
- `Neptune` per Amazon Neptune
- `RDS` per Amazon Relational Database Service
- `Redshift` per Amazon Redshift
- `SAP HANA on Amazon EC2`per database SAP HANA su istanze Amazon Elastic Compute Cloud
- `S3`per Amazon Simple Storage Service (Amazon S3)
- `Storage Gateway`per AWS Storage Gateway
- `Timestream` per Amazon Timestream
- `VirtualMachine`per macchine virtuali VMware

Tipo: matrice di stringhe

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListBackupJobs

Servizio: AWS Backup

Restituisce un elenco di processi di backup esistenti per un account autenticato negli ultimi 30 giorni. Per un periodo di tempo più lungo, prendere in considerazione l'utilizzo di questi strumenti di monitoraggio.

Sintassi della richiesta

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

ByAccountId

L'ID account da cui elencare i processi. Restituisce solo i processi di backup associati all'ID account specificato.

Se utilizzato da un account di AWS Organizations gestione, pass * restituisce tutti i lavori all'interno dell'organizzazione.

Modello: `^[0-9]{12}$`

ByBackupVaultName

Restituisce solo i processi di backup che verranno archiviati nel vault di backup specificato. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

ByCompleteAfter

Restituisce solo i processi di backup completati dopo una data espressa nel formato Unix e nell'ora UTC (Coordinated Universal Time).

ByCompleteBefore

Restituisce solo i processi di backup completati prima di una data espressa nel formato Unix e nell'ora UTC (Coordinated Universal Time).

ByCreatedAfter

Restituisce solo i processi di backup creati dopo la data specificata.

ByCreatedBefore

Restituisce solo i processi di backup creati prima della data specificata.

ByMessageCategory

Si tratta di un parametro opzionale che può essere utilizzato per filtrare i lavori con un valore MessageCategory che corrisponde al valore immesso.

Stringhe di esempio possono essere `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `InvalidParameters`.

Consulta Monitoraggio.

Il carattere jolly () restituisce il conteggio di tutte le categorie di messaggi.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutte le categorie di messaggi e restituisce la somma.

ByParentJobId

Si tratta di un filtro per elencare i processi (nidificati) figlio in base all'ID del processo padre.

ByResourceArn

Restituisce solo i processi di backup che corrispondono alla al nome della risorsa Amazon (ARN) specificata.

ByResourceType

Restituisce solo i processi di backup per le risorse specificate:

- `Aurora` per Amazon Aurora
- `CloudFormation`per AWS CloudFormation
- `DocumentDB` per Amazon DocumentDB (compatibile con MongoDB)
- `DynamoDB` per Amazon DynamoDB
- `EBS` per Amazon Elastic Block Store
- `EC2` per Amazon Elastic Compute Cloud
- `EFS` per Amazon Elastic File System

- `FSx` per Amazon FSx
- `Neptune` per Amazon Neptune
- `Redshift` per Amazon Redshift
- `RDS` per Amazon Relational Database Service
- `SAP HANA on Amazon EC2` per database SAP HANA
- `Storage Gatewayper` AWS Storage Gateway
- `S3` per Amazon S3
- `Timestream` per Amazon Timestream
- `VirtualMachine` per macchine virtuali

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Restituisce solo i processi di backup che si trovano nello stato specificato.

`Completed with issues` è uno stato specifico della console AWS Backup . Per l'API, questo stato si riferisce ai processi `COMPLETED` e a `MessageCategory` con un valore diverso da `SUCCESS`, vale a dire, lo stato è completato ma è accompagnato da un messaggio di stato.

Per ottenere il numero di processi per `Completed with issues`, esegui due richieste GET e sottrai il secondo numero più piccolo:

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

Valori validi: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobs": [
      {
         "AccountId": "string",
         "BackupJobId": "string",
         "BackupOptions": {
            "string" : "string"
         },
         "BackupSizeInBytes": number,
         "BackupType": "string",
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "BytesTransferred": number,
         "CompletionDate": number,
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "ExpectedCompletionDate": number,
         "IamRoleArn": "string",
         "InitiationDate": number,
         "IsParent": boolean,
         "MessageCategory": "string",
         "ParentJobId": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "StartBy": number,
         "State": "string",
         "StatusMessage": "string"
```

```
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupJobs

Un array di strutture contenenti metadati sui processi di backup restituiti in formato JSON.

Tipo: matrice di oggetti BackupJob

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListBackupJobSummaries

Servizio: AWS Backup

È la richiesta di riepilogo dei processi di backup creati o eseguiti negli ultimi 30 giorni. È possibile includere i parametri AccountID, State,, ResourceType, MessageCategory AggregationPeriod MaxResults, o NextToken per filtrare i risultati.

Questa richiesta restituisce un riepilogo che contiene Regione, Account ResourceType, Stato MessageCategory, StartTime, EndTime, e Numero di lavori inclusi.

Sintassi della richiesta

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

AccountId

Restituisce il numero di processi per l'account specificato.

Se la richiesta viene inviata da un account membro o da un account che non fa parte di AWS Organizations, verranno restituiti i lavori all'interno dell'account del richiedente.

Gli account root, amministratore e amministratore delegato possono utilizzare il valore ANY per restituire il numero di processi di ogni account dell'organizzazione.

AGGREGATE_ALL aggrega i numeri dei processi di tutti gli account dell'organizzazione autenticata, quindi restituisce la somma.

Modello: `^[0-9]{12}$`

AggregationPeriod

Periodo per i risultati restituiti.

- ONE_DAY- Il numero di lavori giornalieri per i 14 giorni precedenti.
- SEVEN_DAYS- Il numero aggregato dei lavori per i 7 giorni precedenti.
- FOURTEEN_DAYS- Il numero aggregato dei lavori per i 14 giorni precedenti.

Valori validi: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Il numero massimo di elementi da restituire.

Il valore è un numero intero. L'intervallo di valori validi è compreso tra 1 e 500.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

MessageCategory

Questo parametro restituisce il numero di processi per la categoria di messaggi specificata.

Stringhe di esempio valide sono `AccessDenied`, `Success` e `InvalidParameters`. Vedi Monitoraggio per un elenco delle MessageCategory stringhe accettate.

Il valore ANY restituisce il conteggio di tutte le categorie di messaggi.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutte le categorie di messaggi e restituisce la somma.

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

ResourceType

Restituisce il numero di processi per il tipo di risorsa specificato. Usa la richiesta `GetSupportedResourceTypes` per ottenere le stringhe per i tipi di risorsa supportati.

Il valore ANY restituisce il conteggio di tutti i tipi di risorse.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutti i tipi di risorsa e restituisce la somma.

Il tipo di AWS risorsa di cui eseguire il backup; ad esempio, un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS).

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Questo parametro restituisce il numero di processi con lo stato specificato.

Il valore ANY restituisce il conteggio di tutti gli stati.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutti gli stati e restituisce la somma.

`Completed with issues` è uno stato specifico della console AWS Backup . Per l'API, questo stato si riferisce ai processi `COMPLETED` e a `MessageCategory` con un valore diverso da `SUCCESS`, vale a dire, lo stato è completato ma è accompagnato da un messaggio di stato. Per ottenere il numero di processi per `Completed with issues`, esegui due richieste GET e sottrai il secondo numero più piccolo:

OTTIENI /audit/? backup-job-summaries AggregationPeriod=fourteen_days&state=Completato

OTTIENI /audit/? backup-job-summaries AggregationPeriod=QUATTORDICI_GIORNI& =successo&state=Completato MessageCategory

Valori validi: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "BackupJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AggregationPeriod

Il periodo per i risultati restituiti.

- `ONE_DAY`- Il numero di lavori giornalieri per i 14 giorni precedenti.
- `SEVEN_DAYS`- Il numero aggregato dei lavori per i 7 giorni precedenti.
- `FOURTEEN_DAYS`- Il numero aggregato dei lavori per i 14 giorni precedenti.

Tipo: stringa

BackupJobSummaries

Le informazioni di riepilogo.

Tipo: matrice di oggetti BackupJobSummary

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListBackupPlans

Servizio: AWS Backup

Elenca i piani di backup attivi per l'account.

Sintassi della richiesta

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

IncludeDeleted

Un valore booleano con un valore predefinito di `FALSE` che restituisce i piani di backup eliminati se impostato su `TRUE`.

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlansList": [
      {
```

```
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlansList

Informazioni sui piani di backup.

Tipo: matrice di oggetti BackupPlansListMember

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListBackupPlanTemplates

Servizio: AWS Backup

Elenca i modelli del piano di backup.

Sintassi della richiesta

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

Il numero massimo di articoli da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlanTemplatesList

Un array di elementi dell'elenco di modelli contenenti i metadati sui modelli salvati.

Tipo: matrice di oggetti BackupPlanTemplatesListMember

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListBackupPlanVersions

Servizio: AWS Backup

Restituisce i metadati della versione dei piani di backup, inclusi nomi della risorsa Amazon (ARN), ID dei piani di backup, date di creazione ed eliminazione, nomi dei piani e ID versione.

Sintassi della richiesta

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

Identifica in modo univoco un piano di backup.

Campo obbligatorio: sì

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupPlanVersionsList": [
      {
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupPlanVersionsList

Un array di elementi dell'elenco delle versioni contenenti i metadati relativi ai piani di backup.

Tipo: matrice di oggetti BackupPlansListMember

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python

- AWS SDK per Ruby V3

ListBackupSelections

Servizio: AWS Backup

Restituisce un array contenente i metadati delle risorse associate al piano di backup di destinazione.

Sintassi della richiesta

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

Identifica in modo univoco un piano di backup.

Campo obbligatorio: sì

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupSelectionsList": [
```

```
      {
         "BackupPlanId": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "IamRoleArn": "string",
         "SelectionId": "string",
         "SelectionName": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupSelectionsList

Un array di elementi dell'elenco di selezione di backup contenente metadati relativi a ciascuna risorsa dell'elenco.

Tipo: matrice di oggetti BackupSelectionsListMember

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListBackupVaults

Servizio: AWS Backup

Restituisce un elenco di container di storage dei punti di ripristino insieme alle informazioni su di essi.

Sintassi della richiesta

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

ByShared

Questo parametro ordinerà l'elenco di vault in base ai vault condivisi.

ByVaultType

Questo parametro ordinerà l'elenco di vault in base al tipo di vault.

Valori validi: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupVaultList": [
      {
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "EncryptionKeyArn": "string",
         "LockDate": number,
         "Locked": boolean,
         "MaxRetentionDays": number,
         "MinRetentionDays": number,
         "NumberOfRecoveryPoints": number
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupVaultList

Un array di membri dell'elenco dei vault di backup contenenti metadati di vault, inclusi nome della risorsa Amazon (ARN), nome visualizzato, data di creazione, numero di punti di ripristino salvati e informazioni di crittografia se le risorse salvate nel vault di backup sono crittografate.

Tipo: matrice di oggetti BackupVaultListMember

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListCopyJobs

Servizio: AWS Backup

Restituisce i metadati relativi ai processi di copia.

Sintassi della richiesta

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

ByAccountId

L'ID account da cui elencare i processi. Restituisce solo i processi di copia associati all'ID account specificato.

Modello: `^[0-9]{12}$`

ByCompleteAfter

Restituisce solo i processi di copia completati dopo una data espressa nel formato Unix e nell'ora UTC (Coordinated Universal Time).

ByCompleteBefore

Restituisce solo i processi di copia completati prima di una data espressa nel formato Unix e nell'ora UTC (Coordinated Universal Time).

ByCreatedAfter

Restituisce solo i processi di copia creati dopo la data specificata.

ByCreatedBefore

Restituisce solo i processi di copia creati prima della data specificata.

ByDestinationVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup di origine da cui copiare, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

ByMessageCategory

Questo è un parametro opzionale che può essere utilizzato per filtrare i lavori con un valore MessageCategory che corrisponde al valore immesso.

Stringhe di esempio possono essere `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `INVALIDPARAMETERS`.

Visualizza Monitoraggio per un elenco di stringhe accettate.

Il valore ANY restituisce il conteggio di tutte le categorie di messaggi.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutte le categorie di messaggi e restituisce la somma.

ByParentJobId

Si tratta di un filtro per elencare i processi (nidificati) figlio in base all'ID del processo padre.

ByResourceArn

Restituisce solo i processi di copia che corrispondono al nome della risorsa Amazon (ARN) specificata.

ByResourceType

Restituisce solo i processi di backup per le risorse specificate:

- `Aurora` per Amazon Aurora
- `CloudFormation`per AWS CloudFormation
- `DocumentDB` per Amazon DocumentDB (compatibile con MongoDB)
- `DynamoDB` per Amazon DynamoDB
- `EBS` per Amazon Elastic Block Store
- `EC2` per Amazon Elastic Compute Cloud
- `EFS` per Amazon Elastic File System
- `FSx` per Amazon FSx
- `Neptune` per Amazon Neptune
- `Redshift` per Amazon Redshift
- `RDS` per Amazon Relational Database Service
- `SAP HANA on Amazon EC2` per database SAP HANA
- `Storage Gateway`per AWS Storage Gateway

- `S3` per Amazon S3
- `Timestream` per Amazon Timestream
- `VirtualMachine` per macchine virtuali

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Restituisce solo i processi di copia che si trovano nello stato specificato.

Valori validi: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta di restituzione di un MaxResults numero di articoli, NextToken consente di restituire più elementi nell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "ChildJobsInState": {
            "string" : number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
```

```
         "CopyJobId": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "DestinationBackupVaultArn": "string",
         "DestinationRecoveryPointArn": "string",
         "IamRoleArn": "string",
         "IsParent": boolean,
         "MessageCategory": "string",
         "NumberOfChildJobs": number,
         "ParentJobId": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "SourceBackupVaultArn": "string",
         "SourceRecoveryPointArn": "string",
         "State": "string",
         "StatusMessage": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CopyJobs

Un array di strutture contenenti metadati sui processi di copia restituiti in formato JSON.

Tipo: matrice di oggetti CopyJob

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta di restituzione di un MaxResults numero di articoli, NextToken consente di restituire più elementi nell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListCopyJobSummaries

Servizio: AWS Backup

Questa richiesta ottiene un elenco di processi di copia creati o eseguiti negli ultimi 30 giorni. È possibile includere i parametri AccountID, State,, ResourceType, MessageCategory AggregationPeriod MaxResults, o NextToken per filtrare i risultati.

Questa richiesta restituisce un riepilogo che contiene Regione, Account RestourceType, Stato MessageCategory, StartTime, EndTime, e Numero di lavori inclusi.

Sintassi della richiesta

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

AccountId

Restituisce il numero di processi per l'account specificato.

Se la richiesta viene inviata da un account membro o da un account che non fa parte di AWS Organizations, verranno restituiti i lavori all'interno dell'account del richiedente.

Gli account root, amministratore e amministratore delegato possono utilizzare il valore ANY per restituire il numero di processi di ogni account dell'organizzazione.

AGGREGATE_ALL aggrega i numeri dei processi di tutti gli account dell'organizzazione autenticata, quindi restituisce la somma.

Modello: ^[0-9]{12}$

AggregationPeriod

Periodo per i risultati restituiti.

- ONE_DAY- Il numero di lavori giornalieri per i 14 giorni precedenti.
- SEVEN_DAYS- Il numero aggregato dei lavori per i 7 giorni precedenti.
- FOURTEEN_DAYS- Il numero aggregato dei lavori per i 14 giorni precedenti.

Valori validi: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Questo parametro imposta il numero massimo di elementi da restituire.

Il valore è un numero intero. L'intervallo di valori validi è compreso tra 1 e 500.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

MessageCategory

Questo parametro restituisce il numero di processi per la categoria di messaggi specificata.

Stringhe di esempio valide sono `AccessDenied`, `Success` e `InvalidParameters`. Vedi Monitoraggio per un elenco delle MessageCategory stringhe accettate.

Il valore ANY restituisce il conteggio di tutte le categorie di messaggi.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutte le categorie di messaggi e restituisce la somma.

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

ResourceType

Restituisce il numero di processi per il tipo di risorsa specificato. Usa la richiesta `GetSupportedResourceTypes` per ottenere le stringhe per i tipi di risorsa supportati.

Il valore ANY restituisce il conteggio di tutti i tipi di risorse.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutti i tipi di risorsa e restituisce la somma.

Il tipo di AWS risorsa di cui eseguire il backup; ad esempio, un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS).

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Questo parametro restituisce il numero di processi con lo stato specificato.

Il valore ANY restituisce il conteggio di tutti gli stati.

AGGREGATE_ALL aggrega i numeri dei processi per tutti gli stati e restituisce la somma.

Valori validi: CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "CopyJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AggregationPeriod

Il periodo in cui vengono restituiti i risultati.

- `ONE_DAY`- Il numero di lavori giornalieri per i 14 giorni precedenti.
- `SEVEN_DAYS`- Il numero aggregato dei lavori per i 7 giorni precedenti.
- `FOURTEEN_DAYS`- Il numero aggregato dei lavori per i 14 giorni precedenti.

Tipo: stringa

CopyJobSummaries

Questo risultato mostra un riepilogo che contiene la regione, l'account, lo stato ResourceType MessageCategory, StartTime EndTime, e il numero di lavori inclusi.

Tipo: matrice di oggetti CopyJobSummary

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListFrameworks

Servizio: AWS Backup

Restituisce un elenco di tutti i framework per un Account AWS and. Regione AWS

Sintassi della richiesta

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

Il numero di risultati desiderato è compreso tra 1 e 1.000. Facoltativo. Se non specificato, la query restituirà 1 MB di dati.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

Un identificatore restituito dalla precedente chiamata a questa operazione, che può essere utilizzato per restituire il successivo set di elementi nell'elenco.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
```

```
            "FrameworkName": "string",
            "NumberOfControls": number
        }
    ],
    "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Frameworks

I framework con i dettagli per ogni framework, tra cui il nome del framework, Amazon Resource Name (ARN), la descrizione, il numero di controlli, l'ora di creazione e lo stato della distribuzione.

Tipo: matrice di oggetti Framework

NextToken

Un identificatore restituito dalla precedente chiamata a questa operazione, che può essere utilizzato per restituire il successivo set di elementi nell'elenco.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListLegalHolds

Servizio: AWS Backup

Questa azione restituisce i metadati relativi ai blocchi a fini legali attivi e precedenti.

Sintassi della richiesta

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

Il numero massimo di elementi dell'elenco di risorse da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "LegalHolds": [
      {
         "CancellationDate": number,
         "CreationDate": number,
         "Description": "string",
         "LegalHoldArn": "string",
         "LegalHoldId": "string",
```

```
            "Status": "string",
            "Title": "string"
        }
    ],
    "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

LegalHolds

Si tratta di un array di blocchi a fini legali restituiti, attivi e precedenti.

Tipo: matrice di oggetti LegalHold

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListProtectedResources

Servizio: AWS Backup

Restituisce una serie di risorse da cui è stato eseguito correttamente il backup AWS Backup, incluso l'ora in cui la risorsa è stata salvata, un Amazon Resource Name (ARN) della risorsa e un tipo di risorsa.

Sintassi della richiesta

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
```

```
            "LastRecoveryPointArn": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string"
        }
    ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

Results

Una serie di risorse di cui è stato eseguito correttamente il backup, AWS Backup includendo l'ora in cui la risorsa è stata salvata, un Amazon Resource Name (ARN) della risorsa e un tipo di risorsa.

Tipo: matrice di oggetti ProtectedResource

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListProtectedResourcesByBackupVault

Servizio: AWS Backup

Questa richiesta elenca le risorse protette corrispondenti a ciascun vault di backup.

Sintassi della richiesta

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

BackupVaultAccountId

L'elenco delle risorse protette dall'archivio di backup all'interno degli archivi specificati in base all'ID dell'account.

Modello: `^[0-9]{12}$`

backupVaultName

L'elenco delle risorse protette dall'archivio di backup all'interno degli archivi specificati per nome.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

Results

Questi sono i risultati restituiti per la richiesta. ListProtectedResourcesByBackupVault

Tipo: matrice di oggetti ProtectedResource

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRecoveryPointsByBackupVault

Servizio: AWS Backup

Restituisce informazioni dettagliate sui punti di ripristino archiviati in un vault di backup.

Sintassi della richiesta

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

BackupVaultAccountId

Questo parametro ordina l'elenco dei punti di ripristino in base all'ID account.

Modello: `^[0-9]{12}$`

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

> **Note**
>
> È possibile che il nome del vault di backup non sia disponibile quando un servizio supportato crea il backup.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

ByBackupPlanId

Restituisce solo i punti di ripristino che corrispondono all'ID del piano di backup specificato.

ByCreatedAfter

Restituisce solo i punti di ripristino creati dopo il timestamp specificato.

ByCreatedBefore

Restituisce solo i punti di ripristino creati prima del timestamp specificato.

ByParentRecoveryPointArn

Ciò restituisce solo i punti di ripristino che corrispondono al nome della risorsa Amazon (ARN) del punto di ripristino (composito) padre.

ByResourceArn

Restituisce solo i processi di ripristino che corrispondono al nome della risorsa Amazon (ARN) specificata.

ByResourceType

Restituisce solo i punti di ripristino che corrispondono ai tipi di risorsa specificati.

- `Aurora` per Amazon Aurora
- `CloudFormation`per AWS CloudFormation
- `DocumentDB` per Amazon DocumentDB (compatibile con MongoDB)
- `DynamoDB` per Amazon DynamoDB
- `EBS` per Amazon Elastic Block Store
- `EC2` per Amazon Elastic Compute Cloud
- `EFS` per Amazon Elastic File System
- `FSx` per Amazon FSx
- `Neptune` per Amazon Neptune
- `Redshift` per Amazon Redshift
- `RDS` per Amazon Relational Database Service
- `SAP HANA on Amazon EC2` per database SAP HANA
- `Storage Gateway`per AWS Storage Gateway
- `S3` per Amazon S3
- `Timestream` per Amazon Timestream
- `VirtualMachine` per macchine virtuali

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeInBytes": number,
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CalculatedLifecycle": {
            "DeleteAt": number,
            "MoveToColdStorageAt": number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IamRoleArn": "string",
         "IsEncrypted": boolean,
```

```
            "IsParent": boolean,
            "LastRestoreTime": number,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "ParentRecoveryPointArn": "string",
            "RecoveryPointArn": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string",
            "SourceBackupVaultArn": "string",
            "Status": "string",
            "StatusMessage": "string",
            "VaultType": "string"
         }
      ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

RecoveryPoints

Un array di oggetti contenenti informazioni dettagliate sui punti di ripristino salvati in un vault di backup.

Tipo: matrice di oggetti RecoveryPointByBackupVault

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRecoveryPointsByLegalHold

Servizio: AWS Backup

Questa azione restituisce gli ARN (Amazon Resource Name) dei punti di ripristino del blocco a fini legati specificato.

Sintassi della richiesta

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

legalHoldId

L'ID della custodia legale.

Campo obbligatorio: sì

MaxResults

Il numero massimo di elementi dell'elenco di risorse da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite.

Tipo: stringa

RecoveryPoints

I punti di ripristino.

Tipo: matrice di oggetti RecoveryPointMember

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRecoveryPointsByResource

Servizio: AWS Backup

Le informazioni sui punti di ripristino del tipo specificato da una risorsa Amazon Resource Name (ARN).

> **Note**
>
> Per Amazon EFS e Amazon EC2, questa azione elenca solo i punti di ripristino creati da AWS Backup.

Sintassi della richiesta

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

ManagedByAWSBackupOnly

Questo attributo filtra i punti di ripristino in base alla proprietà.

Se è impostato su`TRUE`, la risposta conterrà i punti di ripristino associati alle risorse selezionate gestite da AWS Backup.

Se è impostato su`FALSE`, la risposta conterrà tutti i punti di ripristino associati alla risorsa selezionata.

Tipo: Booleano

MaxResults

Il numero massimo di elementi da restituire.

> **Note**
>
> Amazon RDS richiede un valore pari almeno 20.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

resourceArn

Un ARN che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeBytes": number,
         "BackupVaultName": "string",
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IsParent": boolean,
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceName": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

RecoveryPoints

Un array di oggetti contenente informazioni dettagliate sui punti di ripristino del tipo di risorsa specificato.

> **Note**
>
> Restituiscono solo i punti di ripristino Amazon EFS e Amazon EC2. BackupVaultName

Tipo: matrice di oggetti RecoveryPointByResource

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListReportJobs

Servizio: AWS Backup

Restituisce i dettagli relativi ai processi di report.

Sintassi della richiesta

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

ByCreationAfter

Restituisce solo i processi di report che sono stati creati dopo la data e l'ora specificati nel formato Unix e nell'ora UTC (Coordinated Universal Time). Ad esempio, il valore 1516925490 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.

ByCreationBefore

Restituisce solo i processi di report che sono stati creati prima della data e ora specificati nel formato Unix e nell'ora UTC (Coordinated Universal Time). Ad esempio, il valore 1516925490 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.

ByReportPlanName

Restituisce solo i processi di report con il nome del piano di report specificato.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

Restituisce solo i processi di report che si trovano nello stato specificato. Gli stati sono:

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

Il numero di risultati desiderato è compreso tra 1 e 1.000. Facoltativo. Se non specificato, la query restituirà 1 MB di dati.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

Un identificatore restituito dalla precedente chiamata a questa operazione, che può essere utilizzato per restituire il successivo set di elementi nell'elenco.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportJobs": [
      {
         "CompletionTime": number,
         "CreationTime": number,
         "ReportDestination": {
            "S3BucketName": "string",
            "S3Keys": [ "string" ]
         },
         "ReportJobId": "string",
         "ReportPlanArn": "string",
         "ReportTemplate": "string",
         "Status": "string",
         "StatusMessage": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

Un identificatore restituito dalla precedente chiamata a questa operazione, che può essere utilizzato per restituire il successivo set di elementi nell'elenco.

- Tipo: stringa

ReportJobs

I dettagli relativi ai processi di report in formato JSON.

Tipo: matrice di oggetti ReportJob

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListReportPlans

Servizio: AWS Backup

Restituisce un elenco dei piani di report. Per informazioni dettagliate su un singolo piano di report, utilizzare `DescribeReportPlan`.

Sintassi della richiesta

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

Il numero di risultati desiderato è compreso tra 1 e 1.000. Facoltativo. Se non specificato, la query restituirà 1 MB di dati.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

Un identificatore restituito dalla precedente chiamata a questa operazione, che può essere utilizzato per restituire il successivo set di elementi nell'elenco.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportPlans": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
```

```
         "LastAttemptedExecutionTime": number,
         "LastSuccessfulExecutionTime": number,
         "ReportDeliveryChannel": {
            "Formats": [ "string" ],
            "S3BucketName": "string",
            "S3KeyPrefix": "string"
         },
         "ReportPlanArn": "string",
         "ReportPlanDescription": "string",
         "ReportPlanName": "string",
         "ReportSetting": {
            "Accounts": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "OrganizationUnits": [ "string" ],
            "Regions": [ "string" ],
            "ReportTemplate": "string"
         }
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

Un identificatore restituito dalla precedente chiamata a questa operazione, che può essere utilizzato per restituire il successivo set di elementi nell'elenco.

Tipo: stringa

ReportPlans

I piani del rapporto con informazioni dettagliate per ogni piano. Queste informazioni includono il nome della risorsa Amazon (ARN), il nome del piano di report, la descrizione, le impostazioni, il canale di distribuzione, lo stato di implementazione, l'ora di creazione e le ore ultimo tentativo ed esecuzione completata.

