aws

Panduan Developer

AWS Backup

AWS Backup: Panduan Developer

Table of Contents

Apa itu AWS Backup?

AWS Backup adalah layanan yang dikelola sepenuhnya yang memudahkan untuk memusatkan dan mengotomatiskan perlindungan data di seluruh AWS layanan, di cloud, dan di tempat. Dengan menggunakan layanan ini, Anda dapat mengonfigurasi kebijakan pencadangan dan memantau aktivitas AWS sumber daya Anda di satu tempat. Ini memungkinkan Anda untuk mengotomatiskan dan mengkonsolidasikan tugas pencadangan yang sebelumnya dilakukan service-by-service, dan menghilangkan kebutuhan untuk membuat skrip khusus dan proses manual. Dengan beberapa klik di AWS Backup konsol, Anda dapat mengotomatiskan kebijakan dan jadwal perlindungan data Anda.

AWS Backup tidak mengatur cadangan yang Anda ambil di AWS lingkungan Anda di luar. AWS Backup Oleh karena itu, jika Anda menginginkan end-to-end solusi terpusat untuk persyaratan kepatuhan bisnis dan peraturan, mulailah menggunakan AWS Backup hari ini.

Ikhtisar fitur

AWS Backup menyediakan banyak fitur dan kemampuan, termasuk yang berikut ini.

Manajemen cadangan terpusat

AWS Backup menyediakan konsol cadangan terpusat, satu set API cadangan, dan AWS Command Line Interface (AWS CLI) untuk mengelola cadangan di seluruh AWS layanan yang digunakan aplikasi Anda. Dengan AWS Backup, Anda dapat mengelola kebijakan pencadangan secara terpusat yang memenuhi persyaratan pencadangan Anda. Anda kemudian dapat menerapkannya ke AWS sumber daya Anda di seluruh AWS layanan, memungkinkan Anda untuk mencadangkan data aplikasi Anda secara konsisten dan sesuai. Konsol cadangan AWS Backup terpusat menawarkan tampilan gabungan dari pencadangan dan log aktivitas pencadangan Anda, sehingga memudahkan untuk mengaudit cadangan Anda dan memastikan kepatuhan.

Cadangan berbasis kebijakan

Dengan AWS Backup, Anda dapat membuat kebijakan cadangan yang dikenal sebagai rencana cadangan. Gunakan paket cadangan ini untuk menentukan persyaratan cadangan Anda dan kemudian menerapkannya ke AWS sumber daya yang ingin Anda lindungi di seluruh AWS layanan yang Anda gunakan. Anda dapat membuat rencana cadangan terpisah yang masing-masing memenuhi persyaratan kepatuhan bisnis dan peraturan tertentu. Ini membantu memastikan bahwa

setiap AWS sumber daya didukung sesuai dengan kebutuhan Anda. Paket Backup memudahkan untuk menerapkan strategi pencadangan di seluruh organisasi dan di seluruh aplikasi Anda dengan cara yang terukur.

Untuk semua opsi konfigurasi untuk paket cadangan, lihatOpsi dan konfigurasi paket Backup.

Kebijakan pencadangan berbasis tag

Anda dapat menggunakan AWS Backup untuk menerapkan rencana cadangan ke AWS sumber daya Anda dengan berbagai cara, termasuk menandai mereka. Penandaan memudahkan penerapan strategi pencadangan Anda di semua aplikasi Anda dan untuk memastikan bahwa semua AWS sumber daya Anda dicadangkan dan dilindungi. AWS tag adalah cara yang bagus untuk mengatur dan mengklasifikasikan AWS sumber daya Anda. Integrasi dengan AWS tag memungkinkan Anda menerapkan rencana cadangan dengan cepat ke sekelompok AWS sumber daya, sehingga mereka didukung secara konsisten dan sesuai.

Untuk semua cara Anda dapat menetapkan sumber daya Anda ke rencana cadangan, lihatMenetapkan sumber daya ke rencana cadangan.

Kebijakan manajemen siklus hidup

AWS Backup memungkinkan Anda memenuhi persyaratan kepatuhan sambil meminimalkan biaya penyimpanan cadangan dengan menyimpan cadangan di tingkat penyimpanan dingin berbiaya rendah. Anda dapat mengonfigurasi kebijakan siklus hidup yang secara otomatis mentransisikan cadangan dari penyimpanan hangat ke penyimpanan dingin sesuai dengan jadwal yang Anda tentukan.