Tipo: matrice di oggetti ReportPlan

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRestoreJobs

Servizio: AWS Backup

Restituisce un elenco di processi AWS Backup avviati per ripristinare una risorsa salvata, inclusi i dettagli sul processo di ripristino.

Sintassi della richiesta

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

ByAccountId

L'ID account da cui elencare i processi. Restituisce solo i processi di ripristino associati all'ID account specificato.

Modello: `^[0-9]{12}$`

ByCompleteAfter

Restituisce solo i processi di copia completati dopo una data espressa nel formato Unix e nell'ora UTC (Coordinated Universal Time).

ByCompleteBefore

Restituisce solo i processi di copia completati prima di una data espressa nel formato Unix e nell'ora UTC (Coordinated Universal Time).

ByCreatedAfter

Restituisce solo i processi di ripristino creati dopo la data specificata.

ByCreatedBefore

Restituisce solo i processi di ripristino creati prima della data specificata.

ByResourceType

Includi questo parametro per restituire solo i processi di ripristino per le risorse specificate:

- `Aurora` per Amazon Aurora

- `CloudFormation`per AWS CloudFormation
- `DocumentDB` per Amazon DocumentDB (compatibile con MongoDB)
- `DynamoDB` per Amazon DynamoDB
- `EBS` per Amazon Elastic Block Store
- `EC2` per Amazon Elastic Compute Cloud
- `EFS` per Amazon Elastic File System
- `FSx` per Amazon FSx
- `Neptune` per Amazon Neptune
- `Redshift` per Amazon Redshift
- `RDS` per Amazon Relational Database Service
- `SAP HANA on Amazon EC2` per database SAP HANA
- `Storage Gateway`per AWS Storage Gateway
- `S3` per Amazon S3
- `Timestream` per Amazon Timestream
- `VirtualMachine` per macchine virtuali

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByRestoreTestingPlanArn

Restituisce solo i processi di test di ripristino che corrispondono al nome della risorsa Amazon (ARN) specificata.

ByStatus

Restituisce solo i processi di ripristino associati allo stato processo specificato.

Valori validi: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

RestoreJobs

Un array di oggetti contenenti informazioni dettagliate sui processi per ripristinare le risorse salvate.

Tipo: matrice di oggetti RestoreJobsListMember

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRestoreJobsByProtectedResource

Servizio: AWS Backup

Restituisce i processi di ripristino che contengono la risorsa protetta specificata.

È necessario includere `ResourceArn`. Facoltativamente, puoi includere `NextToken`, `ByStatus`, `MaxResults`, `ByRecoveryPointCreationDateAfter` e `ByRecoveryPointCreationDateBefore`.

Sintassi della richiesta

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

ByRecoveryPointCreationDateAfter

Restituisce solo i processi di ripristino dei punti di ripristino creati dopo la data specificata.

ByRecoveryPointCreationDateBefore

Restituisce solo i processi di ripristino dei punti di ripristino creati prima della data specificata.

ByStatus

Restituisce solo i processi di ripristino associati allo stato processo specificato.

Valori validi: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

resourceArn

Restituisce solo i processi di ripristino che corrispondono al nome della risorsa Amazon (ARN) specificata.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
```

```
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

RestoreJobs

Un array di oggetti contenenti informazioni dettagliate sui processi per ripristinare le risorse salvate.

Tipo: matrice di oggetti RestoreJobsListMember

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRestoreJobSummaries

Servizio: AWS Backup

Questa richiesta ottiene un riepilogo dei processi di ripristino creati o eseguiti negli ultimi 30 giorni. È possibile includere i parametri AccountID, State,, ResourceType AggregationPeriod MaxResults, o NextToken per filtrare i risultati.

Questa richiesta restituisce un riepilogo che contiene Regione, Account RestourceType, Stato MessageCategory, StartTime, EndTime, e Numero di lavori inclusi.

Sintassi della richiesta

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

AccountId

Restituisce il numero di processi per l'account specificato.

Se la richiesta viene inviata da un account membro o da un account che non fa parte di AWS Organizations, verranno restituiti i lavori all'interno dell'account del richiedente.

Gli account root, amministratore e amministratore delegato possono utilizzare il valore ANY per restituire il numero di processi di ogni account dell'organizzazione.

AGGREGATE_ALL aggrega i numeri dei processi di tutti gli account dell'organizzazione autenticata, quindi restituisce la somma.

Modello: `^[0-9]{12}$`

AggregationPeriod

Periodo per i risultati restituiti.

- ONE_DAY- Il numero di lavori giornalieri per i 14 giorni precedenti.
- SEVEN_DAYS- Il numero aggregato dei lavori per i 7 giorni precedenti.
- FOURTEEN_DAYS- Il numero aggregato dei lavori per i 14 giorni precedenti.

Valori validi: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Questo parametro imposta il numero massimo di elementi da restituire.

Il valore è un numero intero. L'intervallo di valori validi è compreso tra 1 e 500.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

ResourceType

Restituisce il numero di processi per il tipo di risorsa specificato. Usa la richiesta `GetSupportedResourceTypes` per ottenere le stringhe per i tipi di risorsa supportati.

Il valore ANY restituisce il conteggio di tutti i tipi di risorse.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutti i tipi di risorsa e restituisce la somma.

Il tipo di AWS risorsa di cui eseguire il backup; ad esempio, un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS).

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Questo parametro restituisce il numero di processi con lo stato specificato.

Il valore ANY restituisce il conteggio di tutti gli stati.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutti gli stati e restituisce la somma.

Valori validi: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "NextToken": "string",
   "RestoreJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AggregationPeriod

Il periodo in cui vengono restituiti i risultati.

- `ONE_DAY`- Il numero di lavori giornalieri per i 14 giorni precedenti.
- `SEVEN_DAYS`- Il numero aggregato dei lavori per i 7 giorni precedenti.
- `FOURTEEN_DAYS`- Il numero aggregato dei lavori per i 14 giorni precedenti.

Tipo: stringa

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

RestoreJobSummaries

Questo risultato contiene un riepilogo che contiene la regione, l'account, lo stato ResourceType MessageCategory, StartTime EndTime, e il numero di lavori inclusi.

Tipo: matrice di oggetti RestoreJobSummary

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRestoreTestingPlans

Servizio: AWS Backup

Restituisce un elenco di piani di test di ripristino.

Sintassi della richiesta

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreTestingPlans": [
      {
         "CreationTime": number,
         "LastExecutionTime": number,
         "LastUpdateTime": number,
         "RestoreTestingPlanArn": "string",
```

```
            "RestoreTestingPlanName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowHours": number
        }
    ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

RestoreTestingPlans

È l'elenco dei piani di test di ripristino restituito.

Tipo: matrice di oggetti RestoreTestingPlanForList

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRestoreTestingSelections

Servizio: AWS Backup

Restituisce un elenco di selezioni del test di ripristino. Può essere filtrato per `MaxResults` e `RestoreTestingPlanName`.

Sintassi della richiesta

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

RestoreTestingPlanName

Restituisce le selezioni del test di ripristino in base al nome del piano di test di ripristino specificato.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

RestoreTestingSelections

Le selezioni del test di ripristino restituite associate al piano di test di ripristino.

Tipo: matrice di oggetti RestoreTestingSelectionForList

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListTags

Servizio: AWS Backup

Restituisce i tag assegnati alla risorsa, ad esempio un punto di ripristino di destinazione, un piano di backup o un archivio di backup.

`ListTags` funziona solo per i tipi di risorse che supportano la gestione AWS Backup completa dei backup. Questi tipi di risorse sono elencati nella tabella Disponibilità delle funzionalità per risorsa.

Sintassi della richiesta

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

MaxResults

Il numero massimo di elementi da restituire.

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

resourceArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa. Destinazioni valide per `ListTags` sono punti di ripristino, piani di backup e vault di backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di elementi restituiti. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di elementi, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

Tags

Informazioni sui tag.

Tipo: mappatura stringa a stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutBackupVaultAccessPolicy

Servizio: AWS Backup

Imposta una policy basate sulle risorse, che viene utilizzata per gestire le autorizzazioni di accesso al vault di backup di destinazione. Richiede un nome del vault di backup e un documento sulla policy di accesso in formato JSON.

Sintassi della richiesta

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Policy

Il documento relativo alla policy di accesso del vault di backup in formato JSON.

Tipo: stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutBackupVaultLockConfiguration

Servizio: AWS Backup

Applica AWS Backup Vault Lock a un archivio di backup, impedendo i tentativi di eliminare qualsiasi punto di ripristino archiviato o creato in un archivio di backup. Vault Lock impedisce inoltre i tentativi di aggiornare la policy del ciclo di vita che controlla il periodo di conservazione di qualsiasi punto di ripristino attualmente archiviato in un vault di backup. Se specificato, Vault Lock impone un periodo di conservazione minimo e massimo per i processi di backup e copia futuri destinati a un vault di backup.

> **Note**
>
> AWS Backup Vault Lock è stato valutato da Cohasset Associates per l'utilizzo in ambienti soggetti alle normative SEC 17a-4, CFTC e FINRA. Per ulteriori informazioni su come AWS Backup Vault Lock si rapporta a queste normative, consulta la valutazione della conformità di Cohasset Associates.

Per ulteriori informazioni, consulta Vault Lock di AWS Backup.

Sintassi della richiesta

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

La configurazione AWS Backup Vault Lock che specifica il nome dell'archivio di backup che protegge.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

ChangeableForDays

La configurazione AWS Backup Vault Lock che specifica il numero di giorni prima della data di blocco. Ad esempio, impostare `ChangeableForDays` su 30 del 1 gennaio 2022 alle 20:00 UTC imposterà la data di blocco su 31 gennaio 2022 alle 20:00 UTC.

AWS Backup impone un periodo di riflessione di 72 ore prima che Vault Lock abbia effetto e diventi immutabile. Pertanto, devi impostare `ChangeableForDays` su 3 o su un valore maggiore.

Prima della data di blocco, puoi eliminare Vault Lock dal vault utilizzando `DeleteBackupVaultLockConfiguration` o modificare la configurazione di Vault Lock utilizzando `PutBackupVaultLockConfiguration`. A partire dalla data di blocco, Vault Lock diventa immutabile e non può essere modificato o eliminato.

Se questo parametro non è specificato, puoi eliminare Vault Lock dal vault utilizzando `DeleteBackupVaultLockConfiguration` o modificare la configurazione di Vault Lock utilizzando `PutBackupVaultLockConfiguration` in qualsiasi momento.

Tipo: long

Campo obbligatorio: no

MaxRetentionDays

La configurazione AWS Backup Vault Lock che specifica il periodo di conservazione massimo durante il quale il vault conserva i suoi punti di ripristino. Questa impostazione può essere utile se, ad esempio, le policy dell'organizzazione richiedono la distruzione di determinati dati dopo averli conservati per quattro anni (1460 giorni).

Se questo parametro non è incluso, Vault Lock non applica un periodo di conservazione massimo sui punti di ripristino nel vault. Se questo parametro è incluso senza un valore, Vault Lock non applica un periodo di conservazione massimo.

Se questo parametro è specificato, qualsiasi processo di backup o copia nel vault deve avere una policy del ciclo di vita con un periodo di conservazione uguale o inferiore al periodo di

conservazione massimo. Se il periodo di conservazione del processo è più lungo del periodo di conservazione massimo, allora il processo di backup o di copia del vault non riesce ed è necessario modificare le impostazioni del ciclo di vita o utilizzare un vault diverso. Il periodo di conservazione massimo più lungo che è possibile specificare è di 36500 giorni (circa 100 anni). I punti di ripristino già salvati nel vault prima dell'applicazione del Vault Lock di non sono interessati.

Tipo: long

Campo obbligatorio: no

MinRetentionDays

La configurazione AWS Backup Vault Lock che specifica il periodo di conservazione minimo durante il quale il vault conserva i propri punti di ripristino. Questa impostazione può essere utile se, ad esempio, le policy dell'organizzazione richiedono la conservazione di determinati dati per almeno sette anni (2555 giorni).

Questo parametro è obbligatorio quando viene creato un blocco del vault AWS CloudFormation; in caso contrario, questo parametro è facoltativo. Se questo parametro non è specificato, Vault Lock non applica un periodo di conservazione minimo.

Se questo parametro è specificato, qualsiasi processo di backup o copia nel vault deve avere una policy del ciclo di vita con un periodo di conservazione uguale o superiore al periodo di conservazione minimo. Se il periodo di conservazione del processo è più breve del periodo di conservazione minimo, allora il processo di backup o di copia del vault non riesce ed è necessario modificare le impostazioni del ciclo di vita o utilizzare un vault diverso. Il periodo di conservazione minimo più breve che è possibile specificare è di 1 giorno. I punti di ripristino già salvati nel vault prima dell'applicazione del Vault Lock di non sono interessati.

Tipo: long

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++

- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutBackupVaultNotifications

Servizio: AWS Backup

Attiva le notifiche su un vault di backup per l'argomento e gli eventi specificati.

Sintassi della richiesta

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupVaultEvents

Un array di eventi che indica lo stato dei processi per il backup delle per il vault di backup.

Per casi d'uso comuni ed esempi di codice, consulta Usare Amazon SNS per tracciare AWS Backup gli eventi.

Sono supportati i seguenti eventi:

- `BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED`

- `COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
- `RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED` | `RECOVERY_POINT_MODIFIED`
- `S3_BACKUP_OBJECT_FAILED` | `S3_RESTORE_OBJECT_FAILED`

> **Note**
>
> L'elenco seguente include sia gli eventi supportati che gli eventi obsoleti che non sono più in uso (a titolo di riferimento). Gli eventi obsoleti non restituiscono stati o notifiche. Consulta l'elenco precedente per gli eventi supportati.

Tipo: matrice di stringhe

Valori validi: `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED`

Campo obbligatorio: sì

SNSTopicArn

Il nome della risorsa Amazon (ARN) che specifica l'argomento per gli eventi di un vault di backup, ad esempio `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Tipo: stringa

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python

- AWS SDK per Ruby V3

PutRestoreValidationResult

Servizio: AWS Backup

Questa richiesta consente di inviare i risultati della convalida del test di ripristino indipendente a esecuzione automatica. `RestoreJobId` e `ValidationStatus` sono obbligatori. Facoltativamente, puoi specificare `ValidationStatusMessage`.

Sintassi della richiesta

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

restoreJobId

Si tratta di un identificatore univoco di un processo di ripristino all'interno AWS Backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

ValidationStatus

Lo stato della convalida del ripristino.

Tipo: stringa

Valori validi: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Campo obbligatorio: sì

ValidationStatusMessage

È una stringa di messaggio opzionale che puoi inserire per descrivere lo stato della convalida del test di ripristino.

- Tipo: stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 204
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartBackupJob

Servizio: AWS Backup

Avvia un processo di backup on demand per la risorsa specificata.

Sintassi della richiesta

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
   "BackupOptions": {
      "string" : "string"
   },
   "BackupVaultName": "string",
   "CompleteWindowMinutes": number,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointTags": {
      "string" : "string"
   },
   "ResourceArn": "string",
   "StartWindowMinutes": number
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupOptions

L'opzione di backup per una risorsa selezionata. Questa opzione è disponibile solo per i processi di backup di Windows Volume Shadow Copy Service (VSS).

Valori validi: imposta su `"WindowsVSS":"enabled"` per abilitare l'opzione di backup `WindowsVSS` e creare un backup di Windows VSS. Imposta su `"WindowsVSS""disabled"` per creare un backup regolare. Per impostazione predefinita, l'opzione `WindowsVSS` non è abilitata.

Tipo: mappatura stringa a stringa

Modello di chiave:`^[a-zA-Z0-9\-\_\.]{1,50}$`

Modello di valore: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

CompleteWindowMinutes

Un valore in minuti durante il quale un backup avviato correttamente deve essere completato. In caso contrario, il processo verrà annullato da AWS Backup . Questo valore è facoltativo. Questo valore inizia il conto alla rovescia a partire dalla pianificazione del backup. Non aggiunge ulteriore tempo per `StartWindowMinutes` o se il backup è iniziato più tardi del previsto.

Analogamente a `StartWindowMinutes`, questo parametro ha un valore massimo di 100 anni (52.560.000 minuti).

Tipo: long

Campo obbligatorio: no

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione; ad esempio, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: stringa

Campo obbligatorio: sì

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `StartBackupJob`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

- Tipo: stringa

Campo obbligatorio: no

Lifecycle

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup eseguirà automaticamente la transizione e la scadenza dei backup in base al ciclo di vita definito.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Questo parametro ha un valore massimo di 100 anni (36.5000 giorni).

Tipo: oggetto Lifecycle

Campo obbligatorio: no

RecoveryPointTags

I tag da assegnare alle risorse.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

ResourceArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

Tipo: stringa

Campo obbligatorio: sì

StartWindowMinutes

Un valore in minuti dopo la pianificazione di un backup prima che un processo venga annullato se non viene avviato correttamente. Questo valore è facoltativo e l'impostazione predefinita è 8 ore. Se questo valore è incluso, devono essere necessari almeno 60 minuti per evitare errori.

Il valore massimo di questo parametro è 100 anni (52.560.000 minuti).

Durante la finestra di avvio, il processo di backup rimane in stato `CREATED` finché non viene avviato correttamente o fino alla scadenza della finestra di avvio. Se all'interno della finestra di avvio AWS Backup viene visualizzato un errore che consente di riprovare il lavoro, AWS Backup riproverà automaticamente a iniziare il processo almeno ogni 10 minuti fino all'avvio corretto del backup (lo stato del lavoro cambia in`RUNNING`) o fino a quando lo stato del lavoro non cambia a `EXPIRED` (cosa che dovrebbe verificarsi al termine della finestra di avvio).

Tipo: long

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupJobId

Identifica in modo univoco una richiesta di backup AWS Backup di una risorsa.

- Tipo: stringa

CreationDate

La data e l'ora di creazione di un processo di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

IsParent

Questo è un valore booleano restituito che indica che si tratta di un processo di backup (composito) padre.

Tipo: Booleano

RecoveryPointArn

Nota: questo campo viene restituito solo per le risorse Amazon EFS e Advanced DynamoDB.

Un ARN che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartCopyJob

Servizio: AWS Backup

Avvia un processo per creare una copia univoca della risorsa specificata.

Non supporta backup continui.

Sintassi della richiesta

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
   "DestinationBackupVaultArn": "string",
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string",
   "SourceBackupVaultName": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

DestinationBackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup di destinazione in cui copiare; ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: stringa

Campo obbligatorio: sì

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione; ad esempio `arn:aws:iam::123456789012:role/S3Access`.

Tipo: stringa

Campo obbligatorio: sì

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `StartCopyJob`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

-Tipo: stringa

Campo obbligatorio: no

Lifecycle

Speciifica il periodo di tempo, in giorni, prima che un punto di ripristino passi alla conservazione a freddo o venga eliminato.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, sulla console, l'impostazione di conservazione deve essere superiore di 90 giorni rispetto all'impostazione del passaggio al freddo dopo giorni. L'impostazione relativa alla transizione a freddo dopo giorni non può essere modificata dopo che un backup è passato a freddo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Per rimuovere il ciclo di vita e i periodi di conservazione esistenti e mantenere i punti di ripristino a tempo indeterminato, specifica -1 per e. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Tipo: oggetto Lifecycle

Campo obbligatorio: no

RecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino da utilizzare per il processo di copia; ad esempio arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Tipo: stringa

Campo obbligatorio: sì

SourceBackupVaultName

Il nome di un container di origine logico in cui vengono archiviati i backup. Gli archivi di Backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la AWS regione in cui vengono creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CopyJobId

Identifica in modo univoco un processo di copia.

- Tipo: stringa

CreationDate

La data e l'ora di creazione di un processo di copia, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

IsParent

Questo è un valore booleano restituito che indica che si tratta di un processo di copia (composito) padre.

Tipo: Booleano

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartReportJob

Servizio: AWS Backup

Avvia un processo di report on demand per il piano di report specificato.

Sintassi della richiesta

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

reportPlanName

Il nome univoco di un piano di report.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `StartReportJobInput`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

- Tipo: stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ReportJobId

L'identificatore del processo di report. Stringa con codifica UTF-8 Unicode univoca generata casualmente con lunghezza massima di 1.024 byte. L'ID processo report non può essere modificato.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartRestoreJob

Servizio: AWS Backup

Recupera la risorsa salvata identificata da un nome della risorsa Amazon (ARN).

Sintassi della richiesta

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

CopySourceTagsToRestoredResource

Si tratta di un parametro facoltativo. Se questo è uguale a `True`, i tag inclusi nel backup verranno copiati nella risorsa ripristinata.

Questo può essere applicato solo ai backup creati tramite AWS Backup.

Tipo: Booleano

Campo obbligatorio: no

IamRoleArn

L'Amazon Resource Name (ARN) del ruolo IAM AWS Backup utilizzato per creare la risorsa di destinazione; ad esempio:. `arn:aws:iam::123456789012:role/S3Access`

- Tipo: stringa

Campo obbligatorio: no

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `StartRestoreJob`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

- Tipo: stringa

Campo obbligatorio: no

Metadata

Un set di coppie chiave-valore di metadati.

Puoi ottenere i metadati di configurazione relativi a una risorsa al momento del backup chiamando `GetRecoveryPointRestoreMetadata`. Tuttavia, per ripristinare una risorsa potrebbero essere necessari altri valori oltre a quelli forniti da `GetRecoveryPointRestoreMetadata`. Ad esempio, potrebbe essere necessario fornire un nuovo nome di risorsa se l'originale esiste già.

Per ulteriori informazioni sui metadati per ogni risorsa, consulta quanto segue:

- Metadati per Amazon Aurora
- Metadati per Amazon DocumentDB
- Metadati per AWS CloudFormation
- Metadati per Amazon DynamoDB
- Metadati per Amazon EBS
- Metadati per Amazon EC2
- Metadati per Amazon EFS
- Metadati per Amazon FSx
- Metadati per Amazon Neptune
- Metadati per Amazon RDS
- Metadati per Amazon Redshift
- Metadati per AWS Storage Gateway
- Metadati per Amazon S3
- Metadati per Amazon Timestream

- Metadati per macchine virtuali

Tipo: mappatura stringa a stringa

Campo obbligatorio: sì

RecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: stringa

Campo obbligatorio: sì

ResourceType

Avvia un processo per ripristinare un punto di ripristino per una delle seguenti risorse:

- `Aurora`- Amazon Aurora
- `DocumentDB`- Amazon DocumentDB
- `CloudFormation` - AWS CloudFormation
- `DynamoDB`- Amazon DynamoDB
- `EBS`- Amazon Elastic Block Store
- `EC2`- Amazon Elastic Compute Cloud
- `EFS`- Amazon Elastic File System
- `FSx`- Amazon FSx
- `Neptune`- Amazon Neptune
- `RDS`- Amazon Relational Database Service
- `Redshift`- Amazon Redshift
- `Storage Gateway` - AWS Storage Gateway
- `S3`- Servizio Amazon Simple Storage
- `Timestream`- Amazon Timestream
- `VirtualMachine`- Macchine virtuali

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

RestoreJobId

Identifica in modo univoco il processo che ripristina un punto di ripristino.

Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StopBackupJob

Servizio: AWS Backup

Tenta di annullare un processo per creare un backup univoco di una risorsa.

Questa azione non è supportata per i seguenti servizi: Amazon FSx per Windows File Server, Amazon FSx for Lustre, Amazon FSx per ONTAP, Amazon NetApp FSx per OpenZFS, Amazon DocumentDB (con compatibilità MongoDB), Amazon RDS, Amazon Aurora e Amazon Neptune Ptune.

Sintassi della richiesta

```
POST /backup-jobs/backupJobId HTTP/1.1
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupJobId

Identifica in modo univoco una richiesta di backup di una risorsa. AWS Backup

Campo obbligatorio: sì

Corpo della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

TagResource

Servizio: AWS Backup

Assegna un set di coppie chiave-valore a un punto di ripristino, un piano di backup o un vault di backup identificato da un nome della risorsa Amazon (ARN).

Questa API è supportata per i punti di ripristino per tipi di risorse tra cui Aurora, Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune e Amazon RDS.

Sintassi della richiesta

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

resourceArn

Un ARN che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo della risorsa con tag.

Gli ARN che non includono sono incompatibili con il tagging. `backup` `TagResourcee` `UntagResource` con ARN non validi si verificherà un errore. I contenuti ARN accettabili possono includere. `arn:aws:backup:us-east` Potrebbe apparire un contenuto ARN non valido. `arn:aws:ec2:us-east`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Tags

Coppie chiave-valore utilizzate per semplificare l'organizzazione delle risorse. Puoi assegnare i tuoi metadati alle risorse create. Per chiarezza, questa è la struttura per assegnare i tag: `[{"Key":"string","Value":"string"}]`.

Tipo: mappatura stringa a stringa

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UntagResource

Servizio: AWS Backup

Rimuove un set di coppie chiave-valore da un punto di ripristino, un piano di backup o un vault di backup identificato da un nome della risorsa Amazon (ARN)

Questa API non è supportata per i punti di ripristino per tipi di risorse tra cui Aurora, Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune e Amazon RDS.

Sintassi della richiesta

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

resourceArn

Un ARN che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo della risorsa con tag.

Gli ARN che non includono sono incompatibili con il tagging. `backup` `TagResource`e `UntagResource` con ARN non validi si verificherà un errore. I contenuti ARN accettabili possono includere. `arn:aws:backup:us-east` Potrebbe apparire un contenuto ARN non valido. `arn:aws:ec2:us-east`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

TagKeyList

Le chiavi per identificare quali tag chiave-valore rimuovere da una risorsa.

Tipo: matrice di stringhe

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateBackupPlan

Servizio: AWS Backup

Aggiorna il piano di backup specificato. La nuova versione è identificata in modo univoco dal relativo ID.

Sintassi della richiesta

```
POST /backup/plans/backupPlanId HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
```

```
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupPlanId

L'ID del piano di backup.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

BackupPlan

Il corpo di un piano di backup. Include un `BackupPlanName` e uno o più set di `Rules`.

Tipo: oggetto BackupPlanInput

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
```

```
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AdvancedBackupSettings

Contiene un elenco di `BackupOptions` per ogni tipo di risorsa.

Tipo: matrice di oggetti AdvancedBackupSetting

BackupPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

-Tipo: stringa

BackupPlanId

Identifica in modo univoco un piano di backup.

-Tipo: stringa

CreationDate

La data e l'ora di creazione di un piano di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

VersionId

Stringhe con codifica UTF-8 Unicode univoche generate casualmente con lunghezza massimo di 1.024 byte. Gli Id della versione non possono essere modificati.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateFramework

Servizio: AWS Backup

Aggiorna il framework specificato.

Sintassi della richiesta

```
PUT /audit/frameworks/frameworkName HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "IdempotencyToken": "string"
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

frameworkName

Il nome univoco di un framework. Contiene da 1 a 256 caratteri, a partire da una lettera, ed è costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

FrameworkControls

I controlli che compongono il framework. Ogni controllo nell'elenco dispone di nome, parametri di input e ambito.

Tipo: matrice di oggetti FrameworkControl

Campo obbligatorio: no

FrameworkDescription

Descrizione facoltativa del framework, per un massimo di 1.024 caratteri.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `.*\S.*`

Campo obbligatorio: no

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `UpdateFrameworkInput`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

-Tipo: stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "CreationTime": number,
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

La data e l'ora di creazione del framework, nella rappresentazione ISO 8601. Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, 2020-07-10T15:00:00.000-08:00 rappresenta il 10 luglio 2020 alle 15:00 8 ore indietro rispetto all'UTC.

Tipo: Timestamp

FrameworkArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

FrameworkName

Il nome univoco di un framework. Contiene da 1 a 256 caratteri, a partire da una lettera, ed è costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AlreadyExistsException

La risorsa richiesta esiste già.

Codice di stato HTTP: 400

ConflictException

AWS Backup non può eseguire l'azione richiesta finché non termina l'esecuzione di un'azione precedente. Riprova più tardi.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

LimitExceededException

È stato superato un limite nella richiesta, ad esempio il numero massimo di elementi consentiti in una richiesta.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateGlobalSettings

Servizio: AWS Backup

Aggiorna se l' AWS account è abilitato al backup tra account. Restituisce un errore se l'account non è un account di gestione Organizations. Utilizza l'API `DescribeGlobalSettings` per determinare le impostazioni correnti.

Sintassi della richiesta

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

GlobalSettings

Un valore per `isCrossAccountBackupEnabled` e una regione. Esempio: `update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateRecoveryPointLifecycle

Servizio: AWS Backup

Imposta il ciclo di vita delle transizioni di un punto di ripristino.

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup esegue automaticamente le transizioni e le scadenze dei backup in base al ciclo di vita definito dall'utente.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Questa operazione non supporta backup continui.

Sintassi della richiesta

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

backupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

recoveryPointArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Lifecycle

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup esegue automaticamente le transizioni e le scadenze dei backup in base al ciclo di vita definito dall'utente.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

Tipo: oggetto Lifecycle

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
```

```
   },
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BackupVaultArn

Un ARN che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: stringa

CalculatedLifecycle

Un oggetto `CalculatedLifecycle` contenente i timestamp `DeleteAt` e `MoveToColdStorageAt`.

Tipo: oggetto CalculatedLifecycle

Lifecycle

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup esegue automaticamente le transizioni e le scadenze dei backup in base al ciclo di vita definito dall'utente.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Tipo: oggetto Lifecycle

RecoveryPointArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

-Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

InvalidRequestException

Indica che si è verificato un errore nell'input alla richiesta. Ad esempio, un parametro è del tipo errato.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateRegionSettings

Servizio: AWS Backup

Aggiorna le attuali impostazioni opt-in del servizio per la regione.

Utilizza l'API `DescribeRegionSettings` per determinare i tipi di risorse supportati.

Sintassi della richiesta

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

ResourceTypeManagementPreference

Abilita o disabilita la AWS Backup gestione completa dei backup per un tipo di risorsa. Per abilitare la AWS Backup gestione completa di DynamoDB insieme alle funzionalità di backup avanzate AWS Backup di DynamoDB, segui la procedura per abilitare il backup avanzato di DynamoDB a livello di codice.

Tipo: mappatura da stringa a matrice

Modello di chiave:`^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

ResourceTypeOptInPreference

Aggiorna l'elenco di servizi insieme alle preferenze opt-in per la regione.

Se le assegnazioni delle risorse si basano solo sui tag, vengono applicate le impostazioni opt-in del servizio. Se un tipo di risorsa viene assegnato in modo esplicito a un piano di backup, come Amazon S3, Amazon EC2 o Amazon RDS, verrà incluso nel backup anche se l'opt-in non è abilitato per quel particolare servizio. Se in un'assegnazione di risorse sono specificati un tipo di risorsa e i tag, il tipo di risorsa specificato nel piano di backup ha la priorità sulla condizione associata al tag. Le impostazioni opt-in del servizio vengono ignorate in questa situazione.

Tipo: mappatura da stringa a matrice

Modello di chiave:`^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici del linguaggio, consulta quanto segue: AWS

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateReportPlan

Servizio: AWS Backup

Aggiorna il piano di report specificato.

Sintassi della richiesta

```
PUT /audit/report-plans/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

reportPlanName

Il nome univoco del piano di report. Contiene da 1 a 256 caratteri, a partire da una lettera, ed è costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

IdempotencyToken

Una stringa scelta dal cliente che puoi usare per distinguere tra chiamate altrimenti identiche a `UpdateReportPlanInput`. Riprovare una richiesta riuscita con lo stesso token di idempotenza restituisce un messaggio di completamento senza alcuna azione eseguita.

- Tipo: stringa

Campo obbligatorio: no

ReportDeliveryChannel

Le informazioni su dove inviare i report, in particolare il nome del bucket Amazon S3, il prefisso della chiave S3 e i formati dei report.

Tipo: oggetto ReportDeliveryChannel

Campo obbligatorio: no

ReportPlanDescription

Descrizione facoltativa del piano di report, per un massimo di 1.024 caratteri.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `.*\S.*`

Campo obbligatorio: no

ReportSetting

Il modello di report per il report. I report vengono creati utilizzando un modello di report. I modelli di report sono:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Se il modello di report è `RESOURCE_COMPLIANCE_REPORT` o`CONTROL_COMPLIANCE_REPORT`, questa risorsa API descrive anche la copertura del report Regioni AWS e i framework.

Tipo: oggetto ReportSetting

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

La data e l'ora di creazione di un piano di report, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

ReportPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

ReportPlanName

Il nome univoco del piano di report.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

AWS Backup non può eseguire l'azione richiesta finché non termina l'esecuzione di un'azione precedente. Riprova più tardi.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateRestoreTestingPlan

Servizio: AWS Backup

Questa richiesta invia le modifiche al piano di test di ripristino specificato. Non è possibile aggiornare `RestoreTestingPlanName` dopo la creazione.

`RecoveryPointSelection` può contenere:

- `Algorithm`
- `ExcludeVaults`
- `IncludeVaults`
- `RecoveryPointTypes`
- `SelectionWindowDays`

Sintassi della richiesta

```
PUT /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   }
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

RestoreTestingPlanName

Il nome del piano di test di ripristino.

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

RestoreTestingPlan

Specifica il corpo di un piano di test di ripristino.

Tipo: oggetto RestoreTestingPlanForUpdate

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

L'ora in cui è stato creato il piano di test delle risorse.

Tipo: Timestamp

RestoreTestingPlanArn

Il nome della risorsa Amazon (ARN) univoco del piano di test di ripristino.

-Tipo: stringa

RestoreTestingPlanName

Il nome non può essere modificato dopo la creazione. Il nome può contenere solo caratteri alfanumerici e caratteri di sottolineatura. La lunghezza massima è 50 caratteri.

- Tipo: stringa

UpdateTime

L'ora in cui è stato completato l'aggiornamento del piano di test di ripristino.

Tipo: Timestamp

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

AWS Backup non può eseguire l'azione richiesta finché non termina l'esecuzione di un'azione precedente. Riprova più tardi.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateRestoreTestingSelection

Servizio: AWS Backup

Aggiorna la selezione del test di ripristino specificata.

Con questa richiesta è possibile aggiornare la maggior parte degli elementi tranne `RestoreTestingSelectionName`.

È possibile utilizzare sia ARN di risorse protette che condizioni, ma non entrambe.

Sintassi della richiesta

```
PUT /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "ValidationWindowHours": number
   }
}
```

Parametri della richiesta URI

La richiesta utilizza i seguenti parametri URI.

RestoreTestingPlanName

Il nome del piano di test di ripristino è necessario per aggiornare il piano di test indicato.

Campo obbligatorio: sì

RestoreTestingSelectionName

La selezione del test di ripristino richiesta (nome della selezione del test di ripristino che si desidera aggiornare).

Campo obbligatorio: sì

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

RestoreTestingSelection

Per aggiornare la selezione del test di ripristino, puoi utilizzare ARN o condizioni di risorse protette, ma non entrambi. In altre parole, se la selezione è `ProtectedResourceArns`, la richiesta di aggiornamento con il parametro `ProtectedResourceConditions` non ha esito positivo.

Tipo: oggetto RestoreTestingSelectionForUpdate

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string",
   "UpdateTime": number
```

```
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CreationTime

L'ora in cui la selezione del test delle risorse è stata aggiornata correttamente.

Tipo: Timestamp

RestoreTestingPlanArn

Stringa univoca che costituisce il nome del piano di test di ripristino.

- Tipo: stringa

RestoreTestingPlanName

Il piano di test di ripristino a cui è associata la selezione aggiornata del test di ripristino.

- Tipo: stringa

RestoreTestingSelectionName

Il nome della selezione del test di ripristino restituito.

- Tipo: stringa

UpdateTime

L'ora in cui è stato completato l'aggiornamento per la selezione del test di ripristino.

Tipo: Timestamp

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

AWS Backup non può eseguire l'azione richiesta finché non termina l'esecuzione di un'azione precedente. Riprova più tardi.

Codice di stato HTTP: 400

InvalidParameterValueException

Indica che si è verificato un errore con il valore di un parametro. Ad esempio, il valore non è compreso nell'intervallo.

Codice di stato HTTP: 400

MissingParameterValueException

Indica che manca un parametro obbligatorio.

Codice di stato HTTP: 400

ResourceNotFoundException

Una risorsa necessaria per l'azione non esiste.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

AWS Backup gateway

Le seguenti azioni sono supportate da AWS Backup gateway:

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AssociateGatewayToServer

Servizio: AWS Backup gateway

Associa un gateway di backup al server. Dopo aver completato il processo di associazione, puoi eseguire il backup e il ripristino delle macchine virtuali tramite il gateway.

Sintassi della richiesta

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway. Usa l'`ListGateways`operazione per restituire un elenco di gateway per il tuo account e Regione AWS.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

ServerArn

Il nome della risorsa Amazon (ARN) del server che ospita le macchine virtuali.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GatewayArn

Il nome della risorsa Amazon (ARN) di un gateway.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateGateway

Servizio: AWS Backup gateway

Crea un gateway di backup. Dopo aver creato un gateway, puoi associarlo a un server utilizzando l'operazione `AssociateGatewayToServer`.

Sintassi della richiesta

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ActivationKey

La chiave di attivazione del gateway creato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Modello: `^[0-9a-zA-Z\-]+$`

Campo obbligatorio: sì

GatewayDisplayName

Il nome visualizzato del gateway creato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: sì

GatewayType

Il tipo di gateway creato.

Tipo: stringa

Valori validi: `BACKUP_VM`

Campo obbligatorio: sì

Tags

Un elenco di massimo 50 tag da assegnare al gateway. Ogni tag è una coppia chiave-valore.

Tipo: matrice di oggetti Tag

Campo obbligatorio: no

Sintassi della risposta

```
{
   "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway creato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteGateway

Servizio: AWS Backup gateway

Elimina un gateway di backup.

Sintassi della richiesta

```
{
   "GatewayArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway da eliminare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway eliminato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteHypervisor

Servizio: AWS Backup gateway

Elimina un hypervisor.

Sintassi della richiesta

```
{
   "HypervisorArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor da eliminare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "HypervisorArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor eliminato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non può continuare perché le autorizzazioni non sono sufficienti.

Codice di stato HTTP: 400

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DisassociateGatewayFromServer

Servizio: AWS Backup gateway

Annulla l'associazione di un gateway di backup dal server specificato. Al termine del processo di annullamento dell'associazione, il gateway non può più accedere alle macchine virtuali sul server.

Sintassi della richiesta

```
{
   "GatewayArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway da dissociare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway dissociato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetBandwidthRateLimitSchedule

Servizio: AWS Backup gateway

Recupera la pianificazione del limite di velocità della larghezza di banda per un gateway specificato. Per impostazione predefinita, i gateway non dispongono di pianificazioni relative ai limiti di velocità della larghezza di banda, il che significa che non è in vigore alcuna limitazione della velocità della larghezza di banda. Utilizzarlo per ottenere la pianificazione del limiti di velocità della larghezza di banda di un gateway.

Sintassi della richiesta

```
{
   "GatewayArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway. Usa l'ListGatewaysoperazione per restituire un elenco di gateway per il tuo account e Regione AWS.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "BandwidthRateLimitIntervals": [
      {
```

```
            "AverageUploadRateLimitInBitsPerSec": number,
            "DaysOfWeek": [ number ],
            "EndHourOfDay": number,
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
         }
      ],
      "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

BandwidthRateLimitIntervals

Un array contenente gli intervalli di pianificazione del limite di velocità della larghezza di banda per un gateway. Quando nessun intervallo del limite di velocità della larghezza di banda è stato pianificato, l'array è vuoto.

Tipo: matrice di oggetti BandwidthRateLimitInterval

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 20 elementi.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway. Usa l'ListGatewaysoperazione per restituire un elenco di gateway per il tuo account e Regione AWS.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetGateway

Servizio: AWS Backup gateway

Fornendo l'ARN (Amazon Resource Name), questa API restituisce il gateway.

Sintassi della richiesta

```
{
   "GatewayArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
         "DayOfWeek": number,
```

```
            "HourOfDay": number,
            "MinuteOfHour": number
        },
        "NextUpdateAvailabilityTime": number,
        "VpcEndpoint": "string"
    }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Gateway

Fornendo l'ARN (Amazon Resource Name), questa API restituisce il gateway.

Tipo: oggetto GatewayDetails

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetHypervisor

Servizio: AWS Backup gateway

Questa azione richiede informazioni sull'hypervisor specificato a cui si connetterà il gateway. Un hypervisor è un hardware, software o firmware che crea e gestisce macchine virtuali e alloca risorse alle stesse.

Sintassi della richiesta

```
{
   "HypervisorArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
      "LatestMetadataSyncStatus": "string",
```

```
        "LatestMetadataSyncStatusMessage": "string",
        "LogGroupArn": "string",
        "Name": "string",
        "State": "string"
    }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Hypervisor

Dettagli relativi all'hypervisor richiesto.

Tipo: oggetto HypervisorDetails

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetHypervisorPropertyMappings

Servizio: AWS Backup gateway

Questa azione recupera le mappature delle proprietà per l'hypervisor specificato. Una mappatura delle proprietà dell'hypervisor mostra la relazione tra le proprietà dell'entità disponibili dall'hypervisor e le proprietà disponibili in. AWS

Sintassi della richiesta

```
{
   "HypervisorArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
```

```
            "VmwareTagName": "string"
        }
    ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

L'Amazon Resource Name (ARN) del ruolo IAM.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

Questa è una visualizzazione delle mappature dei tag VMware ai tag AWS .

Tipo: matrice di oggetti VmwareToAwsTagMapping

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua AWS , consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetVirtualMachine

Servizio: AWS Backup gateway

Se si fornisce l'ARN (Amazon Resource Name), questa API restituisce la macchina virtuale.

Sintassi della richiesta

```
{
   "ResourceArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ResourceArn

Il nome della risorsa Amazon (ARN) della macchina virtuale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
```

```
            {
               "VmwareCategory": "string",
               "VmwareTagDescription": "string",
               "VmwareTagName": "string"
            }
         ]
      }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

VirtualMachine

Questo oggetto contiene gli attributi di base di `VirtualMachine` contenuti dall'output di `GetVirtualMachine`

Tipo: oggetto VirtualMachineDetails

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ImportHypervisorConfiguration

Servizio: AWS Backup gateway

Esegui la connessione a un hypervisor importando la relativa configurazione.

Sintassi della richiesta

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Host

L'host del server dell'hypervisor. Può essere un indirizzo IP o un nome dominio completo (FQDN).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 128 caratteri.

Modello: `^.+$`

Campo obbligatorio: sì

KmsKeyArn

Il AWS Key Management Service per l'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Campo obbligatorio: no

Name

Il nome dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: sì

Password

La password dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[ -~]+$`

Campo obbligatorio: no

Tags

Tag della configurazione dell'hypervisor da importare.

Tipo: matrice di oggetti Tag

Campo obbligatorio: no

Username

Il nome utente dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "HypervisorArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor dissociato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non può continuare perché le autorizzazioni non sono sufficienti.

Codice di stato HTTP: 400

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListGateways

Servizio: AWS Backup gateway

Elenca i gateway di backup di proprietà di un Account AWS Regione AWS utente interno. L'elenco restituito è ordinato per Amazon Resource Name (ARN) del gateway.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Il numero massimo di gateway da elencare.

Tipo: integer

Intervallo valido: valore minimo di 1.

Campo obbligatorio: no

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `MaxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1000.

Modello: `^.+$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Gateways

Un elenco di gateway.

Tipo: matrice di oggetti Gateway

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `maxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1000.

Modello: `^.+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListHypervisors

Servizio: AWS Backup gateway

Elenca gli hypervisor.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Il numero massimo di hypervisor da elencare.

Tipo: integer

Intervallo valido: valore minimo di 1.

Campo obbligatorio: no

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `maxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1000.

Modello: `^.+$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Hypervisors

Un elenco di oggetti `Hypervisor`, ordinati in base ai nomi delle risorse Amazon (ARN).

Tipo: matrice di oggetti Hypervisor

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `maxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1000.

Modello: `^.+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListTagsForResource

Servizio: AWS Backup gateway

Elenca i tag applicati alla risorsa identificata dal relativo nome della risorsa Amazon (ARN).

Sintassi della richiesta

```
{
   "ResourceArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ResourceArn

Il nome della risorsa Amazon (ARN) dei tag della risorsa da elencare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ResourceArn

Il nome della risorsa Amazon (ARN) dei tag della risorsa elencati.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

Un elenco dei tag della risorsa.

Tipo: matrice di oggetti Tag

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListVirtualMachines

Servizio: AWS Backup gateway

Elenca le macchine virtuali.

Sintassi della richiesta

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor connesso alla macchina virtuale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: no

MaxResults

Il numero massimo di macchine virtuali da elencare.

Tipo: integer

Intervallo valido: valore minimo di 1.

Campo obbligatorio: no

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `maxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1000.

Modello: `^.+$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

L'elemento successivo che segue un elenco parziale di risorse restituite. Ad esempio, se viene effettuata una richiesta per restituire il numero `maxResults` di risorse, `NextToken` consente di restituire più elementi dell'elenco a partire dalla posizione indicata dal token successivo.

- Tipo: stringa

  Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1000.

  Modello: `^.+$`

VirtualMachines

Un elenco di oggetti `VirtualMachine`, ordinati in base ai nomi delle risorse Amazon (ARN).

Tipo: matrice di oggetti VirtualMachine

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutBandwidthRateLimitSchedule

Servizio: AWS Backup gateway

Questa operazione imposta la pianificazione del limite di velocità della larghezza di banda per un gateway specificato. Per impostazione predefinita, i gateway non dispongono di una pianificazione del limite di velocità della larghezza di banda, il che significa che non è in vigore alcuna limitazione della velocità della larghezza di banda. Utilizzarlo per avviare una pianificazione del limite di velocità della larghezza di banda di un gateway.

Sintassi della richiesta

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

BandwidthRateLimitIntervals

Un array contenente gli intervalli di pianificazione del limite di velocità della larghezza di banda per un gateway. Quando nessun intervallo del limite di velocità della larghezza di banda è stato pianificato, l'array è vuoto.

Tipo: matrice di oggetti BandwidthRateLimitInterval

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 20 elementi.

Campo obbligatorio: sì

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway. Usa l'ListGatewaysoperazione per restituire un elenco di gateway per il tuo account e Regione AWS.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway. Usa l'ListGatewaysoperazione per restituire un elenco di gateway per il tuo account e Regione AWS.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutHypervisorPropertyMappings

Servizio: AWS Backup gateway

Questa operazione imposta le mappature delle proprietà per l'hypervisor specificato. Una mappatura delle proprietà dell'hypervisor mostra la relazione tra le proprietà dell'entità disponibili dall'hypervisor e le proprietà disponibili in. AWS

Sintassi della richiesta

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

IamRoleArn

L'Amazon Resource Name (ARN) del ruolo IAM.

- Tipo: stringa

  Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

  Modello: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

  Campo obbligatorio: sì

VmwareToAwsTagMappings

Questa azione richiede le mappature dei tag VMware ai tag AWS .

Tipo: matrice di oggetti VmwareToAwsTagMapping

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "HypervisorArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

- Tipo: stringa

  Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

  Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non può continuare perché le autorizzazioni non sono sufficienti.

Codice di stato HTTP: 400

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua AWS , consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutMaintenanceStartTime

Servizio: AWS Backup gateway

Imposta l'ora di inizio della manutenzione per un gateway.

Sintassi della richiesta

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

DayOfMonth

Il giorno del mese di inizio della manutenzione su un gateway.

I valori validi sono compresi tra `Sunday` e `Saturday`.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 31.

Campo obbligatorio: no

DayOfWeek

Il giorno della settimana di inizio della manutenzione su un gateway.

Tipo: integer

Intervallo valido: valore minimo di 0. Valore massimo di 6.

Campo obbligatorio: no

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway, utilizzato per specificare l'ora di inizio della manutenzione.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

HourOfDay

L'ora del giorno di inizio della manutenzione su un gateway.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 23.

Campo obbligatorio: sì

MinuteOfHour

Il minuto dell'ora di inizio della manutenzione su un gateway.

Tipo: integer

Intervallo valido: valore minimo di 0. Valore massimo di 59.

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GatewayArn

Il nome della risorsa Amazon (ARN) di un gateway per il quale si imposta l'ora di inizio della manutenzione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartVirtualMachinesMetadataSync

Servizio: AWS Backup gateway

Questa azione invia una richiesta per sincronizzare i metadati tra le macchine virtuali specificate.

Sintassi della richiesta

```
{
   "HypervisorArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "HypervisorArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non può continuare perché le autorizzazioni non sono sufficienti.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

TagResource

Servizio: AWS Backup gateway

Il tag della risorsa.

Sintassi della richiesta

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ResourceARN

Il nome della risorsa Amazon (ARN) della risorsa a cui assegnare tag.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Tags

Un elenco di tag da assegnare alla risorsa.

Tipo: matrice di oggetti Tag

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ResourceARN": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ResourceARN

Il nome della risorsa Amazon (ARN) della risorsa a cui sono stati assegnati tag.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

TestHypervisorConfiguration

Servizio: AWS Backup gateway

Esegue il test della configurazione dell'hypervisor per verificare che il gateway di backup sia in grado di connettersi all'hypervisor e alle relative risorse.

Sintassi della richiesta

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway all'hypervisor da testare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Host

L'host del server dell'hypervisor. Può essere un indirizzo IP o un nome dominio completo (FQDN).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 128 caratteri.

Modello: `^.+$`

Campo obbligatorio: sì

Password

La password dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[ -~]+$`

Campo obbligatorio: no

Username

Il nome utente dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UntagResource

Servizio: AWS Backup gateway

Rimuovi i tag dalla risorsa.

Sintassi della richiesta

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ResourceARN

Il nome della risorsa Amazon (ARN) della risorsa da cui rimuovere i tag.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

TagKeys

L'elenco delle chiavi tag che specificano quali tag rimuovere.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ResourceARN": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ResourceARN

Il nome della risorsa Amazon (ARN) della risorsa da cui sono stati rimossi i tag.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateGatewayInformation

Servizio: AWS Backup gateway

Aggiorna il nome di un gateway. Specifica il gateway da aggiornare utilizzando il nome della risorsa Amazon (ARN) del gateway nella richiesta.

Sintassi della richiesta

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway da aggiornare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

GatewayDisplayName

Il nome visualizzato aggiornato del gateway.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway aggiornato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateGatewaySoftwareNow

Servizio: AWS Backup gateway

Aggiorna il software macchina virtuale (VM) del gateway. La richiesta attiva immediatamente l'aggiornamento software.

> **Note**
>
> Quando si effettua questa richiesta, viene immediatamente ricevuta una risposta `200 OK`. Tuttavia, il completamento dell'aggiornamento potrebbe richiedere tempo.

Sintassi della richiesta

```
{
   "GatewayArn": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway da aggiornare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

Sintassi della risposta

```
{
```

```
   "GatewayArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway aggiornato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateHypervisor

Servizio: AWS Backup gateway

Aggiorna i metadati di un hypervisor, inclusi host, nome utente e password. Specifica quale hypervisor aggiornare utilizzando il nome della risorsa Amazon (ARN) del gateway nella richiesta.

Sintassi della richiesta

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Host

L'host aggiornato dell'hypervisor. Può essere un indirizzo IP o un nome dominio completo (FQDN).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 128 caratteri.

Modello: `^.+$`

Campo obbligatorio: no

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor da aggiornare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: sì

LogGroupArn

Il nome della risorsa Amazon (ARN) del gruppo di gateway all'interno del log richiesto.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Modello: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Campo obbligatorio: no

Name

Il nome aggiornato per l'hypervisor

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

Password

La password aggiornata per l'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[ -~]+$`

Campo obbligatorio: no

Username

Il nome utente aggiornato per l'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "HypervisorArn": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor aggiornato.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non può continuare perché le autorizzazioni non sono sufficienti.

Codice di stato HTTP: 400

ConflictException

L'operazione non può continuare perché non è supportata.

Codice di stato HTTP: 400

InternalServerException

L'azione non è riuscita perché si è verificato un errore interno. Riprova più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

Non è stata trovata una risorsa necessaria per l'azione.

Codice di stato HTTP: 400

ThrottlingException

Il TPS è stato limitato per proteggere da volumi di richieste elevate, voluti o non voluti.

Codice di stato HTTP: 400

ValidationException

L'operazione non è riuscita perché si è verificato un errore di convalida.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

Tipi di dati

I seguenti tipi di dati sono supportati da AWS Backup:

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue
- LegalHold
- Lifecycle

- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

I seguenti tipi di dati sono supportati da AWS Backup gateway:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor

- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

I seguenti tipi di dati sono supportati da AWS Backup:

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope
- CopyAction
- CopyJob

- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList

- RestoreTestingSelectionForUpdate

AdvancedBackupSetting

Servizio: AWS Backup

Le opzioni di backup per ogni tipo di risorsa.

Indice

BackupOptions

Specifica l'opzione di backup per una risorsa selezionata. Questa opzione è disponibile solo per i processi di backup di Windows VSS.

Valori validi:

Imposta su `"WindowsVSS":"enabled"` per abilitare l'opzione di backup `WindowsVSS` e creare un backup di Windows VSS.

Imposta su `"WindowsVSS":"disabled"` per creare un backup regolare. Per impostazione predefinita, l'opzione `WindowsVSS` non è abilitata.

Se si specifica un'opzione non valida, si ottiene un'eccezione `InvalidParameterValueException`.

Per ulteriori informazioni sui backup di Windows VSS, consulta Creazione di backup di Windows VSS.

Tipo: mappatura stringa a stringa

Modello di chiave:`^[a-zA-Z0-9\-\_\.]{1,50}$`

Modello di valore: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

ResourceType

Specifica un oggetto contenente il tipo di risorsa e le opzioni di backup. L'unico tipo di risorsa supportato sono le istanze Amazon EC2 con Windows Volume Shadow Copy Service (VSS). Per un CloudFormation esempio, consulta il CloudFormation modello di esempio per abilitare Windows VSS nella Guida per l' AWS Backup utente.

Valori validi: `EC2`.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupJob

Servizio: AWS Backup

Contiene informazioni dettagliate su un processo di backup.

Indice

AccountId

L'ID account proprietario del processo di backup.

Tipo: stringa

Modello: `^[0-9]{12}$`

Campo obbligatorio: no

BackupJobId

Identifica in modo univoco una richiesta di backup AWS Backup di una risorsa.