Untuk daftar sumber daya yang dapat dialihkan ke cold storage, lihat. Ketersediaan fitur berdasarkan sumber daya Untuk langkah-langkah mengaktifkan penyimpanan dingin dalam paket cadangan, lihat Tingkatan siklus hidup dan penyimpanan.

Cadangan Lintas Wilayah

Dengan menggunakan AWS Backup, Anda dapat menyalin cadangan ke beberapa permintaan yang berbeda Wilayah AWS atau secara otomatis sebagai bagian dari rencana pencadangan terjadwal. Pencadangan Lintas Wilayah sangat berharga jika Anda memiliki kelangsungan bisnis atau persyaratan kepatuhan untuk menyimpan cadangan jarak minimum dari data produksi Anda. Untuk informasi selengkapnya, lihat Membuat salinan cadangan di seluruh Wilayah AWS.

Manajemen lintas akun dan pencadangan lintas akun

Anda dapat menggunakan AWS Backup untuk mengelola backup Anda di semua Akun AWS bagian dalam struktur Anda AWS Organizations. Dengan manajemen lintas akun, Anda dapat secara otomatis menggunakan kebijakan pencadangan untuk menerapkan rencana pencadangan di seluruh Akun AWS organisasi Anda. Hal ini membuat kepatuhan dan perlindungan data efisien dalam skala besar dan mengurangi overhead operasional. Ini juga membantu menghilangkan duplikasi rencana cadangan secara manual di seluruh akun individu. Untuk informasi selengkapnya, lihat Mengelola AWS Backup sumber daya di beberapa Akun AWS.

Anda juga dapat menyalin cadangan ke beberapa yang berbeda Akun AWS di dalam struktur AWS Organizations manajemen Anda. Dengan cara ini, Anda dapat "mengipasi" cadangan ke satu akun repositori, lalu "mengosongkan" cadangan untuk ketahanan yang lebih besar. Membuat salinan cadangan di seluruh Akun AWS.

Sebelum Anda dapat menggunakan manajemen lintas akun dan fitur pencadangan lintas akun, Anda harus memiliki struktur organisasi yang sudah ada yang dikonfigurasi. AWS OrganizationsUnit organisasi (OU) adalah sekelompok akun yang dapat dikelola sebagai satu kesatuan. AWS Organizations adalah daftar akun yang dapat dikelompokkan ke dalam unit organisasi dan dikelola sebagai satu kesatuan.

Audit dan pelaporan dengan AWS Backup Audit Manager

AWS Backup Audit Manager membantu Anda menyederhanakan tata kelola data dan pengelolaan kepatuhan cadangan Anda. AWS AWS Backup Audit Manager menyediakan kontrol bawaan dan dapat disesuaikan yang dapat Anda selaraskan dengan persyaratan organisasi Anda. Anda juga dapat menggunakan kontrol ini untuk melacak aktivitas dan sumber daya pencadangan secara otomatis.

AWS Backup Audit Manager dapat membantu Anda menemukan aktivitas dan sumber daya tertentu yang belum sesuai dengan kontrol yang Anda tetapkan. Ini juga menghasilkan laporan harian yang dapat Anda gunakan untuk menunjukkan bukti kepatuhan terhadap kontrol Anda dari waktu ke waktu.

Untuk menyertakan kepatuhan cadangan Anda di samping postur kepatuhan Anda secara keseluruhan, Anda dapat secara otomatis mengimpor temuan AWS Backup Audit Manager ke dalamnya AWS Audit Manager.

Cadangan inkremental

AWS Backup secara efisien menyimpan cadangan periodik Anda secara bertahap. Cadangan pertama AWS sumber daya mencadangkan salinan lengkap data Anda. Untuk setiap pencadangan inkremental berturut-turut, hanya perubahan pada AWS sumber daya Anda yang dicadangkan. Pencadangan tambahan memungkinkan Anda mendapatkan keuntungan dari perlindungan data dari pencadangan yang sering sekaligus meminimalkan biaya penyimpanan.