-Tipo: stringa

Campo obbligatorio: no

BackupOptions

Specifica l'opzione di backup per una risorsa selezionata. Questa opzione è disponibile solo per i processi di backup di Windows Volume Shadow Copy Service (VSS).

Valori validi: imposta su `"WindowsVSS":"enabled"` per abilitare l'opzione di backup `WindowsVSS` e creare un backup di Windows VSS. Imposta su `"WindowsVSS":"disabled"` per creare un backup regolare. Se si specifica un'opzione non valida, si ottiene un'eccezione `InvalidParameterValueException`.

Tipo: mappatura stringa a stringa

Modello di chiave:`^[a-zA-Z0-9\-\_\.]{1,50}$`

Modello di valore: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

BackupSizeInBytes

La dimensione, in byte, di un backup.

Tipo: long

Campo obbligatorio: no

BackupType

Rappresenta il tipo di backup per un processo di backup.

- Tipo: stringa

Campo obbligatorio: no

BackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

Campo obbligatorio: no

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: no

BytesTransferred

La dimensione in byte trasferiti in un vault di backup nel momento in cui è stata richiesta la verifica dello stato del processo.

Tipo: long

Campo obbligatorio: no

CompletionDate

La data e l'ora di complemento di un processo di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

CreatedBy

Contiene informazioni di identificazione sulla creazione di un processo di backup, tra cui `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` e `BackupRuleId` del piano backup utilizzato per crearlo.

Tipo: oggetto RecoveryPointCreator

Campo obbligatorio: no

CreationDate

La data e l'ora di creazione di un processo di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

ExpectedCompletionDate

La data e l'ora prevista di complemento di un processo di backup delle risorse, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `ExpectedCompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione. I ruoli IAM diversi dal ruolo predefinito devono includere `AWSBackup` o `AwsBackup` nel nome del ruolo. Ad esempio, `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. I nomi ruolo senza queste stringhe non dispongono delle autorizzazioni per eseguire processi di backup.

-Tipo: stringa

Campo obbligatorio: no

InitiationDate

La data in cui è stato avviato il processo di backup.

Tipo: Timestamp

Campo obbligatorio: no

IsParent

Questo è un valore booleano che indica che si tratta di un processo di backup (composito) padre.

Tipo: Booleano

Campo obbligatorio: no

MessageCategory

Questo parametro è il numero di processi per la categoria di messaggi specificata.

Stringhe di esempio possono essere `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `INVALIDPARAMETERS`. Vedi Monitoraggio per un elenco di MessageCategory stringhe.

Il valore ANY restituisce il conteggio di tutte le categorie di messaggi.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutte le categorie di messaggi e restituisce la somma.

- Tipo: stringa

Campo obbligatorio: no

ParentJobId

Questo identifica in modo univoco una richiesta ad AWS Backup di eseguire il backup di una risorsa. Il risultato sarà l'ID processo (composito) padre.

- Tipo: stringa

Campo obbligatorio: no

PercentDone

Contiene una percentuale stimata di completamento di un processo nel momento in cui è stato richiesto lo stato del processo.

- Tipo: stringa

Campo obbligatorio: no

RecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

Campo obbligatorio: no

ResourceArn

Un ARN che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

Campo obbligatorio: no

ResourceName

Il nome non univoco della risorsa che appartiene al backup specificato.

- Tipo: stringa

Campo obbligatorio: no

ResourceType

Il tipo di AWS risorsa di cui eseguire il backup; ad esempio, un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS). Per i backup di Windows Volume Shadow Copy Service (VSS), l'unico tipo di risorsa supportato è Amazon EC2.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

StartBy

Specifica l'ora in formato Unix e UTC (Coordinated Universal Time) in cui è necessario avviare un processo di backup prima che venga annullato. Il valore viene calcolato aggiungendo la finestra

di avvio all'ora pianificata. Pertanto, se l'ora pianificata era le 18:00 e la finestra di avvia è di 2 ore, l'ora `StartBy` sarebbe le 20:00 della data specificata. Il valore di `StartBy` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

State

Lo stato corrente di un processo di backup.

-Tipo: stringa

Valori validi: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

Campo obbligatorio: no

StatusMessage

Un messaggio dettagliato che spiega lo stato del processo di backup di una risorsa.

-Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupJobSummary

Servizio: AWS Backup

È un riepilogo dei processi creati o eseguiti negli ultimi 30 giorni.

Il riepilogo restituito può contenere quanto segue: Regione, Account RestourceType, Stato MessageCategory StartTime, EndTime,, e Numero di lavori inclusi.

Indice

AccountId

L'ID dell'account proprietario dei processi del riepilogo.

Tipo: stringa

Modello: `^[0-9]{12}$`

Campo obbligatorio: no

Count

Il valore espresso come numero di processi in un riepilogo dei processi.

Tipo: integer

Campo obbligatorio: no

EndTime

Il valore in formato numerico dell'ora di fine di un processo.

Questo valore indica l'ora in formato Unix, Coordinated Universal Time (UTC) con precisione al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

MessageCategory

Questo parametro è il numero di processi per la categoria di messaggi specificata.

Stringhe di esempio sono `AccessDenied`, `Success` e `InvalidParameters`. Vedi Monitoraggio per un elenco di MessageCategory stringhe.

Il valore ANY restituisce il conteggio di tutte le categorie di messaggi.

AGGREGATE_ALL aggrega i numeri dei processi per tutte le categorie di messaggi e restituisce la somma.

- Tipo: stringa

Campo obbligatorio: no

Region

Le AWS regioni all'interno del riepilogo del lavoro.

- Tipo: stringa

Campo obbligatorio: no

ResourceType

Il valore del numero di processi per il tipo di risorsa specificato. La richiesta GetSupportedResourceTypes restituisce le stringhe per i tipi di risorsa supportati.

Tipo: stringa

Modello: ^[a-zA-Z0-9\-_\.]{1,50}$

Campo obbligatorio: no

StartTime

Il valore in formato numerico dell'ora di inizio di un processo.

Questo valore indica l'ora in formato Unix, Coordinated Universal Time (UTC) con precisione al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

State

Questo valore indica il numero di processi con lo stato specificato.

- Tipo: stringa

Valori validi: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupPlan

Servizio: AWS Backup

Contiene un nome di visualizzazione del piano di backup e una gamma di oggetti `BackupRule`, ciascuno dei quali specifica una regola di backup. Ogni regola in un piano di backup è un'attività pianificata separata e può eseguire il backup di un'altra gamma di risorse AWS .

Indice

BackupPlanName

Il nome visualizzato di un piano di backup. Deve contenere da 1 a 50 caratteri alfanumerici o i caratteri '-_.' punti (.).

Tipo: stringa

Campo obbligatorio: sì

Rules

Un array di oggetti `BackupRule`, ciascuno dei quali specifica un'operazione pianificata che viene utilizzato per eseguire il backup di una gamma di risorse.

Tipo: matrice di oggetti BackupRule

Campo obbligatorio: sì

AdvancedBackupSettings

Contiene un elenco di `BackupOptions` per ogni tipo di risorsa.

Tipo: matrice di oggetti AdvancedBackupSetting

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2

- AWS SDK per Ruby V3

BackupPlanInput

Servizio: AWS Backup

Contiene un nome di visualizzazione del piano di backup e una gamma di oggetti `BackupRule`, ciascuno dei quali specifica una regola di backup. Ogni regola in un piano di backup è un'attività pianificata separata.

Indice

BackupPlanName

Il nome visualizzato di un piano di backup. Deve contenere da 1 a 50 caratteri alfanumerici o i caratteri '-_.' punti (.).

Tipo: stringa

Campo obbligatorio: sì

Rules

Un array di oggetti `BackupRule`, ciascuno dei quali specifica un'operazione pianificata che viene utilizzato per eseguire il backup di una gamma di risorse.

Tipo: matrice di oggetti BackupRuleInput

Campo obbligatorio: sì

AdvancedBackupSettings

Specifica un elenco di `BackupOptions` per ogni tipo di risorsa. Queste impostazioni sono disponibili solo per i processi di backup di Windows Volume Shadow Copy Service (VSS).

Tipo: matrice di oggetti AdvancedBackupSetting

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2

- AWS SDK per Ruby V3

BackupPlansListMember

Servizio: AWS Backup

Contiene metadati relativi a un piano di backup.

Indice

AdvancedBackupSettings

Contiene un elenco di `BackupOptions` per un tipo di risorsa.

Tipo: matrice di oggetti AdvancedBackupSetting

Campo obbligatorio: no

BackupPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

-Tipo: stringa

Campo obbligatorio: no

BackupPlanId

Identifica in modo univoco un piano di backup.

-Tipo: stringa

Campo obbligatorio: no

BackupPlanName

Il nome visualizzato di un piano di backup salvato.

-Tipo: stringa

Campo obbligatorio: no

CreationDate

La data e l'ora di creazione di un piano di backup delle risorse, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Questo parametro è facoltativo.

Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

- Tipo: stringa

Campo obbligatorio: no

DeletionDate

La data e l'ora di eliminazione di un piano di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `DeletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

LastExecutionDate

L'ultima volta che è stato eseguito questo piano di backup. Una data e ora, in formato UNIX e nell'ora Universal Coordinated Time (UTC). Il valore di `LastExecutionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

VersionId

Stringhe con codifica UTF-8 Unicode univoche generate casualmente con lunghezza massimo di 1.024 byte. Gli ID versione non possono essere modificati.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupPlanTemplatesListMember

Servizio: AWS Backup

Un oggetto che specifica i metadati associati a un modello di piano di backup.

Indice

BackupPlanTemplateId

Identifica in modo univoco un modello di piano di backup archiviato.

- Tipo: stringa

Campo obbligatorio: no

BackupPlanTemplateName

Il nome visualizzato opzionale di un modello di piano di backup.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupRule

Servizio: AWS Backup

Specifica un'attività pianificata utilizzata per eseguire il backup di una selezione di risorse.

Indice

RuleName

Un nome visualizzato per una regola di backup. Deve contenere da 1 a 50 caratteri alfanumerici o i caratteri '-_.' punti (.).

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: sì

TargetBackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

CompletionWindowMinutes

Un valore in minuti dopo che un processo di backup viene avviato correttamente prima che sia completato o annullato da AWS Backup. Questo valore è facoltativo.

Tipo: long

Campo obbligatorio: no

CopyActions

Una matrice di oggetti `CopyAction`, che contiene i dettagli dell'operazione di copia.

Tipo: matrice di oggetti CopyAction

Campo obbligatorio: no

EnableContinuousBackup

Specifica se AWS Backup crea backup continui. Le vere cause della creazione AWS Backup di backup continui in grado di point-in-time ripristinare (PITR). False (o non specificata) causa la creazione di copie AWS Backup di backup istantanee.

Tipo: Booleano

Campo obbligatorio: no

Lifecycle

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup esegue automaticamente le transizioni e le scadenze dei backup in base al ciclo di vita definito dall'utente.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Tipo: oggetto Lifecycle

Campo obbligatorio: no

RecoveryPointTags

I tag assegnati alle risorse associate a questa regola quando vengono ripristinate dal backup.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

RuleId

Identifica in modo univoco una regola utilizzata per pianificare il backup di una selezione di risorse.

- Tipo: stringa

Campo obbligatorio: no

ScheduleExpression

Un'espressione cron in UTC che specifica quando AWS Backup avvia un processo di backup. Per ulteriori informazioni sulle espressioni AWS cron, consulta Schedule Expressions for Rules nella Amazon CloudWatch Events User Guide. . Due esempi di espressioni AWS cron sono `15 * ? * * *` (eseguire un backup ogni ora a 15 minuti dopo l'ora) e `0 12 * * ? *` (eseguire un backup ogni giorno alle 12:00 UTC). Per una tabella di esempi, fai clic sul collegamento precedente e scorri la pagina verso il basso.

- Tipo: stringa

Campo obbligatorio: no

ScheduleExpressionTimezone

Il fuso orario in cui è impostata l'espressione di pianificazione. Per impostazione predefinita, ScheduleExpressions sono in formato UTC. Puoi modificarlo impostando un fuso orario specifico.

- Tipo: stringa

Campo obbligatorio: no

StartWindowMinutes

Un valore in minuti dopo la pianificazione di un backup prima che un processo venga annullato se non viene avviato correttamente. Questo valore è facoltativo. Se questo valore è incluso, devono essere necessari almeno 60 minuti per evitare errori.

Durante la finestra di avvio, il processo di backup rimane in stato `CREATED` finché non viene avviato correttamente o fino alla scadenza della finestra di avvio. Se all'interno della finestra di avvio AWS Backup viene visualizzato un errore che consente di riprovare il processo, AWS Backup riproverà automaticamente a iniziare il processo almeno ogni 10 minuti fino all'avvio corretto del backup (lo stato del lavoro cambia in`RUNNING`) o fino a quando lo stato del lavoro non cambia a `EXPIRED` (cosa che dovrebbe verificarsi allo scadere della finestra di avvio).

Tipo: long

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupRuleInput

Servizio: AWS Backup

Specifica un'attività pianificata utilizzata per eseguire il backup di una selezione di risorse.

Indice

RuleName

Un nome visualizzato per una regola di backup. Deve contenere da 1 a 50 caratteri alfanumerici o i caratteri '-_.' punti (.).

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: sì

TargetBackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: sì

CompletionWindowMinutes

Un valore in minuti dopo che un processo di backup viene avviato correttamente prima che sia completato o annullato da AWS Backup. Questo valore è facoltativo.

Tipo: long

Campo obbligatorio: no

CopyActions

Una matrice di oggetti `CopyAction`, che contiene i dettagli dell'operazione di copia.

Tipo: matrice di oggetti CopyAction

Campo obbligatorio: no

EnableContinuousBackup

Specifica se AWS Backup crea backup continui. Le vere cause della creazione AWS Backup di backup continui in grado di point-in-time ripristinare (PITR). False (o non specificata) causa la creazione di copie AWS Backup di backup istantanee.

Tipo: Booleano

Campo obbligatorio: no

Lifecycle

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup eseguirà automaticamente la transizione e la scadenza dei backup in base al ciclo di vita definito.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione «transizione al freddo dopo giorni» non può essere modificata dopo il passaggio di un backup alla conservazione a freddo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Questo parametro ha un valore massimo di 100 anni (36.5000 giorni).

Tipo: oggetto Lifecycle

Campo obbligatorio: no

RecoveryPointTags

I tag da assegnare alle risorse.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

ScheduleExpression

Un'espressione CRON in UTC che specifica quando AWS Backup avvia un processo di backup.

- Tipo: stringa

Campo obbligatorio: no

ScheduleExpressionTimezone

Il fuso orario in cui è impostata l'espressione di pianificazione. Per impostazione predefinita, ScheduleExpressions sono in formato UTC. Puoi modificarlo impostando un fuso orario specifico.

- Tipo: stringa

Campo obbligatorio: no

StartWindowMinutes

Un valore in minuti dopo la pianificazione di un backup prima che un processo venga annullato se non viene avviato correttamente. Questo valore è facoltativo. Se questo valore è incluso, devono essere necessari almeno 60 minuti per evitare errori.

Il valore massimo di questo parametro è 100 anni (52.560.000 minuti).

Durante la finestra di avvio, il processo di backup rimane in stato `CREATED` finché non viene avviato correttamente o fino alla scadenza della finestra di avvio. Se all'interno della finestra di avvio AWS Backup viene visualizzato un errore che consente di riprovare il processo, AWS Backup riproverà automaticamente a iniziare il processo almeno ogni 10 minuti fino all'avvio corretto del backup (lo stato del lavoro cambia in`RUNNING`) o fino a quando lo stato del lavoro non cambia a `EXPIRED` (cosa che dovrebbe verificarsi al termine della finestra di avvio).

Tipo: long

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupSelection

Servizio: AWS Backup

Utilizzato per specificare un set di risorse per un piano di backup.

Ti consigliamo di specificare condizioni, tag o risorse da includere o escludere. In caso contrario, Backup tenta di selezionare tutte le risorse di storage supportate e attivate, il che potrebbe avere implicazioni indesiderate sui costi.

Per ulteriori informazioni, vedere Assegnazione di risorse a livello di codice.

Indice

IamRoleArn

L'ARN del ruolo IAM AWS Backup utilizzato per l'autenticazione durante il backup della risorsa di destinazione; ad esempio,. `arn:aws:iam::123456789012:role/S3Access`

Tipo: stringa

Campo obbligatorio: sì

SelectionName

Il nome di visualizzazione di un documento di selezione delle risorse. Deve contenere da 1 a 50 caratteri alfanumerici o i caratteri '-_.' punti (.).

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: sì

Conditions

Le condizioni che definisci per assegnare risorse ai tuoi piani di backup utilizzando i tag. Ad esempio, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }`.

`Conditions`supporta`StringEquals`, `StringLikeStringNotEquals`, e`StringNotLike`. Gli operatori di condizione fanno distinzione tra maiuscole e minuscole.

Se si specificano più condizioni, le risorse corrispondono in gran parte a tutte le condizioni (logica AND).

Tipo: oggetto Conditions

Campo obbligatorio: no

ListOfTags

Le condizioni che definisci per assegnare risorse ai tuoi piani di backup utilizzando i tag. Ad esempio, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}`.

`ListOfTags`supporta solo`StringEquals`. Gli operatori di condizione fanno distinzione tra maiuscole e minuscole.

Se si specificano più condizioni, le risorse corrispondono in gran parte a qualsiasi condizione (logica OR).

Tipo: matrice di oggetti Condition

Campo obbligatorio: no

NotResources

Gli Amazon Resource Names (ARN) delle risorse da escludere da un piano di backup. Il numero massimo di ARN è 500 senza caratteri jolly o 30 ARN con caratteri jolly.

Se devi escludere molte risorse da un piano di backup, prendi in considerazione una strategia di selezione delle risorse diversa, ad esempio assegnare solo uno o alcuni tipi di risorse o perfezionare la selezione delle risorse utilizzando i tag.

Tipo: matrice di stringhe

Campo obbligatorio: no

Resources

Gli Amazon Resource Names (ARN) delle risorse da assegnare a un piano di backup. Il numero massimo di ARN è 500 senza caratteri jolly o 30 ARN con caratteri jolly.

Se occorre assegnare molte risorse a un piano di backup, prendere in considerazione una strategia di selezione delle risorse diversa, come assegnare tutte le risorse di un tipo di risorsa o perfezionare la selezione delle risorse utilizzando i tag.

Se specifichi più ARN, le risorse corrispondono molto a qualsiasi ARN (logica OR).

Tipo: matrice di stringhe

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupSelectionsListMember

Servizio: AWS Backup

Contiene metadati relativi a un oggetto `BackupSelection`.

Indice

BackupPlanId

Identifica in modo univoco un piano di backup.

- Tipo: stringa

Campo obbligatorio: no

CreationDate

La data e l'ora di creazione di un piano di backup, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Questo parametro è facoltativo.

Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

- Tipo: stringa

Campo obbligatorio: no

IamRoleArn

Specifica il nome della risorsa Amazon (ARN) del ruolo IAM per creare il punto di ripristino di destinazione; ad esempio `arn:aws:iam::123456789012:role/S3Access`.

- Tipo: stringa

Campo obbligatorio: no

SelectionId

Identifica in modo univoco una richiesta per assegnare un set di risorse a un piano di backup.

- Tipo: stringa

Campo obbligatorio: no

SelectionName

Il nome di visualizzazione di un documento di selezione delle risorse.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

BackupVaultListMember

Servizio: AWS Backup

Contiene metadati relativi a un vault di backup.

Indice

BackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

Campo obbligatorio: no

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: no

CreationDate

La data e l'ora di creazione di un backup delle risorse, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

CreatorRequestId

Una stringa univoca che identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Questo parametro è facoltativo.

Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

- Tipo: stringa

Campo obbligatorio: no

EncryptionKeyArn

Una chiave di crittografia lato server che è possibile specificare per crittografare i backup da servizi che supportano la AWS Backup gestione completa, ad esempio. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Se specifichi una chiave, è necessario specificare il relativo ARN, non il relativo alias. Se non specifichi una chiave, AWS Backup crea una chiave KMS per impostazione predefinita.

Per sapere quali AWS Backup servizi supportano la AWS Backup gestione completa e come AWS Backup gestisce la crittografia per i backup dei servizi che non supportano ancora la gestione completa AWS Backup, vedi Encryption for backup in AWS Backup

-Tipo: stringa

Campo obbligatorio: no

LockDate

La data e l'ora in cui la configurazione di AWS Backup Vault Lock diventa immutabile, il che significa che non può essere modificata o eliminata.

Se hai applicato Vault Lock al vault senza specificare una data di blocco, puoi modificare le impostazioni di Vault Lock o eliminare completamente Vault Lock dal vault, in qualsiasi momento.

Questo valore è in formato Unix, ora Coordinated Universal Time (UTC) ed è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

Locked

Un valore booleano che indica se AWS Backup Vault Lock si applica al vault di backup selezionato. Se `true`, Vault Lock impedisce le operazioni di eliminazione e aggiornamento sui punti di ripristino nel vault selezionato.

Tipo: Booleano

Campo obbligatorio: no

MaxRetentionDays

L'impostazione AWS Backup Vault Lock che specifica il periodo di conservazione massimo durante il quale il vault conserva i propri punti di ripristino. Se questo parametro non è specificato, Vault Lock non applica un periodo di conservazione massimo sui punti di ripristino nel vault (consentendo lo storage a tempo indeterminato).

Se specificato, qualsiasi processo di backup o copia nel vault deve avere una policy del ciclo di vita con un periodo di conservazione uguale o inferiore al periodo di conservazione massimo. Se il periodo di conservazione del processo è più lungo del periodo di conservazione massimo, allora il processo di backup o di copia del vault non riesce ed è necessario modificare le impostazioni del ciclo di vita o utilizzare un vault diverso. I punti di ripristino già archiviati nel vault prima di Vault Lock non sono interessati.

Tipo: long

Campo obbligatorio: no

MinRetentionDays

L'impostazione AWS Backup Vault Lock che specifica il periodo di conservazione minimo durante il quale il vault conserva i propri punti di ripristino. Se questo parametro non è specificato, Vault Lock non applica un periodo di conservazione minimo.

Se specificato, qualsiasi processo di backup o copia nel vault deve avere una policy del ciclo di vita con un periodo di conservazione uguale o superiore al periodo di conservazione minimo. Se il periodo di conservazione del processo è più breve del periodo di conservazione minimo, allora il processo di backup o di copia del vault non riesce ed è necessario modificare le impostazioni del ciclo di vita o utilizzare un vault diverso. I punti di ripristino già archiviati nel vault prima di Vault Lock non sono interessati.

Tipo: long

Campo obbligatorio: no

NumberOfRecoveryPoints

Il numero di punti di ripristino archiviati in un vault di backup.

Tipo: long

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta AWS quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CalculatedLifecycle

Servizio: AWS Backup

Contiene i timestamp `DeleteAt` e `MoveToColdStorageAt`, utilizzati per specificare un ciclo di vita per un punto di ripristino.

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup esegue automaticamente le transizioni e le scadenze dei backup in base al ciclo di vita definito dall'utente.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Indice

DeleteAt

Un timestamp che specifica quando eliminare un punto di ripristino.

Tipo: Timestamp

Campo obbligatorio: no

MoveToColdStorageAt

Un timestamp che specifica quando eseguire la transizione di un punto di ripristino allo storage a freddo.

Tipo: Timestamp

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Condition

Servizio: AWS Backup

Contiene una matrice di triplette costituite da un tipo di condizione (ad esempio `StringEquals`), una chiave e un valore. Utilizzato per filtrare le risorse utilizzando i relativi tag e assegnarle a un piano di backup. Distinzione tra lettere maiuscole e minuscole.

Indice

ConditionKey

La chiave in una coppia chiave-valore. Ad esempio, nel `Department: Accounting`, `Department` è la chiave.

Tipo: stringa

Campo obbligatorio: sì

ConditionType

Un'operazione applicata a una coppia chiave-valore utilizzata per assegnare risorse al piano di backup. La condizione supporta solo `StringEquals`. Per opzioni di assegnazione più flessibili, tra cui `StringLike` e la possibilità di escludere risorse dal piano di backup, utilizza `Conditions` (con una "s" alla fine) per `BackupSelection`.

Tipo: stringa

Valori validi: `STRINGEQUALS`

Campo obbligatorio: sì

ConditionValue

Il valore in una coppia chiave-valore. Ad esempio, nel `Department: Accounting`, `Accounting` è il valore.

Tipo: stringa

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ConditionParameter

Servizio: AWS Backup

Include informazioni sui tag che definisci per assegnare risorse con tag per un piano di backup.

Includi il prefisso `aws:ResourceTag` nei tag. Ad esempio, `"aws:ResourceTag/TagKey1": "Value1"`.

Indice

ConditionKey

La chiave in una coppia chiave-valore. Ad esempio, nel `Department: Accounting`, `Department` è la chiave.

- Tipo: stringa

Campo obbligatorio: no

ConditionValue

Il valore in una coppia chiave-valore. Ad esempio, nel `Department: Accounting`, `Accounting` è il valore.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Conditions

Servizio: AWS Backup

Contiene informazioni sulle risorse da includere o escludere da un piano di backup utilizzando i relativi tag. Le condizioni distinguono maiuscole e minuscole.

Indice

StringEquals

Filtra i valori delle risorse con tag solo per le risorse a cui hai aggiunto tag con lo stesso valore. Detta anche “corrispondenza esatta”.

Tipo: matrice di oggetti ConditionParameter

Campo obbligatorio: no

StringLike

Filtra i valori delle risorse con tag per i valori dei tag corrispondenti con l'uso di un carattere jolly (*) in qualunque punto della stringa. Ad esempio, “prod*” o “*rod*” corrispondono al valore del tag “production”.

Tipo: matrice di oggetti ConditionParameter

Campo obbligatorio: no

StringNotEquals

Filtra i valori delle risorse con tag solo per le risorse a cui hai aggiunto tag che non hanno lo stesso valore. Detta anche “corrispondenza negata”.

Tipo: matrice di oggetti ConditionParameter

Campo obbligatorio: no

StringNotLike

Filtra i valori delle risorse con tag per i valori dei tag non corrispondenti con l'uso di un carattere jolly (*) in qualunque punto della stringa.

Tipo: matrice di oggetti ConditionParameter

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ControlInputParameter

Servizio: AWS Backup

I parametri per un controllo. Un controllo può avere zero, uno o più parametri. Un esempio di controllo con due parametri è il seguente: "la frequenza del piano di backup è almeno `daily` e il periodo di conservazione è almeno `1 year`". Il primo parametro è `daily`, mentre il secondo parametro è `1 year`.

Indice

ParameterName

Il nome di un parametro, ad esempio `BackupPlanFrequency`.

- Tipo: stringa

Campo obbligatorio: no

ParameterValue

Il valore del parametro, ad esempio `hourly`.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ControlScope

Servizio: AWS Backup

Un framework consiste in uno o più controlli. Ogni controllo ha il proprio ambito di controllo. L'ambito di controllo può includere uno o più tipi di risorse, una combinazione di chiavi e valori di un tag oppure una combinazione di un singolo tipo di risorsa e un singolo ID risorsa. Se non è specificato alcun ambito, le valutazioni per la regola vengono attivate quando la configurazione di una qualunque risorsa nel gruppo di registrazione cambia.

> **Note**
>
> Per impostare un ambito di controllo che includa tutta una risorsa particolare, lascia vuoto il campo `ControlScope` o non passarlo quando richiami `CreateFramework`.

Indice

ComplianceResourceIds

L'ID dell'unica AWS risorsa che vuoi che il tuo ambito di controllo contenga.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 100 elementi.

Campo obbligatorio: no

ComplianceResourceTypes

Descrive se l'ambito di controllo include uno o più tipi di risorsa, ad esempio `EFS` o `RDS`.

Tipo: matrice di stringhe

Campo obbligatorio: no

Tags

La coppia chiave-valore del tag applicata alle AWS risorse che desideri attivare una valutazione per una regola. È possibile fornire fino a una sola coppia chiave-valore. Il valore del tag è facoltativo, ma non può essere una stringa vuota se si crea o si modifica un framework dalla console (sebbene il valore possa essere una stringa vuota se inclusa in un CloudFormation modello).

La struttura a cui assegnare un tag è: `[{"Key":"string","Value":"string"}]`.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CopyAction

Servizio: AWS Backup

I dettagli dell'operazione di copia.

Indice

DestinationBackupVaultArn

Un Amazon Resource Name (ARN) che identifica in modo univoco l'insieme di credenziali di backup di destinazione per il backup copiato. Ad esempio, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: stringa

Campo obbligatorio: sì

Lifecycle

Speciifica il periodo di tempo, in giorni, prima che un punto di ripristino passi alla conservazione a freddo o venga eliminato.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, sulla console, l'impostazione di conservazione deve essere superiore di 90 giorni rispetto all'impostazione del passaggio al freddo dopo giorni. L'impostazione relativa alla transizione a freddo dopo giorni non può essere modificata dopo che un backup è passato a freddo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Per rimuovere il ciclo di vita e i periodi di conservazione esistenti e mantenere i punti di ripristino a tempo indeterminato, specifica -1 per e. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Tipo: oggetto Lifecycle

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CopyJob

Servizio: AWS Backup

Contiene informazioni dettagliate su un processo di copia.

Indice

AccountId

L'ID account proprietario del processo di copia.

Tipo: stringa

Modello: `^[0-9]{12}$`

Campo obbligatorio: no

BackupSizeInBytes

La dimensione, in byte, di un processo di copia.

Tipo: long

Campo obbligatorio: no

ChildJobsInState

Ciò restituisce le statistiche dei processi di copia figlio (nidificati) inclusi.

Tipo: mappatura stringa a intero lungo

Chiavi valide: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Campo obbligatorio: no

CompletionDate

La data e l'ora di completamento di un processo di copia, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

CompositeMemberIdentifier

L'identificatore di una risorsa all'interno di un gruppo composito, ad esempio un punto di ripristino annidato (figlio) appartenente a uno stack composito (principale). L'ID viene trasferito dall'ID logico all'interno di uno stack.

- Tipo: stringa

Campo obbligatorio: no

CopyJobId

Identifica in modo univoco un processo di copia.

- Tipo: stringa

Campo obbligatorio: no

CreatedBy

Contiene informazioni sul piano e sulla regola di backup AWS Backup utilizzati per avviare il backup del punto di ripristino.

Tipo: oggetto RecoveryPointCreator

Campo obbligatorio: no

CreationDate

La data e l'ora di creazione di un processo di copia, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

DestinationBackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di copia di destinazione, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

Campo obbligatorio: no

DestinationRecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino di destinazione; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

Campo obbligatorio: no

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione; ad esempio `arn:aws:iam::123456789012:role/S3Access`.

- Tipo: stringa

Campo obbligatorio: no

IsParent

Questo è un valore booleano che indica che si tratta di un processo di copia (composito) padre.

Tipo: Booleano

Campo obbligatorio: no

MessageCategory

Questo parametro è il numero di processi per la categoria di messaggi specificata.

Stringhe di esempio possono essere `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` e `InvalidParameters`. Vedi Monitoraggio per un elenco di MessageCategory stringhe.

Il valore ANY restituisce il conteggio di tutte le categorie di messaggi.

`AGGREGATE_ALL` aggrega i numeri dei processi per tutte le categorie di messaggi e restituisce la somma

- Tipo: stringa

Campo obbligatorio: no

NumberOfChildJobs

Il numero di lavori di copia secondari (annidati).

Tipo: long

Campo obbligatorio: no

ParentJobId

Questo identifica in modo univoco una richiesta ad AWS Backup per copiare una risorsa. Il risultato sarà l'ID processo (composito) padre.

- Tipo: stringa

Campo obbligatorio: no

ResourceArn

La AWS risorsa da copiare, ad esempio un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS).

- Tipo: stringa

Campo obbligatorio: no

ResourceName

Il nome non univoco della risorsa che appartiene al backup specificato.

- Tipo: stringa

Campo obbligatorio: no

ResourceType

Il tipo di AWS risorsa da copiare; ad esempio, un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS).

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

SourceBackupVaultArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un vault di backup di origine, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

- Tipo: stringa

Campo obbligatorio: no

SourceRecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino di origine; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

Campo obbligatorio: no

State

Lo stato corrente di un processo di copia.

- Tipo: stringa

Valori validi: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Campo obbligatorio: no

StatusMessage

Un messaggio dettagliato che spiega lo stato del processo di copia di una risorsa.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta AWS quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CopyJobSummary

Servizio: AWS Backup

È un riepilogo dei processi di copia creati o eseguiti negli ultimi 30 giorni.

Il riepilogo restituito può contenere quanto segue: Regione, Account RestourceType, Stato MessageCategory StartTime, EndTime,, e Numero di lavori inclusi.

Indice

AccountId

L'ID dell'account proprietario dei processi del riepilogo.

Tipo: stringa

Modello: `^[0-9]{12}$`

Campo obbligatorio: no

Count

Il valore espresso come numero di processi in un riepilogo dei processi.

Tipo: integer

Campo obbligatorio: no

EndTime

Il valore in formato numerico dell'ora di fine di un processo.

Questo valore indica l'ora in formato Unix, Coordinated Universal Time (UTC) con precisione al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

MessageCategory

Questo parametro è il numero di processi per la categoria di messaggi specificata.

Stringhe di esempio sono `AccessDenied`, `Success` e `InvalidParameters`. Vedi Monitoraggio per un elenco di MessageCategory stringhe.

Il valore ANY restituisce il conteggio di tutte le categorie di messaggi.

AGGREGATE_ALL aggrega i numeri dei processi per tutte le categorie di messaggi e restituisce la somma.

- Tipo: stringa

Campo obbligatorio: no

Region

Le AWS regioni all'interno del riepilogo del lavoro.

- Tipo: stringa

Campo obbligatorio: no

ResourceType

Il valore del numero di processi per il tipo di risorsa specificato. La richiesta GetSupportedResourceTypes restituisce le stringhe per i tipi di risorsa supportati

Tipo: stringa

Modello: ^[a-zA-Z0-9\-_\.]{1,50}$

Campo obbligatorio: no

StartTime

Il valore in formato numerico dell'ora di inizio di un processo.

Questo valore indica l'ora in formato Unix, Coordinated Universal Time (UTC) con precisione al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

State

Questo valore indica il numero di processi con lo stato specificato.

- Tipo: stringa

Valori validi: `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DateRange

Servizio: AWS Backup

Questo è un filtro di risorse che contiene FromDate: DateTime e ToDate: DateTime. Entrambi i valori sono obbligatori. DateTime I valori futuri non sono consentiti.

La data e l'ora sono in formato Unix e ora UTC (Coordinated Universal Time) e hanno una precisione al millisecondo (i millisecondi sono opzionali). Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Indice

FromDate

Questo valore è la data di inizio, inclusiva.

La data e l'ora sono in formato Unix e ora UTC (Coordinated Universal Time) e hanno una precisione al millisecondo (i millisecondi sono opzionali).

Tipo: Timestamp

Campo obbligatorio: sì

ToDate

Questo valore è la data di fine, inclusiva.

La data e l'ora sono in formato Unix e ora UTC (Coordinated Universal Time) e hanno una precisione al millisecondo (i millisecondi sono opzionali).

Tipo: Timestamp

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Framework

Servizio: AWS Backup

Contiene informazioni dettagliate su un framework. I framework contengono controlli che valutano e generano report sugli eventi e sulle risorse di backup. I framework generano risultati di conformità giornalieri.

Indice

CreationTime

La data e l'ora di creazione del framework, nella rappresentazione ISO 8601. Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, 2020-07-10T15:00:00.000-08:00 rappresenta il 10 luglio 2020 alle 15:00 8 ore indietro rispetto all'UTC.

Tipo: Timestamp

Campo obbligatorio: no

DeploymentStatus

Lo stato di implementazione di un framework. Gli stati sono:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

- Tipo: stringa

Campo obbligatorio: no

FrameworkArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

Campo obbligatorio: no

FrameworkDescription

Descrizione facoltativa del framework, per un massimo di 1.024 caratteri.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `.*\S.*`

Campo obbligatorio: no

FrameworkName

Il nome univoco di un framework. Contiene da 1 a 256 caratteri, a partire da una lettera, ed è costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: no

NumberOfControls

Il numero di controlli contenuti dal framework.

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

FrameworkControl

Servizio: AWS Backup

Contiene informazioni dettagliate su tutti i controlli di un framework. Ogni framework deve contenere almeno un controllo.

Indice

ControlName

Il nome di un controllo. Il nome deve contenere da 1 a 256 caratteri.

Tipo: stringa

Campo obbligatorio: sì

ControlInputParameters

Le coppie nome/valore.

Tipo: matrice di oggetti ControlInputParameter

Campo obbligatorio: no

ControlScope

L'ambito di un controllo. L'ambito del controllo stabilisce gli elementi da valutare. I tre ambiti di controllo esemplificativi sono: un piano di backup specifico, tutti i piani di backup con un tag specifico o tutti i piani di backup.

Per ulteriori informazioni, consulta `ControlScope.`

Tipo: oggetto ControlScope

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2

- AWS SDK per Ruby V3

KeyValue

Servizio: AWS Backup

Coppia di due stringhe correlate. I caratteri consentiti sono lettere, spazi e numeri che possono essere rappresentati nel formato UTF-8 e i caratteri seguenti: `+ - = . _ : /`.

Indice

Key

La chiave tag (String). La chiave non può iniziare con `aws:`.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Tipo: stringa

Campo obbligatorio: sì

Value

Il valore della chiave.

Limitazioni di lunghezza: lunghezza massima di 256.

Modello: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Tipo: stringa

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

LegalHold

Servizio: AWS Backup

Un blocco a fini legali è uno strumento amministrativo che impedisce l'eliminazione dei backup mentre sono bloccati. Finché il blocco è in vigore, i backup bloccati non possono essere eliminati e le policy del ciclo di vita che potrebbero alterare lo stato del backup (ad esempio la transizione allo storage a freddo) vengono rimandate finché il blocco a fini legali non viene rimosso. Un backup può essere oggetto di molteplici blocchi a fini legali. I blocchi a fini legali vengono applicati a uno o più backup (noti anche come punti di ripristino). Questi backup possono essere filtrati in base ai tipi di risorse e agli ID risorse.

Indice

CancellationDate

L'ora in cui la sospensione legale è stata annullata.

Tipo: Timestamp

Campo obbligatorio: no

CreationDate

L'ora in cui è stata creata la conservazione legale.

Tipo: Timestamp

Campo obbligatorio: no

Description

La descrizione di un blocco legale.

- Tipo: stringa

Campo obbligatorio: no

LegalHoldArn

L'Amazon Resource Name (ARN) della riserva legale; ad esempio,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

- Tipo: stringa

Campo obbligatorio: no

LegalHoldId

L'ID della custodia legale.

- Tipo: stringa

Campo obbligatorio: no

Status

Lo stato della custodia legale.

- Tipo: stringa

Valori validi: `CREATING | ACTIVE | CANCELING | CANCELED`

Campo obbligatorio: no

Title

Il titolo del possesso legale.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Lifecycle

Servizio: AWS Backup

Speciifica il periodo di tempo, in giorni, prima che un punto di ripristino passi alla conservazione a freddo o venga eliminato.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, sulla console, l'impostazione di conservazione deve essere superiore di 90 giorni rispetto all'impostazione del passaggio al freddo dopo giorni. L'impostazione relativa alla transizione a freddo dopo giorni non può essere modificata dopo che un backup è passato a freddo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Per rimuovere il ciclo di vita e i periodi di conservazione esistenti e mantenere i punti di ripristino a tempo indeterminato, specifica -1 per e. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Indice

DeleteAfterDays

Il numero di giorni dopo la creazione in cui un punto di ripristino viene eliminato. Questo valore deve corrispondere ad almeno 90 giorni dal numero di giorni specificato in`MoveToColdStorageAfterDays`.

Tipo: long

Campo obbligatorio: no

MoveToColdStorageAfterDays

Il numero di giorni dopo la creazione in cui un punto di ripristino viene spostato nella cella frigorifera.

Tipo: long

Campo obbligatorio: no

OptInToArchiveForSupportedResources

Se il valore è vero, il piano di backup trasferisce le risorse supportate al livello di archiviazione (a freddo) in base alle impostazioni del ciclo di vita.

Tipo: Booleano

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ProtectedResource

Servizio: AWS Backup

Una struttura contenente informazioni su una risorsa di backup.

Indice

LastBackupTime

La data e l'ora di esecuzione dell'ultimo backup di una risorsa, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `LastBackupTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

LastBackupVaultArn

L'ARN (Amazon Resource Name) dell'archivio di backup che contiene il punto di ripristino di backup più recente.

- Tipo: stringa

Campo obbligatorio: no

LastRecoveryPointArn

L'ARN (Amazon Resource Name) del punto di ripristino più recente.

- Tipo: stringa

Campo obbligatorio: no

ResourceArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

Campo obbligatorio: no

ResourceName

Il nome non univoco della risorsa che appartiene al backup specificato.

- Tipo: stringa

Campo obbligatorio: no

ResourceType

Il tipo di AWS risorsa, ad esempio un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS). Per i backup di Windows Volume Shadow Copy Service (VSS), l'unico tipo di risorsa supportato è Amazon EC2.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ProtectedResourceConditions

Servizio: AWS Backup

Le condizioni che definisci per le risorse nel tuo piano di test di ripristino utilizzando i tag.

Ad esempio, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Gli operatori di condizione fanno distinzione tra maiuscole e minuscole.

Indice

StringEquals

Filtra i valori delle risorse con tag solo per le risorse a cui hai aggiunto tag con lo stesso valore. Detta anche “corrispondenza esatta”.

Tipo: matrice di oggetti KeyValue

Campo obbligatorio: no

StringNotEquals

Filtra i valori delle risorse con tag solo per le risorse a cui hai aggiunto tag che non hanno lo stesso valore. Detta anche “corrispondenza negata”.

Tipo: matrice di oggetti KeyValue

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RecoveryPointByBackupVault

Servizio: AWS Backup

Contiene informazioni dettagliate sui punti di ripristino archiviati in un vault di backup.

Indice

BackupSizeInBytes

La dimensione, in byte, di un backup.

Tipo: long

Campo obbligatorio: no

BackupVaultArn

Un ARN che identifica in modo univoco un vault di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

-Tipo: stringa

Campo obbligatorio: no

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: no

CalculatedLifecycle

Un oggetto `CalculatedLifecycle` contenente i timestamp `DeleteAt` e `MoveToColdStorageAt`.

Tipo: oggetto CalculatedLifecycle

Campo obbligatorio: no

CompletionDate

La data e l'ora di completamento del processo di ripristino di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

CompositeMemberIdentifier

L'identificatore di una risorsa all'interno di un gruppo composito, ad esempio un punto di ripristino annidato (figlio) appartenente a uno stack composito (principale). L'ID viene trasferito dall'ID logico all'interno di uno stack.

-Tipo: stringa

Campo obbligatorio: no

CreatedBy

Contiene informazioni identificative sulla creazione di un punto di ripristino, tra cui `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` e `BackupRuleId` del piano di backup utilizzato per crearlo.

Tipo: oggetto RecoveryPointCreator

Campo obbligatorio: no

CreationDate

La data e l'ora di creazione di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

EncryptionKeyArn

La chiave di crittografia lato server utilizzata per proteggere i backup, ad esempio `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

- Tipo: stringa

Campo obbligatorio: no

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione; ad esempio, `arn:aws:iam::123456789012:role/S3Access`.

- Tipo: stringa

Campo obbligatorio: no

IsEncrypted

Un valore booleano che viene restituito come `TRUE` se il punto di ripristino specificato è crittografato o `FALSE` se il punto di ripristino non è crittografato.

Tipo: Booleano

Campo obbligatorio: no

IsParent

Questo è un valore booleano che indica che si tratta di un punto di ripristino (composito) padre.

Tipo: Booleano

Campo obbligatorio: no

LastRestoreTime

La data e l'ora dell'ultimo ripristino di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `LastRestoreTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

Lifecycle

Il ciclo di vita definisce quando una risorsa protetta viene trasferita alla conservazione a freddo e quando scade. AWS Backup esegue automaticamente le transizioni e le scadenze dei backup in base al ciclo di vita definito dall'utente.

I backup trasferiti allo storage dei dati inattivi devono essere archiviati nello storage dei dati inattivi per un minimo di 90 giorni. Pertanto, l'impostazione "conservazione" deve essere 90 giorni maggiore dell'impostazione "transizione a inattivo dopo". L'impostazione "transizione a inattivo dopo" non può essere modificata dopo che è stata eseguita la transizione di un backup a inattivo.

I tipi di risorse che possono passare alla conservazione a freddo sono elencati nella tabella Disponibilità delle funzionalità per risorsa. AWS Backup ignora questa espressione per altri tipi di risorse.

Tipo: oggetto Lifecycle

Campo obbligatorio: no

ParentRecoveryPointArn

L'Amazon Resource Name (ARN) del punto di ripristino principale (composito).

- Tipo: stringa

Campo obbligatorio: no

RecoveryPointArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

Campo obbligatorio: no

ResourceArn

Un ARN che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

Campo obbligatorio: no

ResourceName

Il nome non univoco della risorsa che appartiene al backup specificato.

- Tipo: stringa

Campo obbligatorio: no

ResourceType

Il tipo di AWS risorsa salvata come punto di ripristino; ad esempio, un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS). Per i backup di Windows Volume Shadow Copy Service (VSS), l'unico tipo di risorsa supportato è Amazon EC2.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

SourceBackupVaultArn

Il vault di backup da cui è stato originariamente copiato il punto di ripristino. Se il punto di ripristino viene ripristinato nello stesso account, questo valore sarà `null`.

- Tipo: stringa

Campo obbligatorio: no

Status

Un codice di stato che specifica lo stato del punto di ripristino.

- Tipo: stringa

Valori validi: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Campo obbligatorio: no

StatusMessage

Un messaggio che spiega lo stato attuale del punto di ripristino.

- Tipo: stringa

Campo obbligatorio: no

VaultType

Il tipo di archivio in cui è archiviato il punto di ripristino descritto.

- Tipo: stringa

Valori validi: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RecoveryPointByResource

Servizio: AWS Backup

Contiene informazioni dettagliate su un punto di ripristino salvato.

Indice

BackupSizeBytes

La dimensione, in byte, di un backup.

Tipo: long

Campo obbligatorio: no

BackupVaultName

Il nome di un container logico in cui vengono archiviati i backup. I vault di backup sono identificati da nomi univoci per l'account utilizzato per crearli e per la Regione AWS in cui sono stati creati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: no

CreationDate

La data e l'ora di creazione di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

EncryptionKeyArn

La chiave di crittografia lato server utilizzata per proteggere i backup, ad esempio `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

-Tipo: stringa

Campo obbligatorio: no

IsParent

Questo è un valore booleano che indica che si tratta di un punto di ripristino (composito) padre.

Tipo: Booleano

Campo obbligatorio: no

ParentRecoveryPointArn

L'Amazon Resource Name (ARN) del punto di ripristino principale (composito).

- Tipo: stringa

Campo obbligatorio: no

RecoveryPointArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un punto di ripristino, ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

Campo obbligatorio: no

ResourceName

Il nome non univoco della risorsa che appartiene al backup specificato.

- Tipo: stringa

Campo obbligatorio: no

Status

Un codice di stato che specifica lo stato del punto di ripristino.

- Tipo: stringa

Valori validi: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Campo obbligatorio: no

StatusMessage

Un messaggio che spiega lo stato attuale del punto di ripristino.

- Tipo: stringa

Campo obbligatorio: no

VaultType

Il tipo di archivio in cui è archiviato il punto di ripristino descritto.

- Tipo: stringa

Valori validi: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RecoveryPointCreator

Servizio: AWS Backup

Contiene informazioni sul piano e sulla regola di backup AWS Backup utilizzati per avviare il backup del punto di ripristino.

Indice

BackupPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di backup, ad esempio `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

- Tipo: stringa

Campo obbligatorio: no

BackupPlanId

Identifica in modo univoco un piano di backup.

- Tipo: stringa

Campo obbligatorio: no

BackupPlanVersion

Gli ID versione sono stringhe con codifica UTF-8 Unicode univoche generate casualmente con lunghezza massimo di 1.024 byte. e non possono essere modificati.

- Tipo: stringa

Campo obbligatorio: no

BackupRuleId

Identifica in modo univoco una regola utilizzata per pianificare il backup di una selezione di risorse.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RecoveryPointMember

Servizio: AWS Backup

Questo è un punto di ripristino (nidificato) figlio di un punto di ripristino (composito) padre. Questi punti di ripristino possono essere dissociati dal punto di ripristino (composito) padre, nel qual caso non saranno più un membro.

Indice

BackupVaultName

Il nome dell'archivio di backup (il contenitore logico in cui sono archiviati i backup).

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_]{2,50}$`

Campo obbligatorio: no

RecoveryPointArn

L'Amazon Resource Name (ARN) del punto di ripristino principale (composito).

-Tipo: stringa

Campo obbligatorio: no

ResourceArn

L'Amazon Resource Name (ARN) che identifica in modo univoco una risorsa salvata.

-Tipo: stringa

Campo obbligatorio: no

ResourceType

Il tipo di AWS risorsa che viene salvata come punto di ripristino.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RecoveryPointSelection

Servizio: AWS Backup

Questo specifica i criteri per assegnare un set di risorse, come i tipi di risorse o i vault di backup.

Indice

DateRange

Questo è un filtro di risorse che contiene FromDate: DateTime e ToDate: DateTime. Entrambi i valori sono obbligatori. DateTime I valori futuri non sono consentiti.

La data e l'ora sono in formato Unix e ora UTC (Coordinated Universal Time) e hanno una precisione al millisecondo (i millisecondi sono opzionali). Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: oggetto DateRange

Campo obbligatorio: no

ResourceIdentifiers

Queste sono le risorse incluse nella selezione delle risorse (tra cui il tipo di risorse e vault).

Tipo: matrice di stringhe

Campo obbligatorio: no

VaultNames

Questi sono i nomi dei vault in cui sono contenuti i punti di ripristino selezionati.

Tipo: matrice di stringhe

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2

- AWS SDK per Ruby V3

ReportDeliveryChannel

Servizio: AWS Backup

Contiene informazioni del piano di report indicante dove consegnare i report, in particolare il nome del bucket Amazon S3, il prefisso della chiave S3 e i formati dei report.

Indice

S3BucketName

Il nome univoco del bucket S3 che riceve i report.

Tipo: stringa

Campo obbligatorio: sì

Formats

Il formato dei report: `CSV`, `JSON`, o entrambi. Se non è specificato, il formato predefinito è `CSV`.

Tipo: matrice di stringhe

Campo obbligatorio: no

S3KeyPrefix

Il prefisso con cui AWS Backup Audit Manager invia i report ad Amazon S3. Il prefisso è questa parte del percorso seguente: s3:///your-bucket-name/backup/US-West-2/anno/mese/giorno/nome-report. `prefix` Se non è specificato, non esiste alcun prefisso.

-Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in AWS uno degli SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportDestination

Servizio: AWS Backup

Contiene informazioni del processo di report relative alla destinazione del report.

Indice

S3BucketName

Il nome univoco del bucket Amazon S3 che riceve i report.

- Tipo: stringa

Campo obbligatorio: no

S3Keys

La chiave dell'oggetto che identifica in modo univoco i report nel bucket S3.

Tipo: matrice di stringhe

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportJob

Servizio: AWS Backup

Contiene informazioni dettagliate su un processo di report. Un processo di report compila un report basato su un piano di report e lo pubblica su Amazon S3.

Indice

CompletionTime

La data e l'ora di completamento di un processo di report, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CompletionTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

CreationTime

La data e l'ora di creazione di un processo di report, nel formato orario Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

ReportDestination

Il nome del bucket S3 e le chiavi S3 per la destinazione in cui il processo di report pubblica il report.

Tipo: oggetto ReportDestination

Campo obbligatorio: no

ReportJobId

L'identificatore per un processo di report. Stringa con codifica UTF-8 Unicode univoca generata casualmente con lunghezza massima di 1.024 byte. L'ID processo report non può essere modificato.

- Tipo: stringa

Campo obbligatorio: no

ReportPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

Campo obbligatorio: no

ReportTemplate

Identifica il modello di report per il report. I report vengono creati utilizzando un modello di report. I modelli di report sono:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

- Tipo: stringa

Campo obbligatorio: no

Status

Lo stato di un processo di report. Gli stati sono:

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED` significa che il report è disponibile per la revisione nella destinazione designata. Se lo stato è `FAILED`, esamina `StatusMessage` per il motivo.

- Tipo: stringa

Campo obbligatorio: no

StatusMessage

Un messaggio che spiega lo stato del processo di report.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportPlan

Servizio: AWS Backup

Contiene informazioni dettagliate su un piano di report.

Indice

CreationTime

La data e l'ora di creazione di un piano di report, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

DeploymentStatus

Lo stato di implementazione di un piano di report. Gli stati sono:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED`

-Tipo: stringa

Campo obbligatorio: no

LastAttemptedExecutionTime

La data e l'ora dell'ultimo tentativo di esecuzione di un processo di report associato a questo piano di report, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `LastAttemptedExecutionTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

LastSuccessfulExecutionTime

La data e l'ora dell'ultima esecuzione riuscita di un processo di report associato a questo piano di report, in formato Unix e ora UTC (Coordinated Universal Time). Il valore di `LastSuccessfulExecutionTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

ReportDeliveryChannel

Contiene informazioni su dove e come consegnare i report, in particolare il nome del bucket Amazon S3, il prefisso della chiave S3 e i formati dei report.

Tipo: oggetto ReportDeliveryChannel

Campo obbligatorio: no

ReportPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

Campo obbligatorio: no

ReportPlanDescription

Descrizione facoltativa del piano di report, per un massimo di 1.024 caratteri.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `.*\S.*`

Campo obbligatorio: no

ReportPlanName

Il nome univoco del piano di report. Contiene da 1 a 256 caratteri, a partire da una lettera, ed è costituito da lettere (a-z, A-Z), numeri (0-9) e caratteri di sottolineatura (_).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `[a-zA-Z][_a-zA-Z0-9]*`

Campo obbligatorio: no

ReportSetting

Identifica il modello di report per il report. I report vengono creati utilizzando un modello di report. I modelli di report sono:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Se il modello di report è `RESOURCE_COMPLIANCE_REPORT` o`CONTROL_COMPLIANCE_REPORT`, questa risorsa API descrive anche la copertura del report da Regioni AWS e i framework.