Untuk daftar sumber daya yang mendukung pencadangan tambahan, lihat. Ketersediaan fitur berdasarkan sumber daya

AWS Backup Manajemen penuh

Beberapa jenis sumber daya mendukung AWS Backup manajemen penuh. Manfaat AWS Backup manajemen penuh meliputi:

- Enkripsi independen. AWS Backup secara otomatis mengenkripsi cadangan Anda dengan kunci KMS AWS Backup brankas Anda, alih-alih menggunakan kunci enkripsi yang sama dengan sumber daya sumber Anda. Ini meningkatkan lapisan pertahanan Anda. Untuk informasi selengkapnya, lihat Enkripsi untuk backup di AWS Backup.
- **`awsbackup`**Nama Sumber Daya Amazon (ARN). Backup ARN dimulai dengan `arn:aws:backup` alih-alih. `arn:aws:`*`source-resource`* Ini memungkinkan Anda untuk membuat kebijakan akses yang berlaku khusus untuk cadangan dan bukan sumber daya sumber. Untuk informasi selengkapnya, lihat Pengendalian akses.
- Tagihan cadangan terpusat dan tag alokasi biaya Cost Explorer. . Biaya untuk AWS Backup (termasuk penyimpanan, transfer data, pemulihan, dan penghapusan awal) muncul di bawah “Cadangan” di Amazon Web Services tagihan Anda, alih-alih muncul di bawah setiap sumber daya yang didukung. Anda juga dapat menggunakan tag alokasi biaya Cost Explorer untuk melacak dan mengoptimalkan biaya pencadangan Anda. Untuk informasi selengkapnya, lihat Pengukuran, biaya, dan penagihan.

Untuk melihat jenis sumber daya mana yang memenuhi syarat untuk AWS Backup pengelolaan penuh, lihatKetersediaan fitur berdasarkan sumber daya.

Pemantauan aktivitas Backup

AWS Backup menyediakan dasbor yang memudahkan untuk mengaudit pencadangan dan pemulihan aktivitas di seluruh AWS layanan. Hanya dengan beberapa klik pada AWS Backup konsol,

Anda dapat melihat status pekerjaan cadangan terbaru. Anda juga dapat memulihkan pekerjaan di seluruh AWS layanan untuk memastikan bahwa AWS sumber daya Anda dilindungi dengan benar.

AWS Backup terintegrasi dengan Amazon CloudWatch dan Amazon EventBridge. CloudWatch memungkinkan Anda melacak metrik dan membuat alarm. EventBridge memungkinkan Anda untuk melihat dan memantau AWS Backup acara. Untuk informasi selengkapnya, lihat Memantau AWS Backup peristiwa menggunakan EventBridge dan Memantau AWS Backup metrik dengan CloudWatch.

AWS Backup terintegrasi dengan AWS CloudTrail. CloudTrail memberi Anda tampilan terkonsolidasi dari log aktivitas cadangan yang membuatnya cepat dan mudah untuk mengaudit bagaimana sumber daya Anda dicadangkan. AWS Backup juga terintegrasi dengan Amazon Simple Notification Service (Amazon SNS), memberi Anda notifikasi aktivitas pencadangan, seperti saat pencadangan berhasil atau pemulihan telah dimulai. Untuk informasi selengkapnya, lihat Logging panggilan AWS Backup API dengan CloudTrail dan Menggunakan Amazon SNS untuk melacak AWS Backup peristiwa.

Amankan data Anda di brankas cadangan

Konten dari setiap AWS Backup cadangan tidak dapat diubah, artinya tidak ada yang dapat mengubah konten itu. AWS Backup selanjutnya mengamankan cadangan Anda di brankas cadangan, yang memisahkannya dengan aman dari contoh sumbernya. Misalnya, vault Anda akan menyimpan cadangan Amazon EC2 dan Amazon EBS sesuai dengan kebijakan siklus hidup yang Anda pilih, meskipun Anda menghapus sumber instans Amazon EC2 dan volume Amazon EBS.

Brankas cadangan menawarkan enkripsi dan kebijakan akses berbasis sumber daya yang memungkinkan Anda menentukan siapa yang memiliki akses ke cadangan Anda. Anda dapat menentukan kebijakan akses untuk brankas cadangan yang menentukan siapa yang memiliki akses ke cadangan dalam brankas tersebut dan tindakan apa yang dapat mereka lakukan. Ini menyediakan cara sederhana dan aman untuk mengontrol akses ke cadangan Anda di seluruh AWS layanan. Untuk meninjau AWS dan kebijakan yang dikelola pelanggan AWS Backup, lihat Kebijakan terkelola untuk AWS Backup.

Anda dapat menggunakan AWS Backup Vault Lock untuk mencegah siapa pun (termasuk Anda) menghapus cadangan atau mengubah periode retensi mereka. AWS Backup Vault Lock membantu Anda menegakkan model write-once-read-many(WORM) dan menambahkan lapisan pertahanan lain ke pertahanan Anda secara mendalam. Untuk memulai, lihat AWS Backup Vault Lock.