Tipo: oggetto ReportSetting

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ReportSetting

Servizio: AWS Backup

Contiene informazioni dettagliate sull'impostazione di un report.

Indice

ReportTemplate

Identifica il modello di report per il report. I report vengono creati utilizzando un modello di report. I modelli di report sono:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Tipo: stringa

Campo obbligatorio: sì

Accounts

Questi sono gli account da includere nel report.

Usa il valore stringa di `ROOT` per includere tutte le unità organizzative.

Tipo: matrice di stringhe

Campo obbligatorio: no

FrameworkArns

I nomi delle risorse Amazon (ARN) dei framework coperti da un report.

Tipo: matrice di stringhe

Campo obbligatorio: no

NumberOfFrameworks

Il numero di framework coperti da un report.

Tipo: integer

Campo obbligatorio: no

OrganizationUnits

Sono le unità organizzative da includere nel report.

Tipo: matrice di stringhe

Campo obbligatorio: no

Regions

Sono le regioni da includere nel report.

Utilizzate il carattere jolly come valore di stringa per includere tutte le regioni.

Tipo: matrice di stringhe

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreJobCreator

Servizio: AWS Backup

Contiene informazioni sul piano di test di ripristino utilizzato da AWS Backup per avviare il processo di ripristino.

Indice

RestoreTestingPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di test di ripristino.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreJobsListMember

Servizio: AWS Backup

Contiene metadati relativi a un processo di ripristino.

Indice

AccountId

L'ID account proprietario del processo di ripristino.

Tipo: stringa

Modello: `^[0-9]{12}$`

Campo obbligatorio: no

BackupSizeInBytes

La dimensione, in byte, della risorsa ripristinata.

Tipo: long

Campo obbligatorio: no

CompletionDate

La data e l'ora di completamento del processo di ripristino di un punto di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CompletionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

CreatedBy

Contiene informazioni di identificazione sulla creazione di un processo di ripristino.

Tipo: oggetto RestoreJobCreator

Campo obbligatorio: no

CreatedResourceArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco una risorsa. Il formato dell'ARN dipende dal tipo di risorsa.

- Tipo: stringa

Campo obbligatorio: no

CreationDate

La data e l'ora di creazione di un processo di ripristino, nel formato orario Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

DeletionStatus

Registra lo stato dei dati generati dal test di ripristino. Lo stato può essere `Deleting`, `Failed` o `Successful`.

- Tipo: stringa

Valori validi: `DELETING | FAILED | SUCCESSFUL`

Campo obbligatorio: no

DeletionStatusMessage

Descrive lo stato di eliminazione del processo di ripristino.

- Tipo: stringa

Campo obbligatorio: no

ExpectedCompletionTimeMinutes

La quantità di tempo in minuti prevista per l’esecuzione del processo di ripristino di un punto di ripristino.

Tipo: long

Campo obbligatorio: no

IamRoleArn

Specifica l'ARN del ruolo IAM utilizzato per creare il punto di ripristino di destinazione; ad esempio, `arn:aws:iam::123456789012:role/S3Access`.

- Tipo: stringa

Campo obbligatorio: no

PercentDone

Contiene una percentuale stimata di completamento di un processo nel momento in cui è stato richiesto lo stato del processo.

- Tipo: stringa

Campo obbligatorio: no

RecoveryPointArn

Un ARN che identifica in modo univoco un punto di ripristino; ad esempio `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

- Tipo: stringa

Campo obbligatorio: no

RecoveryPointCreationDate

La data di creazione di un punto di ripristino.

Tipo: Timestamp

Campo obbligatorio: no

ResourceType

Il tipo di risorsa dei processi di ripristino elencati, ad esempio un volume Amazon Elastic Block Store (Amazon EBS) o un database Amazon Relational Database Service (Amazon RDS). Per i backup di Windows Volume Shadow Copy Service (VSS), l'unico tipo di risorsa supportato è Amazon EC2.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

RestoreJobId

Identifica in modo univoco il processo che ripristina un punto di ripristino.

- Tipo: stringa

Campo obbligatorio: no

Status

Un codice di stato che specifica lo stato del processo avviato da AWS Backup per ripristinare un punto di ripristino.

- Tipo: stringa

Valori validi: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

Campo obbligatorio: no

StatusMessage

Un messaggio dettagliato che spiega lo stato del processo di ripristino di un punto di ripristino.

- Tipo: stringa

Campo obbligatorio: no

ValidationStatus

Lo stato della convalida viene eseguito sul processo di ripristino indicato.

- Tipo: stringa

Valori validi: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Campo obbligatorio: no

ValidationStatusMessage

Descrive lo stato della convalida eseguita sul processo di ripristino indicato.

- Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreJobSummary

Servizio: AWS Backup

È il riepilogo dei processi di ripristino creati o eseguiti negli ultimi 30 giorni.

Il riepilogo restituito può contenere quanto segue: Regione, Account ResourceType, Stato MessageCategory StartTime, EndTime,, e Numero di lavori inclusi.

Indice

AccountId

L'ID dell'account proprietario dei processi del riepilogo.

Tipo: stringa

Modello: `^[0-9]{12}$`

Campo obbligatorio: no

Count

Il valore espresso come numero di processi in un riepilogo dei processi.

Tipo: integer

Campo obbligatorio: no

EndTime

Il valore in formato numerico dell'ora di fine di un processo.

Questo valore indica l'ora in formato Unix, Coordinated Universal Time (UTC) con precisione al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

Region

Le AWS regioni all'interno del riepilogo delle offerte di lavoro.

-Tipo: stringa

Campo obbligatorio: no

ResourceType

Il valore del numero di processi per il tipo di risorsa specificato. La richiesta `GetSupportedResourceTypes` restituisce le stringhe per i tipi di risorsa supportati.

Tipo: stringa

Modello: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Campo obbligatorio: no

StartTime

Il valore in formato numerico dell'ora di inizio di un processo.

Questo valore indica l'ora in formato Unix, Coordinated Universal Time (UTC) con precisione al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

State

Questo valore indica il numero di processi con lo stato specificato.

-Tipo: stringa

Valori validi: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2

- AWS SDK per Ruby V3

RestoreTestingPlanForCreate

Servizio: AWS Backup

Contiene i metadati su un piano di test di ripristino.

Indice

RecoveryPointSelection

`RecoveryPointSelection`ha cinque parametri (tre obbligatori e due opzionali). I valori specificati determinano quale punto di ripristino è incluso nel test di ripristino. È necessario indicare con `Algorithm` se si desidera utilizzare il punto di ripristino più recente `SelectionWindowDays` o se si desidera un punto di ripristino casuale e indicare attraverso `IncludeVaults` quali archivi è possibile scegliere i punti di ripristino.

`Algorithm`(obbligatorio) Valori validi: "`LATEST_WITHIN_WINDOW`" o "`RANDOM_WITHIN_WINDOW`».

`Recovery point types`(obbligatorio) Valori validi: "`SNAPSHOT`" e/o "`CONTINUOUS`». Include `SNAPSHOT` per ripristinare solo i punti di ripristino delle istantanee; include `CONTINUOUS` per ripristinare i punti di ripristino continui (point in time restore/PITR); utilizza entrambi per ripristinare un'istantanea o un punto di ripristino continuo. Il punto di ripristino sarà determinato dal valore di. `Algorithm`

`IncludeVaults`(richiesto). È necessario includere uno o più archivi di backup. Usa la wildcard ["*"] o ARN specifici.

`SelectionWindowDays`(opzionale) Il valore deve essere un numero intero (in giorni) compreso tra 1 e 365. Se non è incluso, il valore predefinito è. `30`

`ExcludeVaults`(opzionale). È possibile scegliere di inserire uno o più ARN di backup vault specifici per escludere il contenuto di tali vault dall'idoneità al ripristino. In alternativa, è possibile includere un elenco di selettori. Se questo parametro e il relativo valore non sono inclusi, il valore predefinito è un elenco vuoto.

Tipo: oggetto RestoreTestingRecoveryPointSelection

Campo obbligatorio: sì

RestoreTestingPlanName

RestoreTestingPlanName è una stringa univoca che è il nome del piano di test di ripristino. Non può essere modificato dopo la creazione e deve essere composto solo da caratteri alfanumerici e caratteri di sottolineatura.

Tipo: stringa

Campo obbligatorio: sì

ScheduleExpression

Un'espressione CRON nel fuso orario specificato quando viene eseguito un piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

ScheduleExpressionTimezone

Facoltativo. Questo è il fuso orario in cui viene impostata l'espressione di pianificazione. Per impostazione predefinita, ScheduleExpressions sono in UTC. Puoi modificarlo impostando un fuso orario specifico.

- Tipo: stringa

Campo obbligatorio: no

StartWindowHours

L'impostazione predefinita è 24 ore.

Un valore in ore dopo la pianificazione di un test di ripristino prima che un processo venga annullato se non viene avviato correttamente. Questo valore è facoltativo. Se incluso, il parametro ha un valore massimo di 168 ore (una settimana).

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreTestingPlanForGet

Servizio: AWS Backup

Contiene i metadati su un piano di test di ripristino.

Indice

CreationTime

La data e l'ora di creazione di un piano di test di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: sì

RecoveryPointSelection

I criteri specificati per assegnare un set di risorse, come i tipi di punto di ripristino o i vault di backup.

Tipo: oggetto RestoreTestingRecoveryPointSelection

Campo obbligatorio: sì

RestoreTestingPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

RestoreTestingPlanName

Il nome del piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

ScheduleExpression

Un'espressione CRON nel fuso orario specificato quando viene eseguito un piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

CreatorRequestId

Identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Se la richiesta include un `CreatorRequestId` che corrisponde a un piano di backup esistente, tale piano viene restituito. Questo parametro è facoltativo.

Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

- Tipo: stringa

Campo obbligatorio: no

LastExecutionTime

L'ultima volta che è stato eseguito un test di ripristino con il piano di test di ripristino specificato. Una data e ora, in formato UNIX e nell'ora Universal Coordinated Time (UTC). Il valore di `LastExecutionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

LastUpdateTime

La data e l'ora di aggiornamento del piano di test di ripristino. Questo aggiornamento è in formato Unix e nell'ora Coordinated Universal Time (UTC). Il valore di `LastUpdateTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

ScheduleExpressionTimezone

Facoltativo. Questo è il fuso orario in cui viene impostata l'espressione di pianificazione. Per impostazione predefinita, ScheduleExpressions sono in formato UTC. Puoi modificarlo impostando un fuso orario specifico.

- Tipo: stringa

Campo obbligatorio: no

StartWindowHours

L'impostazione predefinita è 24 ore.

Un valore in ore dopo la pianificazione di un test di ripristino prima che un processo venga annullato se non viene avviato correttamente. Questo valore è facoltativo. Se incluso, il parametro ha un valore massimo di 168 ore (una settimana).

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreTestingPlanForList

Servizio: AWS Backup

Contiene i metadati su un piano di test di ripristino.

Indice

CreationTime

La data e l'ora di creazione di un piano di test di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: sì

RestoreTestingPlanArn

Un nome della risorsa Amazon (ARN) che identifica in modo univoco un piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

RestoreTestingPlanName

Il nome del piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

ScheduleExpression

Un'espressione CRON nel fuso orario specificato quando viene eseguito un piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

LastExecutionTime

L'ultima volta che è stato eseguito un test di ripristino con il piano di test di ripristino specificato. Una data e ora, in formato UNIX e nell'ora Universal Coordinated Time (UTC). Il valore di

`LastExecutionDate` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

LastUpdateTime

La data e l'ora di aggiornamento del piano di test di ripristino. Questo aggiornamento è in formato Unix e nell'ora Coordinated Universal Time (UTC). Il valore di `LastUpdateTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 alle ore 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: no

ScheduleExpressionTimezone

Facoltativo. Questo è il fuso orario in cui viene impostata l'espressione di pianificazione. Per impostazione predefinita, ScheduleExpressions sono in formato UTC. Puoi modificarlo impostando un fuso orario specifico.

-Tipo: stringa

Campo obbligatorio: no

StartWindowHours

L'impostazione predefinita è 24 ore.

Un valore in ore dopo la pianificazione di un test di ripristino prima che un processo venga annullato se non viene avviato correttamente. Questo valore è facoltativo. Se incluso, il parametro ha un valore massimo di 168 ore (una settimana).

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreTestingPlanForUpdate

Servizio: AWS Backup

Contiene i metadati su un piano di test di ripristino.

Indice

RecoveryPointSelection

Obbligatorio: `Algorithm`; `RecoveryPointTypes`; `IncludeVaults` (almeno uno).

Facoltativo: SelectionWindowDays('30' se non specificato); `ExcludeVaults` (il valore predefinito è un elenco vuoto se non è elencato).

Tipo: oggetto RestoreTestingRecoveryPointSelection

Campo obbligatorio: no

ScheduleExpression

Un'espressione CRON nel fuso orario specificato quando viene eseguito un piano di test di ripristino.

- Tipo: stringa

Campo obbligatorio: no

ScheduleExpressionTimezone

Facoltativo. Questo è il fuso orario in cui viene impostata l'espressione di pianificazione. Per impostazione predefinita, ScheduleExpressions sono in UTC. Puoi modificarlo impostando un fuso orario specifico.

- Tipo: stringa

Campo obbligatorio: no

StartWindowHours

L'impostazione predefinita è 24 ore.

Un valore in ore dopo la pianificazione di un test di ripristino prima che un processo venga annullato se non viene avviato correttamente. Questo valore è facoltativo. Se incluso, il parametro ha un valore massimo di 168 ore (una settimana).

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreTestingRecoveryPointSelection

Servizio: AWS Backup

`RecoveryPointSelection`ha cinque parametri (tre obbligatori e due opzionali). I valori specificati determinano quale punto di ripristino è incluso nel test di ripristino. È necessario indicare con `Algorithm` se si desidera utilizzare il punto di ripristino più recente `SelectionWindowDays` o se si desidera un punto di ripristino casuale e indicare attraverso `IncludeVaults` quali archivi è possibile scegliere i punti di ripristino.

`Algorithm`(obbligatorio) Valori validi: "`LATEST_WITHIN_WINDOW`" o "`RANDOM_WITHIN_WINDOW`».

`Recovery point types`(obbligatorio) Valori validi: "`SNAPSHOT`" e/o "`CONTINUOUS`». Include `SNAPSHOT` per ripristinare solo i punti di ripristino delle istantanee; include `CONTINUOUS` per ripristinare i punti di ripristino continui (point in time restore/PITR); utilizza entrambi per ripristinare un'istantanea o un punto di ripristino continuo. Il punto di ripristino sarà determinato dal valore di. `Algorithm`

`IncludeVaults`(richiesto). È necessario includere uno o più archivi di backup. Usa la wildcard ["*"] o ARN specifici.

`SelectionWindowDays`(opzionale) Il valore deve essere un numero intero (in giorni) compreso tra 1 e 365. Se non è incluso, il valore predefinito è. `30`

`ExcludeVaults`(opzionale). È possibile scegliere di inserire uno o più ARN di backup vault specifici per escludere il contenuto di tali vault dall'idoneità al ripristino. In alternativa, è possibile includere un elenco di selettori. Se questo parametro e il relativo valore non sono inclusi, il valore predefinito è un elenco vuoto.

Indice

Algorithm

I valori accettabili sono "LATEST_WITHIN_WINDOW" o "RANDOM_WITHIN_WINDOW"

- Tipo: stringa

Valori validi: `LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW`

Campo obbligatorio: no

ExcludeVaults

I valori accettati sono ARN specifici o un elenco di selettori. L'impostazione predefinita è un elenco vuoto se non specificato.

Tipo: matrice di stringhe

Campo obbligatorio: no

IncludeVaults

I valori accettati sono il carattere jolly ["*"] o ARN specifici oppure sostituzione del carattere jolly ["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf", ...] ["arn:aws:backup:*:*:backup-vault:asdf-*", ...]

Tipo: matrice di stringhe

Campo obbligatorio: no

RecoveryPointTypes

Questi sono i tipi di punto di ripristino.

Include `SNAPSHOT` per ripristinare solo i punti di ripristino delle istantanee; include `CONTINUOUS` per ripristinare i punti di ripristino continui (point in time restore/PITR); utilizza entrambi per ripristinare un'istantanea o un punto di ripristino continuo. Il punto di ripristino sarà determinato dal valore di. `Algorithm`

Tipo: matrice di stringhe

Valori validi: `CONTINUOUS | SNAPSHOT`

Campo obbligatorio: no

SelectionWindowDays

I valori accettati sono numeri interi compresi tra 1 e 365.

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreTestingSelectionForCreate

Servizio: AWS Backup

Contiene metadati relativi a una selezione specifica del test di ripristino.

ProtectedResourceType è obbligatorio, ad esempio Amazon EBS o Amazon EC2.

Consiste in `RestoreTestingSelectionName`, `ProtectedResourceType` e uno dei seguenti parametri:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Ogni tipo di risorsa protetta può avere un solo valore.

Una selezione di test di ripristino può includere un valore jolly ("*") per `ProtectedResourceArns` insieme a `ProtectedResourceConditions`. In alternativa, puoi includere fino a 30 ARN di risorse protette specifiche in `ProtectedResourceArns`.

Esempi di `ProtectedResourceConditions` sono `StringEquals` e `StringNotEquals`.

Indice

IamRoleArn

Il nome della risorsa Amazon (ARN) del ruolo IAM utilizzato da AWS Backup per creare la risorsa di destinazione, ad esempio `arn:aws:iam::123456789012:role/S3Access`.

Tipo: stringa

Campo obbligatorio: sì

ProtectedResourceType

Il tipo di AWS risorsa inclusa in una selezione di test di ripristino, ad esempio un volume Amazon EBS o un database Amazon RDS.

I tipi di risorsa supportati e accettati sono:

- `Aurora` per Amazon Aurora
- `DocumentDB` per Amazon DocumentDB (compatibile con MongoDB)

- `DynamoDB` per Amazon DynamoDB
- `EBS` per Amazon Elastic Block Store
- `EC2` per Amazon Elastic Compute Cloud
- `EFS` per Amazon Elastic File System
- `FSx` per Amazon FSx
- `Neptune` per Amazon Neptune
- `RDS` per Amazon Relational Database Service
- `S3` per Amazon S3

Tipo: stringa

Campo obbligatorio: sì

RestoreTestingSelectionName

Il nome univoco della selezione di test di ripristino che appartiene al relativo piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

ProtectedResourceArns

Ogni risorsa protetta può essere filtrata in base al relativo ARN specifico, ad esempio `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` o tramite un carattere jolly `ProtectedResourceArns: ["*"]`, ma non entrambi.

Tipo: matrice di stringhe

Campo obbligatorio: no

ProtectedResourceConditions

Se hai incluso il carattere jolly in ProtectedResourceArns, puoi includere condizioni relative alle risorse, ad esempio`ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]`.

Tipo: oggetto ProtectedResourceConditions

Campo obbligatorio: no

RestoreMetadataOverrides

È possibile sovrascrivere determinate chiavi di ripristino dei metadati includendo il parametro `RestoreMetadataOverrides` nel corpo di `RestoreTestingSelection`. I valori della chiave non fanno distinzione tra maiuscole e minuscole.

Consulta l'elenco completo dei metadati dedotti del test di ripristino.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

ValidationWindowHours

Il numero di ore (da 1 a 168) disponibili per eseguire uno script di convalida sui dati. I dati vengono eliminati al completamento dello script di convalida o alla fine del periodo di conservazione specificato, a seconda dell'evento che si verifica prima.

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreTestingSelectionForGet

Servizio: AWS Backup

Contiene metadati relativi a una selezione per il test di ripristino.

Indice

CreationTime

La data e l'ora in cui è stata creata la selezione per il test di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 201812:11:30.087.

Tipo: Timestamp

Campo obbligatorio: sì

IamRoleArn

Il nome della risorsa Amazon (ARN) del ruolo IAM utilizzato da AWS Backup per creare la risorsa di destinazione, ad esempio `arn:aws:iam::123456789012:role/S3Access`.

Tipo: stringa

Campo obbligatorio: sì

ProtectedResourceType

Il tipo di AWS risorsa inclusa in una selezione di test delle risorse, ad esempio un volume Amazon EBS o un database Amazon RDS.

Tipo: stringa

Campo obbligatorio: sì

RestoreTestingPlanName

RestoreTestingPlanName è una stringa univoca che è il nome del piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

RestoreTestingSelectionName

Il nome univoco della selezione del test di ripristino che appartiene al relativo piano di test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

CreatorRequestId

Identifica la richiesta e consente di riprovare le richieste non riuscite senza il rischio di eseguire l'operazione due volte. Se la richiesta include un `CreatorRequestId` che corrisponde a un piano di backup esistente, tale piano viene restituito. Questo parametro è facoltativo.

Se utilizzato, questo parametro deve contenere da 1 a 50 caratteri alfanumerici o '-_'. punti (.).

-Tipo: stringa

Campo obbligatorio: no

ProtectedResourceArns

Puoi includere ARN specifici, ad esempio `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, oppure puoi includere un carattere jolly `ProtectedResourceArns: ["*"]`, ma non entrambi.

Tipo: matrice di stringhe

Campo obbligatorio: no

ProtectedResourceConditions

In una selezione per il test delle risorse, questo parametro filtra in base a condizioni specifiche come `StringEquals` o `StringNotEquals`.

Tipo: oggetto ProtectedResourceConditions

Campo obbligatorio: no

RestoreMetadataOverrides

È possibile sovrascrivere determinate chiavi di ripristino dei metadati includendo il parametro `RestoreMetadataOverrides` nel corpo di `RestoreTestingSelection`. I valori della chiave non fanno distinzione tra maiuscole e minuscole.

Consulta l'elenco completo dei metadati dedotti del test di ripristino.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

ValidationWindowHours

Il numero di ore (da 1 a 168) disponibili per eseguire uno script di convalida sui dati. I dati vengono eliminati al completamento dello script di convalida o alla fine del periodo di conservazione specificato, a seconda dell'evento che si verifica prima.

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreTestingSelectionForList

Servizio: AWS Backup

Contiene metadati relativi a una selezione per il test di ripristino.

Indice

CreationTime

La data e l'ora in cui è stata creata la selezione per il test di ripristino, nel formato Unix e nell'ora UTC (Coordinated Universal Time). Il valore di `CreationTime` è preciso al millisecondo. Ad esempio, il valore 1516925490.087 rappresenta venerdì 26 gennaio 2018 12:11:30.087.

Tipo: Timestamp

Campo obbligatorio: sì

IamRoleArn

Il nome della risorsa Amazon (ARN) del ruolo IAM utilizzato da AWS Backup per creare la risorsa di destinazione, ad esempio `arn:aws:iam::123456789012:role/S3Access`.

Tipo: stringa

Campo obbligatorio: sì

ProtectedResourceType

Il tipo di AWS risorsa inclusa in una selezione di test di ripristino, ad esempio un volume Amazon EBS o un database Amazon RDS.

Tipo: stringa

Campo obbligatorio: sì

RestoreTestingPlanName

Stringa univoca che costituisce il nome del piano di test di ripristino.

Il nome non può essere modificato dopo la creazione. Il nome deve contenere solo caratteri alfanumerici e caratteri di sottolineatura. La lunghezza massima è 50 caratteri.

Tipo: stringa

Campo obbligatorio: sì

RestoreTestingSelectionName

Nome univoco di una selezione per il test di ripristino.

Tipo: stringa

Campo obbligatorio: sì

ValidationWindowHours

Questo valore rappresenta il periodo di tempo, in ore, di conservazione dei dati dopo un test di ripristino, in modo da poter completare la convalida facoltativa.

Il valore accettato è un numero intero compreso tra 0 e 168 (l'equivalente in ore di sette giorni).

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

RestoreTestingSelectionForUpdate

Servizio: AWS Backup

Contiene metadati relativi a una selezione per il test di ripristino.

Indice

IamRoleArn

Il nome della risorsa Amazon (ARN) del ruolo IAM utilizzato da AWS Backup per creare la risorsa di destinazione, ad esempio `arn:aws:iam::123456789012:role/S3Access`.

Tipo: stringa

Campo obbligatorio: no

ProtectedResourceArns

Puoi includere un elenco di ARN specifici, ad esempio `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, oppure puoi includere un carattere jolly `ProtectedResourceArns: ["*"]`, ma non entrambi.

Tipo: matrice di stringhe

Campo obbligatorio: no

ProtectedResourceConditions

Le condizioni che definisci per le risorse nel tuo piano di test di ripristino utilizzando i tag.

Ad esempio, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Gli operatori di condizione fanno distinzione tra maiuscole e minuscole.

Tipo: oggetto ProtectedResourceConditions

Campo obbligatorio: no

RestoreMetadataOverrides

È possibile sovrascrivere determinate chiavi di ripristino dei metadati includendo il parametro `RestoreMetadataOverrides` nel corpo di `RestoreTestingSelection`. I valori della chiave non fanno distinzione tra maiuscole e minuscole.

Consulta l'elenco completo dei metadati dedotti del test di ripristino.

Tipo: mappatura stringa a stringa

Campo obbligatorio: no

ValidationWindowHours

Questo valore rappresenta il periodo di tempo, in ore, di conservazione dei dati dopo un test di ripristino, in modo da poter completare la convalida facoltativa.

Il valore accettato è un numero intero compreso tra 0 e 168 (l'equivalente in ore di sette giorni).

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

AWS Backup gateway

I seguenti tipi di dati sono supportati da AWS Backup gateway:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails

- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

Servizio: AWS Backup gateway

Descrive un intervallo del limite di velocità della larghezza di banda per un gateway. Una pianificazione del limite di velocità della larghezza di banda è costituita da uno o più intervalli del limite di velocità della larghezza di banda. Un intervallo del limite di velocità della larghezza di banda definisce un periodo di tempo in uno o più giorni della settimana, durante il quale vengono specificati limiti di velocità della larghezza di banda per il caricamento, il download o entrambi.

Indice

DaysOfWeek

Il componente giorni della settimana dell'intervallo del limite di velocità della larghezza di banda, rappresentato da numeri ordinali da 0 a 6, dove 0 rappresenta la domenica e 6 il sabato.

Tipo: matrice di numeri interi

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 7 elementi.

Intervallo valido: valore minimo di 0. Valore massimo di 6.

Campo obbligatorio: sì

EndHourOfDay

L'ora del giorno in cui termina l'intervallo del limite di velocità della larghezza di banda.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 23.

Campo obbligatorio: sì

EndMinuteOfHour

Il minuto dell'ora in cui termina l'intervallo del limite di velocità della larghezza di banda.

> **Important**
>
> L'intervallo del limite di velocità della larghezza di banda termina alla fine del minuto. Per terminare un intervallo alla fine di un'ora, utilizza il valore 59.

Tipo: integer

Intervallo valido: valore minimo di 0. Valore massimo di 59.

Campo obbligatorio: sì

StartHourOfDay

L'ora del giorno in cui inizia l'intervallo del limite di velocità della larghezza di banda.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 23.

Campo obbligatorio: sì

StartMinuteOfHour

Il minuto dell'ora in cui inizia l'intervallo del limite di velocità della larghezza di banda. L'intervallo inizia all'inizio di tale minuto. Per iniziare un intervallo esattamente all'inizio dell'ora, utilizza il valore `0`.

Tipo: integer

Intervallo valido: valore minimo di 0. Valore massimo di 59.