Support untuk kewajiban kepatuhan

AWS Backup membantu Anda memenuhi kewajiban kepatuhan global Anda. AWS Backup berada dalam lingkup program AWS kepatuhan berikut:

- FedRAMP Tinggi
- GDPR
- SOC 1, 2, dan 3
- PCI
- HIPAA
- dan masih banyak lagi

Memulai

Untuk mempelajari lebih lanjut AWS Backup, kami sarankan Anda mulai dengan Memulai dengan AWS Backup.

AWS Sumber daya dan aplikasi yang didukung

Berikut ini adalah AWS sumber daya dan aplikasi pihak ketiga yang dapat Anda cadangkan dan pulihkan menggunakan AWS Backup. Untuk informasi selengkapnya, lihat the section called "Ketersediaan fitur".

Layanan	Jenis sumber daya yang mendukung
Amazon Elastic Compute Cloud (Amazon EC2)	Instans Amazon EC2 (tidak termasuk AMI yang didukung toko instans)
Amazon Simple Storage Service (Amazon S3)	Data Amazon S3
Toko Blok Elastis Amazon (Amazon EBS)	Volume Amazon EBS
Amazon DynamoDB	Tabel Amazon DynamoDB

Layanan	Jenis sumber daya yang mendukung
Amazon Relational Database Service (Amazon RDS)	Instans basis data Amazon RDS (termasuk semua mesin basis data); Kluster Zona Ketersediaan Multi-Ketersediaan
Amazon Aurora	Cluster Aurora
Amazon Elastic File System (Amazon EFS)	Sistem file Amazon EFS
FSx for Lustre	FSx for Lustre file system
fsX for Windows File Server	FSx untuk sistem file Windows File Server
Amazon FSx untuk ONTAP NetApp	fsX untuk sistem file ONTAP
Amazon FSx untuk OpenZFS	FSx untuk sistem file OpenZFS
AWS Storage Gateway (Gerbang Volume)	AWS Storage Gateway volume
Amazon DocumentDB	Cluster berbasis instans Amazon DocumentDB
Amazon Neptunus	Cluster Amazon Neptunus
Amazon Redshift	Cluster Amazon Redshift
Amazon Timestream	Tabel Amazon Timestream
VMware Cloud™ aktif AWS	Mesin virtual VMware Cloud™ aktif AWS
VMware Cloud™ aktif AWS Outposts	Mesin virtual VMware Cloud™ aktif AWS Outposts
AWS CloudFormation	AWS CloudFormation tumpukan

Layanan	Jenis sumber daya yang mendukung
Database SAP HANA	Database SAP HANA pada instans Amazon EC2

Harga

Dengan AWS Backup, Anda membayar penyimpanan cadangan, memulihkan data, pengujian pemulihan, transfer data lintas wilayah, dan AWS Backup Audit Manager. Untuk informasi selengkapnya, silakan lihat Harga AWS Backup.

AWS Backup ketersediaan fitur

AWS Backup fitur yang ditawarkan sesuai dengan sumber daya dan Wilayah AWS. Bagian dan tabel berikut dapat membantu Anda menentukan ketersediaan fitur.

Daftar Isi

Fitur tersedia untuk semua sumber daya yang didukung

AWS Backup menawarkan fitur-fitur berikut untuk AWS layanan yang didukung, serta untuk aplikasi pihak ketiga yang didukung. Support untuk fitur atau layanan tidak boleh diasumsikan kecuali disebutkan secara eksplisit.

- Jadwal pencadangan otomatis dan manajemen retensi
- Pemantauan cadangan terpusat
- Cadangan terenkripsi
- Pencadangan tambahan
- Manajemen lintas akun dengan AWS Organizations
- Audit dan laporan pencadangan otomatis dengan AWS Backup Audit Manager
- Tulis-sekali, baca-banyak (WORM) dengan Vault Lock AWS Backup

Ketersediaan fitur berdasarkan sumber daya

Untuk menggunakan AWS layanan AWS Backup yang didukung di Wilayah tertentu, layanan harus tersedia di Wilayah. Untuk menentukan ketersediaan layanan di Wilayah, lihat titik akhir layanan di. Referensi Umum AWS