Campo obbligatorio: sì

AverageUploadRateLimitInBitsPerSec

Il componente limite di velocità di caricamento media dell'intervallo del limite di velocità della larghezza di banda, in bit al secondo. Questo campo non viene visualizzato nella risposta se il limite di velocità di caricamento non è impostato.

Tipo: long

Intervallo valido: valore minimo di 51200. Valore massimo di 8000000000000.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Gateway

Servizio: AWS Backup gateway

Un gateway è un'appliance AWS Backup Gateway che funziona sulla rete del cliente per fornire una connettività perfetta allo storage di backup nel AWS cloud.

Indice

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway. Utilizza l'`ListGateways`operazione per restituire un elenco di gateway per il tuo account e. Regione AWS

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: no

GatewayDisplayName

Il nome visualizzato del gateway.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

GatewayType

Il tipo del gateway.

- Tipo: stringa

Valori validi: `BACKUP_VM`

Campo obbligatorio: no

HypervisorId

L'ID hypervisor del gateway.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Campo obbligatorio: no

LastSeenTime

L'ultima volta che il AWS Backup gateway ha comunicato con il gateway, in formato Unix e ora UTC.

Tipo: Timestamp

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

GatewayDetails

Servizio: AWS Backup gateway

I dettagli del gateway.

Indice

GatewayArn

Il nome della risorsa Amazon (ARN) del gateway. Utilizza l'operazione `ListGateways` per restituire un elenco di gateway per l'account e la Regione AWS.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. Lunghezza massima di 180.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: no

GatewayDisplayName

Il nome visualizzato del gateway.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

GatewayType

Il tipo del tipo di gateway.

- Tipo: stringa

Valori validi: `BACKUP_VM`

Campo obbligatorio: no

HypervisorId

L'ID hypervisor del gateway.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Campo obbligatorio: no

LastSeenTime

Dettagli che mostrano l'ultima volta che il AWS Backup gateway ha comunicato con il cloud, in formato Unix e ora UTC.

Tipo: Timestamp

Campo obbligatorio: no

MaintenanceStartTime

Restituisce l'ora di inizio della manutenzione settimanale del gateway, incluso il giorno della settimana. Nota che i valori sono espressi in termini del fuso orario del gateway. Può essere settimanale o mensile.

Tipo: oggetto MaintenanceStartTime

Campo obbligatorio: no

NextUpdateAvailabilityTime

Dettagli che mostrano l'ora di disponibilità del gateway per il prossimo aggiornamento.

Tipo: Timestamp

Campo obbligatorio: no

VpcEndpoint

Il nome DNS dell'endpoint del cloud privato virtuale (VPC) utilizzato dal gateway per connettersi al cloud per il backup gateway.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Hypervisor

Servizio: AWS Backup gateway

Rappresenta le autorizzazioni dell'hypervisor a cui si connetterà il gateway.

Un hypervisor è un hardware, software o firmware che crea e gestisce macchine virtuali e alloca risorse alle stesse.

Indice

Host

L'host del server dell'hypervisor. Può essere un indirizzo IP o un nome dominio completo (FQDN).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 128 caratteri.

Modello: `^.+$`

Campo obbligatorio: no

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: no

KmsKeyArn

L'Amazon Resource Name (ARN) AWS Key Management Service utilizzato per crittografare l'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Campo obbligatorio: no

Name

Il nome dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

State

Lo stato dell'hypervisor.

- Tipo: stringa

Valori validi: `PENDING | ONLINE | OFFLINE | ERROR`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta AWS quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

HypervisorDetails

Servizio: AWS Backup gateway

Questi sono i dettagli dell'hypervisor specificato. Un hypervisor è un hardware, software o firmware che crea e gestisce macchine virtuali e alloca risorse alle stesse.

Indice

Host

L'host del server dell'hypervisor. Può essere un indirizzo IP o un nome dominio completo (FQDN).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 128 caratteri.

Modello: `^.+$`

Campo obbligatorio: no

HypervisorArn

Il nome della risorsa Amazon (ARN) dell'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: no

KmsKeyArn

Il nome della risorsa Amazon (ARN) della AWS KMS utilizzata per crittografare l'hypervisor.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Campo obbligatorio: no

LastSuccessfulMetadataSyncTime

Questa è l'ora dell'ultima sincronizzazione riuscita dei metadati.

Tipo: Timestamp

Campo obbligatorio: no

LatestMetadataSyncStatus

Questo è lo stato più recente per la sincronizzazione dei metadati indicata.

- Tipo: stringa

Valori validi: `CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED`

Campo obbligatorio: no

LatestMetadataSyncStatusMessage

Questo è lo stato più recente per la sincronizzazione dei metadati indicata.

- Tipo: stringa

Campo obbligatorio: no

LogGroupArn

Il nome della risorsa Amazon (ARN) del gruppo di gateway all'interno del log richiesto.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Modello: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Campo obbligatorio: no

Name

Questo è il nome dell'hypervisor specificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

State

Questo è lo stato corrente dell'hypervisor specificato.

Gli stati possibili sono `PENDING`, `ONLINE`, `OFFLINE` o `ERROR`.

-Tipo: stringa

Valori validi: `PENDING | ONLINE | OFFLINE | ERROR`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

MaintenanceStartTime

Servizio: AWS Backup gateway

Questa è l'ora di inizio della manutenzione settimanale del gateway, incluso il giorno e l'ora della settimana. Nota che i valori sono espressi in termini del fuso orario del gateway. Può essere settimanale o mensile.

Indice

HourOfDay

La componente oraria dell'ora di inizio della manutenzione è rappresentata come hh, in cui hh è l'ora (da 0 a 23). L'ora del giorno è espressa nel fuso orario del gateway.

Tipo: integer

Intervallo valido: valore minimo di 0. valore massimo pari a 23.

Campo obbligatorio: sì

MinuteOfHour

La componente in minuti dell'ora di inizio della manutenzione è rappresentata come mm, in cui mm è il minuto (da 0 a 59). Il minuto dell'ora è espresso nel fuso orario del gateway.

Tipo: integer

Intervallo valido: valore minimo di 0. Valore massimo di 59.

Campo obbligatorio: sì

DayOfMonth

Il componente giorno del mese dell'ora di inizio della manutenzione rappresentato come un numero ordinale compreso tra 1 e 28, dove 1 rappresenta il primo giorno del mese e 28 rappresenta l'ultimo giorno del mese.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 31.

Campo obbligatorio: no

DayOfWeek

Un numero ordinale compreso tra 0 e 6 che rappresenta il giorno della settimana, dove 0 rappresenta la domenica e 6 rappresenta il sabato. Il giorno della settimana è espresso nel fuso orario del gateway.

Tipo: integer

Intervallo valido: valore minimo di 0. Valore massimo di 6.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Tag

Servizio: AWS Backup gateway

Una coppia chiave-valore che puoi utilizzare per gestire, filtrare e cercare le risorse. I caratteri consentiti includono lettere UTF-8, numeri, spazi e i caratteri seguenti: + - = . _ : /.

Indice

Key

La parte chiave della coppia chiave-valore di un tag. La chiave non può iniziare con `aws:`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Campo obbligatorio: sì

Value

La parte valore della coppia chiave-valore di un tag.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[^\x00]*$`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

VirtualMachine

Servizio: AWS Backup gateway

Una macchina virtuale che si trova su un hypervisor.

Indice

HostName

Il nome host della macchina virtuale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

HypervisorId

L'ID dell'hypervisor della macchina virtuale.

- Tipo: stringa

Campo obbligatorio: no

LastBackupDate

La data più recente in cui è stato eseguito il backup di una macchina virtuale, in formato Unix e nell'ora UTC.

Tipo: Timestamp

Campo obbligatorio: no

Name

Il nome della macchina virtuale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

Path

Il percorso della macchina virtuale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 4096.

Modello: `^[^\x00]+$`

Campo obbligatorio: no

ResourceArn

Il nome della risorsa Amazon (ARN) della macchina virtuale. Ad esempio, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

VirtualMachineDetails

Servizio: AWS Backup gateway

Gli oggetti `VirtualMachine`, ordinati in base ai nomi delle risorse Amazon (ARN).

Indice

HostName

Il nome host della macchina virtuale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

HypervisorId

L'ID dell'hypervisor della macchina virtuale.

- Tipo: stringa

Campo obbligatorio: no

LastBackupDate

La data più recente in cui è stato eseguito il backup di una macchina virtuale, in formato Unix e nell'ora UTC.

Tipo: Timestamp

Campo obbligatorio: no

Name

Il nome della macchina virtuale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 100.

Modello: `^[a-zA-Z0-9-]*$`

Campo obbligatorio: no

Path

Il percorso della macchina virtuale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 4096.

Modello: `^[^\x00]+$`

Campo obbligatorio: no

ResourceArn

Il nome della risorsa Amazon (ARN) della macchina virtuale. Ad esempio, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 50. La lunghezza massima è 500 caratteri.

Modello: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Campo obbligatorio: no

VmwareTags

Questi sono i dettagli dei tag VMware associati alla macchina virtuale specificata.

Tipo: matrice di oggetti VmwareTag

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

VmwareTag

Servizio: AWS Backup gateway

Un tag VMware è un tag collegato a una macchina virtuale specifica. Un tag è una coppia chiave-valore che puoi utilizzare per gestire, filtrare e cercare le risorse.

Il contenuto dei tag VMware può essere abbinato ai tag. AWS

Indice

VmwareCategory

Questa è la categoria di VMware.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 80.

Campo obbligatorio: no

VmwareTagDescription

Questa è una descrizione definita dall'utente di un tag VMware.

- Tipo: stringa

Campo obbligatorio: no

VmwareTagName

Questo è il nome definito dall'utente di un tag VMware.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 80.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- AWS SDK per C++

- AWS SDK per Java V2
- AWS SDK per Ruby V3

VmwareToAwsTagMapping

Servizio: AWS Backup gateway

Questo mostra la mappatura dei tag VMware ai tag corrispondenti. AWS

Indice

AwsTagKey

La parte fondamentale della coppia chiave-valore del AWS tag.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Campo obbligatorio: sì

AwsTagValue

La parte relativa al valore della coppia chiave-valore del AWS tag.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `^[^\x00]*$`

Campo obbligatorio: sì

VmwareCategory

Questa è la categoria di VMware.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 80.

Campo obbligatorio: sì

VmwareTagName

Questo è il nome definito dall'utente di un tag VMware.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 80.

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Parametri comuni

L'elenco seguente contiene i parametri utilizzati da tutte le azioni per firmare le richieste di Signature Version 4 con una stringa di query. Qualsiasi parametro specifico di un'operazione è riportato nell'argomento relativo all'operazione. Per ulteriori informazioni sull'utilizzo di Signature Version 4, consulta la pagina Firma delle richieste API AWS nella Guida per l'utente di IAM.

Action

azione da eseguire.

Tipo: stringa

Campo obbligatorio: sì

Version

Versione dell'API per cui è scritta la richiesta, espressa nel formato AAAA-MM-GG.

Tipo: stringa

Campo obbligatorio: sì

X-Amz-Algorithm

Algoritmo hash utilizzato per creare la firma della richiesta.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Valori validi: `AWS4-HMAC-SHA256`

Obbligatorio: condizionale

X-Amz-Credential

Il valore dell'ambito delle credenziali, che è una stringa che include la chiave di accesso, la data, la regione di destinazione, il servizio richiesto e una stringa di terminazione ("aws4_request"). Il valore viene espresso nel seguente formato: chiave_accesso/AAAAMMGG/regione/servizio/aws4_request.

Per ulteriori informazioni, consulta la pagina Creazione di una richiesta API AWS firmata nella Guida per l'utente di IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Date

La data utilizzata per creare la firma. Il formato deve essere il formato di base ISO 8601 (YYYYMMDD'T'HHMMSS'Z'). Ad esempio, la seguente combinazione data/ora è un valore X-Amz-Date valido: `20120325T120000Z`.

Condition: X-Amz-Date è facoltativo per tutte le richieste; può essere utilizzato per sovrascrivere la data utilizzata per firmare le richieste. Se l'intestazione Date è specificata nel formato base ISO 8601, X-Amz-Date non è richiesto. Quando utilizzi X-Amz-Date, sostituisce sempre il valore dell'intestazione Date. Per ulteriori informazioni, consulta la pagina Elementi di una firma di richiesta API AWS nella Guida per l'utente di IAM.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Security-Token

Il token di sicurezza provvisorio ottenuto tramite una chiamata ad AWS Security Token Service (AWS STS). Per un elenco di servizi che supportano le credenziali di sicurezza temporanee da

AWS STS, consulta la pagina Servizi AWS che funzionano con IAM nella Guida per l'utente di IAM.

Condizione: se utilizzi le credenziali di sicurezza temporanee fornite da AWS STS, devi includere il token di sicurezza.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Signature

Specifica la firma con codifica esadecimale calcolata dalla stringa da firmare e dalla chiave di firma derivata.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-SignedHeaders

Specifica tutte le intestazioni HTTP incluse come parte della richiesta canonica. Per ulteriori informazioni sulla specifica delle intestazioni firmate, consulta la pagina Creazione di una richiesta API AWS firmata nella Guida per l'utente di IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

Errori comuni

In questa sezione sono riportati gli errori comuni delle azioni API per tutti i servizi AWS. Per gli errori specifici di un'azione API per questo servizio, consulta l'argomento per quell'azione API.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

IncompleteSignature

La firma della richiesta non è conforme agli standard AWS.

Codice di stato HTTP: 400

InternalFailure

L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto interno sconosciuto.

Codice di stato HTTP: 500

InvalidAction

L'azione o l'operazione richiesta non è valida. Verifica che l'operazione sia digitata correttamente.

Codice di stato HTTP: 400

InvalidClientTokenId

Il certificato X.509 o l'ID chiave di accesso AWS forniti non sono presenti nei nostri record.

Codice di stato HTTP: 403

NotAuthorized

Non disponi delle autorizzazioni per eseguire questa azione.

Codice di stato HTTP: 400

OptInRequired

L'ID chiave di accesso AWS necessita di una sottoscrizione al servizio.

Codice di stato HTTP: 403

RequestExpired

La richiesta ha raggiunto il servizio più di 15 minuti dopo il date stamp della richiesta o più di 15 minuti dopo la data di scadenza della richiesta (ad esempio per URL prefirmati) oppure il date stamp della richiesta è più di 15 minuti nel futuro.

Codice di stato HTTP: 400

ServiceUnavailable

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 503

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

ValidationError

L'input non riesce a soddisfare i vincoli specificati da un servizio AWS.

Codice di stato HTTP: 400

Cronologia dei documenti per AWS Backup

- Versione API: 6 dicembre 2023
- Ultimo aggiornamento della documentazione: 3 giugno 2024

La tabella seguente elenca tutti AWS Backup i lanci dal lancio del servizio nel gennaio 2019 a oggi. Per ricevere notifiche sugli aggiornamenti della documentazione, puoi effettuare la sottoscrizione al feed RSS precedente.

Modifica	Descrizione	Data
AWS Backup funzionalità Espansione regionale	AWS Backup il supporto del livello di archiviazione degli snapshot di Amazon EBS è ora disponibile nelle seguenti regioni: • Cina (Pechino) • Cina (Ningxia) • AWS GovCloud (Stati Uniti occidentali) • AWS GovCloud (Stati Uniti orientali)	3 giugno 2024
Policy gestite da AWS aggiornate	AWS Backup ha aggiunto l'autorizzazione `backup:TagResource` alle seguenti politiche gestite: • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup	17 maggio 2024

Modifica	Descrizione	Data
	Per ulteriori informazioni, consulta Aggiornamenti delle politiche.	
AWS Backup ora disponibile nella regione Canada occidentale (Calgary)	Il backup e il ripristino per molti tipi di risorse sono ora disponibili in Regione AWS Canada occidentale (Calgary). Per le funzionalità di backup compatibili, vedi Disponibilità delle funzionalità di Regione AWS. Per i tipi di risorse supportati, vedi Servizi supportati da Regione AWS.	14 marzo 2024
Autorizzazioni aggiunte alla politica gestita	AWS Backup ha aggiornato la politica AWSServiceRolePolicyForBackupRestoreTestingaggiungendo autorizzazioni per supportare tipi di risorse aggiuntivi all'interno della funzionalità di test di ripristino. Per ulteriori informazioni sulle autorizzazioni specifiche aggiunte, consulta Aggiornamenti delle politiche.	14 febbraio 2024

Modifica	Descrizione	Data
Supporto di backup e ripristino per volumi FSx for ONTAP FlexGroup	AWS Backup ora supporta il backup e il ripristino dei FlexGroup volumi FSx for ONTAP nella maggior parte dei casi. Regioni AWS Per ulteriori informazioni, consulta Ripristino di un file system Amazon FSx. .	10 gennaio 2024
Supporto di backup e ripristino per SAP HANA HA	AWS Backup ora offre supporto ai database SAP HANA High Availability per il backup e il ripristino di Amazon EC2. Per ulteriori informazioni, consulta Database SAP HANA su backup di istanze Amazon EC2 e Restoring an SAP HANA High Availability system.	21 dicembre 2023
AWS Backup Controllo Audit Manager per i test di ripristino	AWS Backup Audit Manager ora offre il controllo Restore time for resources meet target per facilitare il monitoraggio dei tempi di ripristino. Questo controllo verifica se il tempo di ripristino di una risorsa soddisfa la durata prevista. Per ulteriori informazioni, consulta Controlli e correzioni e Audit del test di ripristino.	18 dicembre 2023

Modifica	Descrizione	Data
Supporto per l'archiviazione a freddo di Amazon EBS	AWS Backup ora supporta la transizione dei backup EBS dalla conservazione a caldo a quella a freddo. Per ulteriori informazioni, consulta la pagina • Livello di archiviazione di Amazon EBS per l'archiviazione a freddo • Ciclo di vita e livelli di archiviazione • Creazione di un piano di backup	27 novembre 2023
Introduzione al test di ripristino	AWS Backup introduce il test di ripristino, che offre una valutazione automatizzata e periodica della fattibilità del ripristino, nonché la possibilità di monitorare i tempi di durata dei processi di ripristino. Per ulteriori informazioni, consulta Test di ripristino.	27 novembre 2023

Modifica	Descrizione	Data
Policy gestite da AWS aggiornate	AWS Backup ha aggiunto le autorizzazioni `ec2:DescribeSnapshotTierStatus` e le politiche gestite `eec2:ModifySnapshotTier` . `AWSBackupServiceRolePolicyForBackups` `AWSBackupServiceLinkedRolePolicyForBackup` AWS Backup ha inoltre aggiunto le autorizzazioni `ec2:DescribeSnapshotTierStatus` e la politica `ec2:RestoreSnapshotTier` gestita. `AWSBackupServiceRolePolicyForRestores` Queste autorizzazioni sono necessarie affinché gli utenti abbiano la possibilità di trasferire le risorse Amazon EBS archiviate AWS Backup allo storage di archiviazione e di ripristinare le risorse dal livello di archiviazione. Per ulteriori informazioni, consulta Aggiornamenti delle policy.	27 novembre 2023

Modifica	Descrizione	Data
È stata aggiunta l'autorizzazione al passaggio di ruoli per supportare il test di ripristino.	AWS Backup aggiunto a and`restore-testing.backup.amazonaws.com` . `IamPassRolePermissions` `IamCreateServiceLinkedRolePermissions` Questa aggiunta è necessaria per AWS Backup eseguire test di ripristino per conto dei clienti.	27 novembre 2023

Modifica	Descrizione	Data
È stato aggiunto un nuovo ruolo collegato ai servizi	AWS Backup ha aggiunto il nuovo ruolo collegato al servizio denominato `AWSServiceRoleForBackupRestoreTesting`, che fornisce le autorizzazioni di backup per eseguire i test di ripristino. Questo nuovo ruolo collegato al servizio fornisce le autorizzazioni necessarie per eseguire AWS Backup i test di ripristino. Le autorizzazioni includono le azioni `list, read, and write` per i seguenti servizi da includere nei test di ripristino: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx for Lustre, FSx for Windows File Server, FSx for ONTAP, FSx for OpenZFS, Amazon Neptune, Amazon RDS e Amazon S3.	27 novembre 2023

Modifica	Descrizione	Data
Nuovo pannello di controllo delle metriche relative ai lavori nella console AWS Backup	La AWS Backup console ora mostra una dashboard dei lavori, che semplifica il monitoraggio dello stato dei backup su larga scala con una nuova interfaccia utente visiva e metriche aggregate di backup, copia e ripristino per i servizi supportati da. AWS Backup La dashboard dei lavori è disponibile in tutte le regioni in cui è disponibile AWS Backup Audit Manager. Le regioni non elencate potranno comunque accedere alla CloudWatch dashboard. Per ulteriori informazioni, consulta AWS Backup console dashboards.	15 novembre 2023
Supporto per backup di stack nidificati	AWS Backup ha ampliato il supporto per il backup delle AWS CloudFormation risorse. Gli stack di CloudFormation applicazioni che contengono stack annidati al loro interno possono essere inclusi nei backup. Per ulteriori informazioni, consulta Backup degli stack CloudFormation .	8 novembre 2023

Modifica	Descrizione	Data
Supporto per Amazon S3 in Cina (Pechino) e Cina (Ningxia).	AWS Backup il supporto per Amazon S3 è ora disponibile nelle regioni di Cina (Pechino) e Cina (Ningxia). Per ulteriori informazioni, consulta Disponibilità delle funzionalità tramite Regione.	26 ottobre 2023
Support per backup continui e ripristino P di Amazon Aurora oint-in-time	AWS Backup ora supporta backup e point-in-time ripristin o continui (PITR) per le risorse Aurora. Per ulteriori informazioni, consulta Backup continui e ripristino IP. oint-in-time	7 settembre 2023
AWS CloudFormation gli stack supportano l'esclusione di risorse	AWS Backup ora supporta l'opzione di escludere le risorse scelte dallo stack. AWS CloudFormation Per ulteriori informazioni, consulta Backup degli stack AWS CloudFormation.	6 settembre 2023
Regole del piano di backup introducono flessibilità del fuso orario	AWS Backup le regole del piano ora possono avere un fuso orario specifico per le finestre di backup. Per ulteriori informazioni, consulta Gestione dei piani di backup.	28 agosto 2023

Modifica	Descrizione	Data
AWS Backup ora disponibile nella regione di Israele (Tel Aviv)	Molte AWS Backup funzionalità sono ora disponibili nella nuova regione di Israele (Tel Aviv). Per vedere quali risorse sono supportate, visita Disponibilità delle funzionalità tramite Regione AWS.	22 agosto 2023
AWS Backup Audit Manager ora supporta gli account di amministratore delegato	AWS Backup È ora possibile accedere alla generazione di report Audit Manager tramite account amministrativi delegati. Per ulteriori informazioni, consulta la pagina • Controlla i backup e crea report con AWS Backup Audit Manager • Utilizzo dei report di audit • Amministratore delegato	16 agosto 2023
Anteprima del vault di backup logicamente isolato	AWS Backup ora offre un'anteprima di un nuovo tipo di archivio di backup per aiutare a integrare le operazioni di protezione dei dati. Per ulteriori informazioni, consulta Vault logicamente isolati (anteprima).	8 agosto 2023

Modifica	Descrizione	Data
AWS Backup migliora i backup di Amazon S3	AWS Backup offre funzionalità migliorate in termini di prestazioni, dimensioni e velocità per i backup con bucket S3. Per ulteriori informazioni, consulta Backup di Amazon S3.	1° agosto 2023
Funzionalità Tag-on-Restore ora disponibile nelle regioni Cina	I tag che fanno parte di un backup possono ora essere copiati quando si crea un processo di ripristino nelle regioni Cina (Pechino) o Cina (Ningxia). Per ulteriori informazioni, consulta Copia i tag durante un ripristino.	17 luglio 2023
AWS Backup ora supporta Amazon S3 in altre regioni	AWS Backup il supporto per Amazon S3 è ora disponibile nelle regioni di Europa (Spagna), Europa (Zurigo), Asia Pacifico (Hyderabad) e Asia Pacifico (Melbourne). Per ulteriori informazioni, consulta Disponibilità delle funzionalità tramite Regione.	6 luglio 2023

Modifica	Descrizione	Data
Copia tra account si espande in altre regioni	AWS Backup ora supporta la copia di backup su più account della maggior parte delle risorse nelle seguenti regioni: Asia Pacifico (Giacarta), Medio Oriente (Bahrein), Asia Pacifico (Hong Kong), Africa (Città del Capo), Europa (Milano), Asia Pacifico (Osaka), Medio Oriente (Emirati Arabi Uniti), Europa (Spagna), Europa (Zurigo), Asia Pacifico (Hyderabad) e Asia Pacifico (Melbourne). Per ulteriori informazioni, consulta Disponibilità delle funzionalità tramite Regione	5 luglio 2023
Backup Audit Manager disponibile nelle GovCloud aree geografiche	AWS Backup ha ampliato AWS Backup Audit Manager in AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali). Per ulteriori informazioni, consulta Disponibilità delle funzionalità tramite Regione	29 giugno 2023

Modifica	Descrizione	Data
La gestione tra account è ora disponibile nelle regioni GovCloud	AWS Backup ora supporta la gestione delle risorse tra account in AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali). Per ulteriori informazioni, consulta Gestione delle risorse AWS Backup in più account AWS.	29 giugno 2023
Supporto per copie tra regioni di Amazon Aurora in altre regioni	AWS Backup ora supporta copie di backup interregionali per i cluster Aurora da e verso le seguenti regioni: Asia Pacifico (Giacarta), Medio Oriente (Bahrain), Asia Pacifico (Hong Kong), Africa (Città del Capo), Europa (Milano), Medio Oriente (Emirati Arabi Uniti), Europa (Spagna), Europa (Zurigo), Asia Pacifico (Hyderabad) e Asia Pacifico (Melbourne).	5 giugno 2023
Copia dei tag durante il ripristino	I tag che fanno parte di un backup possono ora essere copiati quando si crea un processo di ripristino. Per ulteriori informazioni, consulta Copia i tag durante un ripristino.	22 maggio 2023

Modifica	Descrizione	Data
AWS Backup si integra con le notifiche utente AWS	Ora puoi scegliere di ricevere notifiche correlate a eventi di backup, copia e ripristino tramite la console Notifiche AWS agli utenti. Per ulteriori informazioni, consulta Guida introduttiva alle notifiche AWS utente.	10 maggio 2023
Backup tra regioni disponibili in quattro nuove regioni	AWS Backup ora supporta il backup interregionale nella regione del Medio Oriente (Emirati Arabi Uniti), nella regione Europa (Spagna), nella regione Europa (Zurigo) e nella regione Asia Pacifico (Hyderabad).	28 aprile 2023
Supporto esteso per la copia in più regioni AWS Backup	I backup tra regioni delle risorse Amazon EFS, VMware e DynamoDB possono ora essere eseguiti nelle seguenti regioni: Asia Pacific (Giacarta), Medio Oriente (Bahrein), Asia Pacifico (Hong Kong), Africa (Città del Capo) ed Europa (Milano).	28 aprile 2023