AWS Backup menduku	Cadanga Lintas Wilayah	Pencada an lintas akun	AWS Backup Audit Manager	Pencada an tambaha	Pencada an dan point-in-time pemuliha berkelan utan	Manajem penuh	Siklus hidup ke penyimp an dingin	Pemulihan tingkat item 1	Kembalika n pengujian
Amazon EC2	✓	✓	✓	✓					✓
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
Contoh tunggal Amazon RDS	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Kluster Amazon RDS	✓ [3]	✓ [3]	✓ [4]	✓					✓
Amazon Aurora	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓
Amazon EFS	✓	✓	✓	✓		✓	✓	✓	✓

AWS Backup menduku	Cadanga Lintas Wilayah	Pencada an lintas akun	AWS Backup Audit Manager	Pencada an tambaha	Pencada an dan point-in-time pemuliha berkelan utan	Manajem penuh	Siklus hidup ke penyimp an dingin	Pemulihan tingkat item 1	Kembalika n pengujian
FSx for Lustre	✓	✓	✓	✓					✓
FSx for Windows File Server	✓	✓	✓	✓					✓
fsX untuk ONTAP			✓ [2]	✓					✓
FSx untuk OpenZF	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon Docume B	✓ [3]	✓ [3]	✓						✓
Amazon Neptune	✓ [3]	✓ [3]	✓						✓

AWS Backup menduku	Cadanga Lintas Wilayah	Pencada an lintas akun	AWS Backup Audit Manager	Pencada an tambaha	Pencada an dan point-in-time pemuliha berkelan utan	Manajem penuh	Siklus hidup ke penyimp an dingin	Pemulihan tingkat item 1	Kembalika n pengujian
Amazon Redshift								✓	
Timestre m	✓	✓	✓	✓		✓	✓	✓	
Windows VSS	✓	✓	✓	✓					
mesin virtual	✓	✓	✓	✓		✓	✓	✓	
AWS CloudFo ation template	✓	✓		✓ [5]		✓	✓ [5]		
Amazon Dynamol			✓						✓
Dynamol dengan fitur-fitur AWS Backup canggih	✓	✓	✓			✓	✓		✓

AWS Backup menduku	Cadanga Lintas Wilayah	Pencada an lintas akun	AWS Backup Audit Manager	Pencada an tambaha	Pencada an dan point-in-time pemuliha berkelan utan	Manajem penuh	Siklus hidup ke penyimp an dingin	Pemulihan tingkat item 1	Kembalika n pengujian
Databas SAP HANA pada instans Amazon EC2				✓	✓	✓	✓		

Beberapa jenis sumber daya memiliki kemampuan pencadangan berkelanjutan dan salinan lintas wilayah dan lintas akun tersedia. Ketika salinan lintas wilayah atau lintas akun dari cadangan berkelanjutan dibuat, titik pemulihan yang disalin (cadangan) menjadi cadangan snapshot (periodik). Amazon RDS dan Amazon S3 mendukung salinan snapshot tambahan; Amazon Aurora hanya mendukung salinan snapshot penuh. PITR (Point-in-Time Restore) tidak tersedia untuk salinan ini.

[1] “Item” dalam pemulihan tingkat item bervariasi tergantung pada sumber daya yang didukung. Misalnya, item sistem file adalah file atau direktori, sedangkan item S3 adalah objek S3. Item VMware adalah disk. Untuk informasi selengkapnya, lihat Memulihkan cadangan bagian untuk sumber daya yang didukung.

[2] AWS Backup Audit Manager mendukung sumber daya ini di semua kontrol kecuali salinan lintas akun dan salinan lintas wilayah.

[3] RDS, Aurora, DocumentDB, dan Neptunus tidak mendukung tindakan penyalinan tunggal yang melakukan pencadangan lintas wilayah DAN lintas akun. Anda dapat memilih satu atau yang lain. Anda juga dapat menggunakan AWS Lambda skrip untuk mendengarkan penyelesaian salinan pertama Anda, melakukan salinan kedua Anda, lalu menghapus salinan pertama. Instans database multi availability zone (Multi-AZ) RDS dapat disalin, tetapi klaster multi-AZ saat ini tidak mendukung salinan lintas wilayah atau lintas akun. Lihat Pertimbangan salinan Lintas Wilayah dengan sumber daya tertentu untuk informasi lebih lanjut.

[4] Lihat cadangan zona multi-ketersediaan RDS untuk Wilayah di mana dukungan Backup Audit Manager tersedia.

[5] Dalam cadangan CloudFormation tumpukan, sumber daya bersarang mempertahankan fitur sumber daya mereka. Namun, sumber daya dalam tumpukan tidak mempertahankan fungsionalitas Point-in-Time Restore (PITR) (seperti Amazon S3 dan Amazon RDS). Properti dalam matriks di atas berlaku hanya untuk CloudFormation template dan bukan ke sumber daya dalam tumpukan.

[6] Untuk Aurora, snapshot penuh, dan cadangan tambahan ditawarkan melalui PITR.

Ketersediaan fitur oleh Wilayah AWS

AWS Backup tersedia dalam semua hal berikut Wilayah AWS. AWS Backup fitur tersedia di semua Wilayah ini kecuali dinyatakan lain dalam tabel berikut.

AWS Backup mendukung	Cadangan Lintas Wilayah	Manajemen lintas akun	Pencadangan lintas akun	AWS Backup Audit Manager dan Dasbor Pekerjaan	Kembalikan pengujian
AS Timur (N. Virginia)	✓	✓	✓	✓	✓
AS Timur (Ohio)	✓	✓	✓	✓	✓
AS Barat (California Utara)	✓	✓	✓	✓	✓
AS Barat (Oregon)	✓	✓	✓	✓	✓
Afrika (Cape Town)	✓		✓	✓	✓
Asia Pasifik (Hong Kong)	✓		✓	✓	✓

AWS Backup mendukung	Cadangan Lintas Wilayah	Manajemen lintas akun	Pencadangan lintas akun	AWS Backup Audit Manager dan Dasbor Pekerjaan	Kembalikan pengujian
Asia Pasifik (Hyderabad)	✓		✓		✓
Asia Pasifik (Jakarta)	✓		✓		✓
Asia Pasifik (Melbourne)	✓		✓		✓
Asia Pasifik (Mumbai)	✓	✓	✓	✓	✓
Asia Pasifik (Osaka)	✓	✓	✓		✓
Asia Pasifik (Seoul)	✓	✓	✓	✓	✓
Asia Pasifik (Singapura)	✓	✓	✓	✓	✓
Asia Pasifik (Sydney)	✓	✓	✓	✓	✓
Asia Pasifik (Tokyo)	✓	✓	✓	✓	✓
(Canada (Central)	✓	✓	✓	✓	✓
Kanada Barat (Calgary)	✓ (kecuali Amazon S3)		✓		

AWS Backup mendukung	Cadangan Lintas Wilayah	Manajemen lintas akun	Pencadangan lintas akun	AWS Backup Audit Manager dan Dasbor Pekerjaan	Kembalikan pengujian
China (Beijing)	✓				
Tiongkok (Ningxia)	✓				
Eropa (Frankfurt)	✓	✓	✓	✓	✓
Eropa (Irlandia)	✓	✓	✓	✓	✓
Eropa (London)	✓	✓	✓	✓	✓
Eropa (Milan)	✓		✓	✓	✓
Eropa (Paris)	✓	✓	✓	✓	✓
Eropa (Spanyol)	✓		✓		✓
Eropa (Stockholm)	✓	✓	✓	✓	✓
Eropa (Zürich)	✓		✓		✓
Israel (Tel Aviv)	✓		✓		

AWS Backup mendukung	Cadangan Lintas Wilayah	Manajemen lintas akun	Pencadangan lintas akun	AWS Backup Audit Manager dan Dasbor Pekerjaan	Kembalikan pengujian
Timur Tengah (Bahrain)	✓		✓	✓	✓
Timur Tengah (UEA)	✓		✓		✓
Amerika Selatan (Sao Paulo)	✓	✓	✓	✓	✓
AWS GovCloud (AS-Timur)	✓	✓	✓	✓	
AWS GovCloud (AS-Barat)	✓	✓	✓	✓	

China (Beijing) dan China (Ningxia) mendukung salinan lintas wilayah dari salah satu dari dua Wilayah ini ke yang lain. Salinan Lintas Wilayah tidak didukung dari Wilayah ini ke Wilayah lain atau ke Wilayah ini. Salinan lintas akun tidak didukung untuk Wilayah ini.

Dasbor pekerjaan tidak tersedia di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat). Agregasi dasbor pekerjaan hanya tersedia di Wilayah yang mendukung manajemen lintas akun dan AWS Backup Audit Manager.

Amazon FSx untuk Windows File Server dan Amazon Neptunus tidak mendukung salinan cadangan lintas wilayah di Wilayah keikutsertaan.