Modifica	Descrizione	Data
Backup e ripristino di Amazon S3 nella regione Sud America (San Paolo)	AWS Backup il supporto per Amazon S3 (Amazon Simple Storage Service) è ora disponibile nella regione del Sud America (San Paolo). Per ulteriori informazioni, consulta Backup di Amazon S3.	20 aprile 2023
AWS Backup si espande nella regione Asia Pacifico (Melbourne)	AWS Backup è ora disponibi le nella regione Asia Pacifico (Melbourne). Per ulteriori informazioni, consulta Disponibilità delle funzionalità per AWS regione.	20 aprile 2023
Supporto regionale esteso per Amazon S3	AWS Backup il supporto per Amazon S3 (Amazon Simple Storage Service) è ora disponibile nelle regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali) Per ulteriori informazioni, consulta Backup di Amazon S3.	19 aprile 2023

Modifica	Descrizione	Data
Backup e ripristino di database SAP HANA su istanze Amazon EC2	AWS Backup ora offre la possibilità di eseguire il backup e il ripristino dei database SAP HANA in esecuzione su istanze Amazon EC2 nella maggior parte delle regioni. Per ulteriori informazioni, consulta Database SAP HANA su backup di istanze Amazon EC2.	17 aprile 2023
AWS Backup ora disponibile nelle regioni Europa (Spagna), Europa (Zurigo) e Asia Pacifico (Hyderabad)	AWS Backup il supporto è stato esteso a nuove regioni, tra cui Europa (Spagna), Europa (Zurigo) e Asia Pacifico (Hyderabad). È possibile eseguire il backup e il ripristino delle risorse supportate all'interno di queste regioni. Per ulteriori informazioni, consulta Disponibilità delle funzionalità per AWS regione.	13 aprile 2023

Modifica	Descrizione	Data
Politica AWS gestita aggiornata a `AWSBackupAuditAccess`	Politica AWS gestita aggiornata a AWSBackupAuditAccess. AWS Backup ha sostituito la selezione delle risorse all'interno dell'API `config:DescribeComplianceByConfigRule` con una risorsa wildcard. Per ulteriori informazioni, consulta Aggiornamenti delle policy per AWS Backup.	11 aprile 2023
Hypervisor con Amazon Logs CloudWatch	AWS Backup gli utenti del gateway possono ora integrare gli hypervisor con CloudWatch Logs per gestire i log. Per ulteriori informazioni, vedere Modifica della configurazione di un hypervisor e dei log. CloudWatch	29 marzo 2023
Supporto regionale esteso per Amazon S3	AWS Backup il supporto per Amazon S3 è ora disponibile nelle regioni di Asia Pacifico (Giacarta) e Medio Oriente (Emirati Arabi Uniti).	22 marzo 2023

Modifica	Descrizione	Data
Miglioramento del backup incrementale delle macchine virtuali	I backup di macchine virtuali VMware che presentan o problemi con i dati CBT (Changed Block Tracking) contengono ora informazi oni aggiuntive per aiutare a correggere e risolvere i problemi. Per ulteriori informazioni, consulta Backup incrementali di macchine virtuali e Risoluzio ne dei problemi relativi alle macchine virtuali.	15 marzo 2023
AWS Backup supporto per più adattatori di rete	AWS Backup gateway ora supporta la configurazione di più adattatori di rete Per ulteriori informazioni sulla configurazione degli adattator i di rete, consulta Configura il gateway per più NIC in VMware nella Guida per gli sviluppatori di AWS Backup .	8 marzo 2023
AWS Backup supporto per vSphere 8	AWS Backup ora supporta il backup e il ripristino di macchine virtuali eseguite su VMware vSphere 8. Per ulteriori informazioni sulle opzioni VMware supportate, consulta VM supportate nella Guida per gli sviluppatori di AWS Backup .	8 marzo 2023

Modifica	Descrizione	Data
AWS Backup Audit Manager supporta i backup Amazon RDS Multi-AZ	Backup Audit Manager offre ora il supporto per zone il backup di disponibilità multiple di Amazon Relational Database Service. Per ulteriori informazioni, vedi come controllare i backup e creare report con AWS Backup Audit Manager.	1 febbraio 2023
AWS Backup offre backup incrementale per le tabelle Amazon Timestream	AWS Backup ora offre funzionalità di backup estese per i backup Timestream. I piani di backup ora possono eseguire backup incrementali per ridurre il tempo richiesto per eseguire il backup delle risorse Timestream e i costi di storage. Per ulteriori informazioni, consulta Backup di Amazon Timestream.	23 gennaio 2023
AWS Backup ora disponibile a Dubai	AWS Backup si è estesa alla regione del Medio Oriente (Emirati Arabi Uniti). È possibile eseguire il backup e il ripristino delle risorse supportate all'interno di questa regione.	17 gennaio 2023

Modifica	Descrizione	Data
Copia tra regioni disponibile in altre regioni	AWS Backup ora offre backup interregionali nella regione Asia Pacifico (Giacarta), Medio Oriente (Bahrein), Asia Pacifico (Hong Kong), Africa (Città del Capo) ed Europa (Milano) per la maggior parte delle risorse. Per ulteriori informazioni, consulta Creazione di copie di backup tra Regioni AWS.	21 dicembre 2022
Limitazione (della larghezza di banda della rete) e limiti della larghezza di banda del Backup Gateway	AWS Backup Gateway ora consente di limitare la velocità di upload dai gateway per controllare la quantità di larghezza AWS Backup di banda di rete utilizzata dal gateway. Per supportare questa funzionalità, AWS Backup ha creato e aggiornato le politiche gestite, tra cui e. `AWSBackupFullAccess` `AWSBackupOperatorAccess` Per ulteriori informazioni, consulta Limitazione della larghezza di banda del Backup Gateway.	15 dicembre 2022

Modifica	Descrizione	Data
Supporto per i tag VMware del Backup Gateway	AWS Backup Gateway ora supporta i tag VMware. Gli utenti dispongono della flessibilità aggiuntiva necessaria per creare AWS tag che corrispondano ai tag utilizzati per le macchine virtuali. Per supportare questa funzionalità, AWS Backup ha creato e aggiornato le politiche gestite, tra cui `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` `AWSBackupFullAccess` , `eAWSBackupOperatorAccess` . Per ulteriori informazioni, consulta Tag VMware.	15 dicembre 2022
AWS Backup supporto per Amazon Timestream	AWS Backup ora supporta il backup e il ripristino delle tabelle Amazon Timestream. Per ulteriori informazioni, consulta Backup di Amazon Timestream.	13 dicembre 2022

Modifica	Descrizione	Data
AWS Backup offre Legal Hold	AWS Backup introduce un nuovo strumento per aiutare a proteggere i punti di ripristino tramite una custodia legale. Per ulteriori informazioni, consulta Blocco a fini legali.	27 novembre 2022
AWS Backup Audit Manager Reporting su più regioni e tra account	AWS Backup Audit Manager offre funzionalità aggiuntive alla conformità e ai report sulle mansioni. Gli utenti possono generare report che incorporano più regioni e più account. Per ulteriori informazioni, consulta Utilizzo di report di audit.	27 novembre 2022
AWS Backup supporta Amazon Redshift	AWS Backup ora offre supporto per il backup di cluster Amazon Redshift e per il ripristino di cluster e tabelle Amazon Redshift. Per ulteriori informazioni, consulta Backup di Amazon Redshift.	27 novembre 2022

Modifica	Descrizione	Data
AWS Backup offre supporto per gli stack di applicazioni di backup AWS CloudFormation	AWS Backup offre la capacità di eseguire il backup CloudFormation e il ripristino di applicazioni contenenti più risorse eseguendo il backup di uno stack e ripristinando le risorse al suo interno. Per ulteriori informazioni, consulta Backup degli stack di applicazioni.	27 novembre 2022
AWS Backup offre account amministrativi delegati e delega delle politiche di backup	AWS Backup gli account registrati AWS Organizations possono designare gli account dei membri come account di amministratore delegato. Per ulteriori informazioni, vedere Gestione di più account con. AWS Organizations	27 novembre 2022

Modifica	Descrizione	Data
Anteprima pubblica del backup e del ripristino di SAP HANA su istanze Amazon EC2	AWS Backup e AWS Backint offrono un'anteprima pubblica integrata delle funzionalità per il backup e il ripristino dei database SAP HANA su istanze EC2. Per ulteriori informazioni, consulta l'anteprima pubblica di SAP HANA su istanze Amazon EC2. Per supportare questa anteprima, AWS Backup ha fornito aggiornamenti delle policy e nuove AWS Managed Policies per queste funzionalità.	20 novembre 2022
Ripristino di VMware su istanze Amazon EC2	AWS Backup ora offre la possibilità di ripristinare le macchine virtuali su istanze Amazon EC2, oltre alla possibilità di ripristinare le macchine su EBS, VMware, VMware Cloud on e VMware Cloud on. AWS AWS Outposts Per ulteriori informazioni, consulta la documentazione su come utilizzare la console per ripristinare i punti di ripristino delle macchine virtuali. AWS Backup	9 novembre 2022

Modifica	Descrizione	Data
Funzionalità AWS Backup Vault Lock estesa	AWS Backup Vault Lock può ora essere creato in modalità di governance per ulteriori protezioni IAM o in modalità di conformità per garantire l'immutabilità. Ulteriori informazioni sono disponibili in Vault Lock di AWS Backup.	4 ottobre 2022
AWS Backup Audit Manager ora disponibile nella regione Africa (Città del Capo) e nella regione Europa (Milano)	AWS Backup Audit Manager si è esteso alla regione Africa (Città del Capo) e alla regione Europa (Milano). Per ulteriori informazioni su Backup Audit Manager, vedere Controllare i backup e creare report con AWS Backup Audit Manager.	14 settembre 2022
AWS Backup porta i CloudWatch parametri di Amazon nella dashboard della console di Backup	AWS Backup migliora la dashboard della console di Backup per visualizzare i CloudWatch parametri Amazon integrati per i processi di backup e ripristino per funzionalità e flessibilità di monitoraggio aggiuntive.	8 settembre 2022
Supporto per ulteriore flessibilità di crittografia di Amazon EBS durante il ripristino	AWS Backup ora offre opzioni di crittografia aggiuntive durante il ripristino degli snapshot di Amazon EBS.	1 settembre 2022

Modifica	Descrizione	Data
AWS Backup supporta la copia di backup su più account e più regioni di Amazon S3	AWS Backup ora offre la copia di backup tra regioni e più account per i backup di Amazon S3. Per ulteriori informazioni, consulta Backup di Amazon S3.	28 luglio 2022
AWS Backup Audit Manager offre un supporto di controllo aggiuntivo per FSx for ONTAP	AWS Backup Audit Manager offre ora controlli aggiuntivi per supportare il monitoraggio e l'audit dei volumi FSx for ONTAP, tra cui le risorse di backup sono protette da un piano di backup e dall'ultimo punto di ripristino creato. Per ulteriori informazioni, consulta Controlli e correzione di AWS Backup Audit Manager.	22 luglio 2022
AWS Backup aggiunge il supporto per il backup e il ripristino dei cluster Amazon RDS Multi-AZ per i cluster PostgreSQL e MySQL	AWS Backup ha aggiunto un'opzione di backup e ripristino del cluster Multi-Availability Zone con un'istanza di database principale e due istanze di database in standby leggibili. Per ulteriori informazioni, consulta Backup Amazon RDS Multi-AZ.	20 luglio 2022

Modifica	Descrizione	Data
AWS Backup Audit Manager aggiunge un nuovo controllo per la creazione di punti di ripristino	AWS Backup Audit Manager offre un nuovo controllo di audit per un maggiore supporto alla conformità. `Last recovery point created` è un controllo aggiuntivo opzionale per garantire che i punti di ripristin o vengano creati all'interno di intervalli di tempo specificati. Per ulteriori informazioni, consulta È stato creato l'ultimo punto di ripristino.	29 giugno 2022
È stato aggiunto un esempio di endpoint AWS Backup Gateway	AWS Backup Gateway ha fornito un endpoint di esempio per aiutare gli utenti a connettersi alle VPN (reti private virtuali). Per ulteriori informazioni, consulta Creazione di un AWS Backup endpoint VPC.	14 giugno 2022

Modifica	Descrizione	Data
AWS Backup ora offre endpoint Amazon VPC per VMware	AWS Backup ora supporta gli endpoint Amazon VPC per VMware, consenten doti di utilizzare una rete privata virtuale tra gli ambienti VMware e l'utilizzo. AWS AWS PrivateLink Per ulteriori informazioni, consulta Creazione di un gateway e AWS Backup e AWS PrivateLink.	1 giugno 2022
AWS Backup Audit Manager offre un supporto di controllo aggiuntivo per Amazon S3	Backup Audit Manager offre ora supporto per il controllo di conformità Risorse di backup protette dal piano di backup per i tipi di risorse S3. Per ulteriori informazioni, consulta Controlli e correzion e di AWS Backup Audit Manager.	25 maggio 2022
AWS Backup Audit Manager offre un supporto di controllo aggiuntivo per Storage Gateway	Backup Audit Manager offre ora supporto per il controllo di conformità Risorse di backup protette dal piano di backup per i tipi di risorse Storage Gateway. Per ulteriori informazioni, consulta Controlli e correzion e di AWS Backup Audit Manager.	25 maggio 2022

Modifica	Descrizione	Data
Supporto per Amazon FSx per OpenZFS	AWS Backup ora offre una gestione aggiuntiva della protezione dei dati per il backup e il ripristino su FSx per i file system OpenZFS.	18 maggio 2022
AWS Backup Supporto Audit Manager per VMware	AWS Backup ora fornisce supporto per le macchine virtuali nei controlli e nella correzione di Backup Audit Manager. Per ulteriori informazioni, consulta Controlli e correzione di AWS Backup Audit Manager.	11 maggio 2022
Amazon FSx è ora supportat o nella regione Asia Pacifico (Osaka-Locale)	AWS Backup ora offre il backup di Amazon FSx nella regione Asia Pacifico (Osaka) e di copie interregionali da e verso la regione Asia Pacifico (Osaka).	26 aprile 2022
Supporto per Amazon FSx per Lustre Persistent_2	AWS Backup ora offre la disponibilità generale del supporto per Amazon FSx for Lustre, che supporta livelli più elevati di throughput per unità di storage rispetto ai file system Persistent_1.	5 aprile 2022

Modifica	Descrizione	Data
Miglioramenti a VMware	AWS Backup ora offre il ripristino su Amazon EBS Volume, il ripristino a livello di disco e il supporto per VMware on. AWS Outposts Per ulteriori informazioni, consulta Ripristino di un macchina virtuale.	31 marzo 2022
AWS Backup Disponibilità per l'Asia Pacifico (Giacarta)	AWS Backup è ora disponibile per i clienti nella regione Asia Pacifico (Giacarta).	17 marzo 2022
Nuovi controlli per AWS Backup Audit Manager	AWS Backup Audit Manager introduce tre nuovi controlli di audit: copia interregionale, copia tra account e Backup Vault Lock. Per ulteriori informazioni, consulta Controlli e correzione di AWS Backup Audit Manager.	17 marzo 2022

Modifica	Descrizione	Data
Support per AWS PrivateLink	Con AWS PrivateLink for AWS Backup, puoi connetterti direttamente all' AWS Backup utilizzo di un endpoint di interfaccia nel tuo VPC invece di connetterti tramite Internet pubblico. Gli endpoint dell'interfaccia sono accessibili direttamente dalle applicazioni che si trovano in locale o in un'altra regione. AWS Per ulteriori informazioni, consulta AWS Backup e AWS PrivateLink.	28 febbraio 2022
Supporto per Amazon Simple Storage Service (Amazon S3)	La disponibilità generale AWS Backup per Amazon S3 Regioni AWS è disponibile in tutto, ad eccezione delle regioni di Cina (Pechino), Cina (Ningxia), (Stati Uniti occidentali) e AWS GovCloud AWS GovCloud (Stati Uniti orientali). Per ulteriori informazioni, consulta Utilizzo dei dati di Amazon S3.	14 febbraio 2022
Supporto per il backup avanzato di DynamoDB nelle regioni della Cina AWS	Il backup DynamoDB avanzato è ora disponibile nelle regioni Cina (Pechino) e Cina (Ningxia). Per ulteriori informazioni, consulta Backup DynamoDB avanzato.	18 gennaio 2022

Modifica	Descrizione	Data
Anteprima pubblica del supporto per Amazon S3	AWS Backup offre un'anteprima pubblica dei backup di Amazon S3. Per ulteriori informazioni, consulta Utilizzo dei dati di Amazon S3.	30 novembre 2021
Supporto per macchine virtuali (VM) VMware	Ora puoi utilizzarlo AWS Backup per eseguire automaticamente il backup delle macchine virtuali VMware. Per ulteriori informazioni, consulta Backup di macchine virtuali.	30 novembre 2021
Supporto per il backup DynamoDB avanzato	Ora puoi utilizzare AWS Backup per eseguire le seguenti funzionalità per tutti i nuovi backup di tabelle DynamoDB che crei: cold storage su più livelli, etichettatura per l'allocazione dei costi, copia tra regioni, copia tra account, crittografia indipendente e copia dei tag dalle tabelle DynamoDB di origine. Per ulteriori informazioni, consulta Backup di DynamoDB avanzato la Amazon DynamoDB Developer Guide e Using AWS Backup with DynamoDB.	23 novembre 2021

Modifica	Descrizione	Data
Support per il miglioram ento dell'assegnazione AWS Backup delle risorse nelle regioni della Cina AWS	AWS Backup il miglioram ento dell'assegnazione delle risorse è ora disponibile nella regione Cina (Pechino) e nella regione Cina (Ningxia). Per ulteriori informazioni, consulta Assegnazione di risorse a un piano di backup.	16 novembre 2021
Lancio del miglioramento dell'assegnazione delle risorse AWS Backup	L'ottimizzazione dell'asse gnazione delle risorse di backup offre controlli aggiuntiv i e granulari e nuovi processi semplificati per implementare piani di backup che proteggon o centinaia di migliaia di risorse. AWS Utilizza questa funzionalità per aumentare la velocità, la flessibilità e la precisione durante la protezion e dei dati mediante AWS Backup. Per ulteriori informazi oni, consulta Assegnazione di risorse a un piano di backup.	10 novembre 2021
Supporto per Amazon Neptune	Ora puoi utilizzarlo AWS Backup per eseguire il backup dei cluster Amazon Neptune. Per ulteriori informazioni, consulta Che cos'è AWS Backup?	5 novembre 2021

Modifica	Descrizione	Data
Supporto per Amazon DocumentDB	Ora puoi utilizzarlo AWS Backup per eseguire il backup dei cluster Amazon DocumentDB. Per ulteriori informazioni, consulta Che cos'è AWS Backup?	5 novembre 2021
Support per AWS Backup Vault Lock nelle regioni AWS della Cina	AWS Backup Vault Lock è ora disponibile nella regione della Cina (Pechino) e nella regione della Cina (Ningxia) . Per ulteriori informazioni, consulta Vault Lock di AWS Backup.	3 novembre 2021
Lancio di Vault Lock AWS Backup	Con AWS Backup Vault Lock, è possibile impedire l'elimina zione dei backup archiviati in un AWS Backup archivio di backup. Per ulteriori informazi oni, consulta Vault Lock di AWS Backup.	7 ottobre 2021
Lancio dei report di conformità AWS Backup Audit Manager	Con i report di conformità, è possibile generare report giornalieri sulla conformità delle attività e delle risorse di backup rispetto ai controlli definiti nei framework di AWS Backup Audit Manager. Per ulteriori informazioni, consulta Modelli di report di conformità.	5 ottobre 2021

Modifica	Descrizione	Data
AWS CloudFormation supporto per AWS Backup Audit Manager	Con AWS CloudFormation, ora puoi implementare framework, controlli e piani di report di AWS Backup Audit Manager in modo sicuro e ripetibile su larga scala. Per ulteriori informazioni, consulta Audit e report di Backup con AWS Backup Audit Manager.	4 ottobre 2021
Lancio di AWS Backup Audit Manager	Con AWS Backup Audit Manager, ora puoi definire i controlli per le attività e le risorse di backup e identificare le attività e le risorse che non sono conformi ai tuoi controlli . Puoi anche utilizzare AWS Backup Audit Manager per generare report giornalieri e su richiesta che servono come prova della conformità ai controlli definiti nel tempo. Per ulteriori informazioni, consulta Audit e report di Backup con AWS Backup Audit Manager.	24 agosto 2021
Supporto per nuove operazioni asincrone sui punti di ripristino	AWS Backup ora assume un ruolo collegato ai servizi per gestire le regole del ciclo di vita del backup nel caso in cui tu abbia modificato o eliminato il tuo ruolo IAM originale. Per ulteriori informazioni, consulta Eliminazione di backup.	23 agosto 2021

Modifica	Descrizione	Data
Supporto per backup crash-consistent multi-volume di Amazon EBS	Ora, quando si utilizza AWS Backup per proteggere le istanze Amazon EC2, per impostazione predefinita AWS Backup esegue backup multivolume e coerenti in caso di crash di tutti i volumi Amazon EBS collegati a ciascuna istanza Amazon EC2. Per ulteriori informazioni, consulta Creazione di backup crash-consistent multi-volume di Amazon EBS.	14 giugno 2021
Support per Amazon FSx in aggiunta Regioni AWS	Ora puoi utilizzarli AWS Backup per proteggere i tuoi file system Amazon FSx nelle seguenti regioni: AWS GovCloud (US), regione Europa (Milano), regione Africa (Città del Capo) e regione Medio Oriente (Bahrein). Per ulteriori informazioni, consulta Endpoint e quote di AWS Backup in Riferimenti generali AWS .	15 aprile 2021

Modifica	Descrizione	Data
Supporto per i backup tra regioni e tra account di Amazon FSx	Ora puoi utilizzarli AWS Backup per copiare i backup di Amazon FSx su più Regioni AWS account. Per ulteriori informazioni, consulta Creazione di una copia di backup. Se utilizzi policy gestite dal cliente, devi aggiunger e la nuova autorizzazione `fsx:CopyBackup` per evitare errori nei processi di backup esistenti. Per tale autorizzazione, consulta l'ultima istruzione nella policy di backup di Amazon FSx nelle policy gestite dal cliente.	12 Aprile 2021
Supporto per i tag di allocazio ne dei costi per i backup di Amazon EFS	Ora puoi utilizzare i tag di allocazione dei costi per tenere traccia dei costi dei backup di Amazon EFS a livello dettagliato e visualizz are e filtrare tali tag utilizzan do. AWS Cost Explorer Per ulteriori informazioni, consulta Utilizzo dei tag per l'allocaz ione dei costi.	7 Aprile 2021

Modifica	Descrizione	Data
Autorizzazione FedRAMP di livello High	AWS Backup è ora autorizzato a supportare i carichi di lavoro FedRAMP High. Per ulteriori informazioni, consulta Servizi AWS coperti dal programma di compliance.	25 marzo 2021
Nuovo Regione AWS	AWS Backup è ora disponibile nella regione Asia Pacifico (Osaka). In questa regione, AWS Backup attualmente non supporta Storage Gateway, Amazon FSx e il backup tra account. Per ulteriori informazioni, consulta Endpoint e quote di AWS Backup in Riferimenti generali AWS .	25 marzo 2021
Supporto per le operazioni in batch dei punti di ripristino	È ora possibile utilizzare la AWS Backup console per automatizzare le operazioni in batch per ripulire i punti di ripristino negli archivi di backup. Per ulteriori informazioni, consulta Eliminazione di backup.	23 marzo 2021
Supporto per ripristini nella classe di storage Amazon EFS One Zone	Ora puoi ripristinare i backup Amazon EFS nella classe di storage Amazon EFS One Zone. Per ulteriori informazioni, consulta Ripristino di un file system Amazon EFS.	12 marzo 2021

Modifica	Descrizione	Data
Supporto per il ripristino e il backup continuo di Amazon Relational Database point-in-time Service	Ora puoi utilizzarlo AWS Backup per automatizzare i backup continui di Amazon RDS ed eseguire il point-in-time ripristino (PITR), oltre a orchestrare i backup degli snapshot. Per ulteriori informazioni, consulta Ripristino a un'ora specificata utilizzando il ripristino. point-in-time	10 marzo 2021
Support per Amazon CloudWatch	Ora puoi utilizzarlo CloudWatch per monitorare le AWS Backup metriche. Per ulteriori informazioni, consulta Monitoraggio di eventi e metriche con Amazon CloudWatch e Amazon EventBridge.	3 febbraio 2021
Support per Amazon EventBridge	Ora puoi EventBridge utilizzarlo per monitorare AWS Backup gli eventi. Per ulteriori informazioni, consulta Monitoraggio di eventi e metriche con Amazon CloudWatch e Amazon EventBridge.	3 febbraio 2021

Modifica	Descrizione	Data
Supporto per backup tra account	Ora puoi utilizzarlo AWS Backup per eseguire il backup delle tue risorse su più Account AWS risorse. Per ulteriori informazioni, consulta Creazione di copie di backup tra AWS account.	18 novembre 2020
Supporto per il backup e il ripristino di file system Amazon FSx	Ora puoi utilizzarlo AWS Backup per eseguire il backup dei file system Amazon FSx. Per ulteriori informazioni, consulta Utilizzo dei file system Amazon FSx.	9 novembre 2020
Nuovo Regioni AWS	AWS Backup è ora disponibile in Africa (Città del Capo) e in Europa (Milano) Regioni AWS. Per ulteriori informazioni, consulta Endpoint e quote di AWS Backup in Riferimenti generali AWS .	21 ottobre 2020
Supporto per il backup di Windows abilitato per VSS	Ora puoi eseguire il backup e il ripristino di applicazioni Windows abilitate per VSS (Volume Shadow Copy Service) in esecuzione su istanze Amazon EC2. Per ulteriori informazioni, consulta Creazione di backup Windows VSS.	22 settembre 2020

Modifica	Descrizione	Data
Supporto per il backup automatico Amazon EFS	Ora puoi utilizzarlo AWS Backup per eseguire automaticamente il backup dei file system Amazon EFS. Per ulteriori informazioni, consulta Guida introduttiva 4: Creazione di backup automatici Amazon EFS.	16 luglio 2020
Nuovo Regione AWS	AWS Backup è ora disponibile in AWS GovCloud (US) Region. Per ulteriori informazioni, consulta Endpoint e quote di AWS Backup in Riferimenti generali AWS .	24 giugno 2020
Support per la gestione dei backup su più Account AWS	Ora puoi gestire i backup su più backup Account AWS utilizzando. AWS Organizations Per ulteriori informazioni, consulta Funzionamento della gestione di più account.	24 giugno 2020
Support per Amazon Aurora aggiunto a AWS Backup	Ora puoi AWS Backup configurare il backup delle risorse per Amazon Aurora. Per informazioni, consulta Panoramica di backup e ripristino di un cluster di database Aurora nella Guida per l'utente di Amazon Aurora.	10 giugno 2020

Modifica	Descrizione	Data
Support per la configurazione dei servizi con cui lavorare AWS Backup	È ora possibile AWS Backup configurare il backup delle risorse per AWS servizi specifici. Per ulteriori informazioni, consulta Attivare la gestione dei servizi con AWS Backup.	20 maggio 2020
Supporto per il backup delle istanze Amazon EC2 e aggiunta anche del supporto per il backup tra regioni	Ora è possibile eseguire il backup di intere istanze Amazon EC2, nonché copiare risorse tra Regioni AWS. Per ulteriori informazioni, consulta Creazione di copie di backup tra Regioni AWS.	13 gennaio 2020
Nuova guida	AWS lanci AWS Backup e la Guida per gli AWS Backup sviluppatori.	15 gennaio 2019

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.