Layanan yang didukung oleh Wilayah AWS

AWS Backup mendukung hal berikut di semua Wilayah yang didukung:

- Aurora
- DynamoDB
- DynamoDB dengan fitur-fitur AWS Backup canggih
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

Tabel berikut menunjukkan AWS Backup dukungan untuk lainnya Layanan AWS menurut Wilayah.

Wilayah dan layanan	Amazon FSx	SAP HANA pada instans EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware dan Backup
AS Timur (N. Virginia)	✓	✓	✓	✓	✓	✓
AS Timur (Ohio)	✓	✓	✓	✓	✓	✓
AS Barat (California Utara)	Jendela; Kilau; ONTAP	✓	✓	✓		✓
AS Barat (Oregon)	Jendela; Kilau; ONTAP	✓	✓	✓	✓	✓

Wilayah dan layanan	Amazon FSx	SAP HANA pada instans EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware dan Backup
Afrika (Cape Town)	Jendela; Kilau; ONTAP	✓	✓ [1]	✓		✓
Asia Pasifik (Hong Kong)	✓	✓	✓ [1]	✓		✓
Asia Pasifik (Hyderabad)	Jendela; Kilau; ONTAP		✓ [1]	✓		
Asia Pasifik (Jakarta)	Jendela; Kilau; ONTAP		✓	✓		
Asia Pasifik (Melbourne)	Jendela; Kilau; ONTAP		✓ [1]	✓		
Asia Pasifik (Mumbai)	✓	✓	✓	✓		✓
Asia Pasifik (Osaka)	Jendela; Kilau	✓	✓ [1]	✓		✓

Wilayah dan layanan	Amazon FSx	SAP HANA pada instans EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware dan Backup
Asia Pasifik (Seoul)	✓	✓	✓	✓		✓
Asia Pasifik (Singapura)	✓	✓	✓	✓		✓
Asia Pasifik (Sydney)	✓	✓	✓	✓	✓	✓
Asia Pasifik (Tokyo)	✓	✓	✓	✓	✓	✓
(Canada (Central)	✓	✓	✓	✓		✓
Kanada Barat (Calgary)						
Tiongkok (Beijing)	Jendela; Kilau		✓ [1]	✓	✓	
Tiongkok (Ningxia)	Jendela; Kilau		✓ [1]	✓	✓	
Eropa (Frankfurt)	✓	✓	✓	✓	✓	✓

Wilayah dan layanan	Amazon FSx	SAP HANA pada instans EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware dan Backup
Eropa (Irlandia)	✓	✓	✓	✓	✓	✓
Eropa (London)	✓	✓	✓	✓		✓
Eropa (Milan)	Jendela; Kilau; ONTAP	✓	✓ [1]	✓		✓
Eropa (Paris)	Jendela; Kilau; ONTAP	✓	✓	✓		✓
Eropa (Spanyol)	Jendela; Kilau; ONTAP		✓ [1]	✓		
Eropa (Stockholm)	✓	✓	✓	✓		✓
Eropa (Zürich)	Jendela; Kilau; ONTAP		✓ [1]	✓		
Israel (Tel Aviv)	Jendela; Kilau; ONTAP		✓ [1]	✓		
Timur Tengah (Bahrain)	Jendela; Kilau; ONTAP	✓	✓ [1]	✓		✓

Wilayah dan layanan	Amazon FSx	SAP HANA pada instans EC2	Amazon S3	Storage Gateway	Amazon Timestream	Gateway VMware dan Backup
Timur Tengah (UEA)			✓ [1]	✓		
Amerika Selatan (Sao Paulo)		✓	✓	✓		✓
AWS GovCloud (AS-Barat)	Jendela; Kilau; ONTAP		✓ [1]	✓		✓
AWS GovCloud (AS-Timur)	Jendela; Kilau; ONTAP		✓ [1]	✓		✓

Pemeriksaan di bawah Amazon FSx menunjukkan bahwa FSx for Windows File Server, FSx for Lustre, FSx untuk ONTAP, dan FSx untuk OpenZFS semuanya didukung di Wilayah tersebut oleh; jika tidak, konfigurasi yang didukung akan dicantumkan. AWS Backup

[1] Salinan lintas wilayah dan lintas akun tidak didukung.

AWS Backup: Cara kerjanya

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang memudahkan untuk memusatkan dan mengotomatiskan pencadangan data di seluruh layanan. AWS Dengan AWS Backup, Anda dapat membuat kebijakan cadangan yang disebut rencana cadangan. Anda dapat menggunakan paket ini untuk menentukan persyaratan pencadangan Anda, seperti seberapa sering mencadangkan data Anda dan berapa lama untuk menyimpan cadangan tersebut.

AWS Backup memungkinkan Anda menerapkan rencana cadangan ke AWS sumber daya Anda hanya dengan menandai mereka. AWS Backup kemudian secara otomatis mencadangkan AWS sumber daya Anda sesuai dengan rencana cadangan yang Anda tentukan.

Bagian berikut menjelaskan cara AWS Backup kerja, detail implementasinya, dan pertimbangan keamanan.

Topik

Cara AWS Backup bekerja dengan AWS layanan yang didukung

Beberapa AWS layanan yang AWS Backup didukung menawarkan fitur cadangan mereka sendiri yang berdiri sendiri. Fitur-fitur tersebut tersedia untuk Anda terlepas dari apakah Anda menggunakannya AWS Backup. Namun, cadangan AWS layanan lain yang dibuat tidak tersedia untuk tata kelola pusat melalui. AWS Backup

Untuk mengonfigurasi AWS Backup untuk mengelola perlindungan data secara terpusat untuk semua layanan yang didukung, Anda harus memilih untuk mengelola layanan tersebut AWS Backup, membuat cadangan sesuai permintaan atau menjadwalkan pencadangan menggunakan paket cadangan, dan menyimpan cadangan Anda di brankas cadangan.

Topik

- Bekerja dengan Amazon DynamoDB
- Bekerja dengan sistem file Amazon FSx
- Bekerja dengan Amazon EC2
- Bekerja dengan Amazon EFS
- Bekerja dengan Amazon EBS
- Bekerja dengan Amazon RDS dan Aurora
- Bekerja dengan AWS BackInt
- Bekerja dengan AWS Storage Gateway
- Bekerja dengan Amazon DocumentDB
- Bekerja dengan Amazon Neptunus
- Bekerja dengan Amazon Timestream
- Bekerja dengan AWS Organizations
- Bekerja dengan AWS CloudFormation
- Bekerja dengan AWS BackInt, AWS Systems Manager untuk SAP, dan SAP HANA
- Bagaimana AWS layanan mendukung sumber daya mereka sendiri

Memilih untuk mengelola layanan dengan AWS Backup

Ketika AWS layanan baru tersedia, Anda harus mengaktifkan AWS Backup untuk menggunakan layanan tersebut. Jika Anda mencoba membuat cadangan atau cadangan sesuai permintaan menggunakan sumber daya dari layanan yang tidak diaktifkan, Anda menerima pesan kesalahan dan tidak dapat menyelesaikan prosesnya.

AWS Backup Konsol memiliki dua cara untuk menyertakan jenis sumber daya dalam rencana cadangan: secara eksplisit menetapkan jenis sumber daya dalam rencana cadangan atau menyertakan semua sumber daya. Lihat poin di bawah ini untuk memahami cara kerja pilihan ini dengan layanan opt in.

- Jika penetapan sumber daya hanya didasarkan pada tag, maka pengaturan keikutsertaan layanan diterapkan.
- Jika jenis sumber daya secara eksplisit ditetapkan ke rencana cadangan, itu akan disertakan dalam cadangan meskipun keikutsertaan tidak diaktifkan untuk layanan tertentu. Ini tidak berlaku untuk Aurora, Neptunus, dan Amazon DocumentDB. Agar layanan ini disertakan, keikutsertaan harus diaktifkan.

- Jika kedua jenis sumber daya dan tag ditentukan dalam penetapan sumber daya, jenis sumber daya yang ditentukan difilter terlebih dahulu, lalu tag lebih lanjut memfilter sumber daya tersebut.

  Pengaturan keikutsertaan layanan diabaikan untuk sebagian besar jenis sumber daya. Namun Aurora, Neptunus, dan Amazon DocumentDB memerlukan layanan opt-in.
- Untuk Amazon FSx untuk NetApp ONTAP, saat menggunakan pemilihan sumber daya berbasis tag, terapkan tag ke volume individual alih-alih seluruh sistem file.

Pengaturan keikutsertaan layanan khusus untuk Wilayah. Saat akun menggunakan AWS Backup (membuat brankas cadangan atau paket cadangan) di Wilayah, akun secara otomatis dipilih ke semua jenis sumber daya yang didukung oleh AWS Backup di Wilayah pada saat itu. Layanan yang didukung yang ditambahkan ke Wilayah tersebut di kemudian hari tidak akan secara otomatis disertakan dalam paket cadangan. Anda dapat memilih untuk memilih jenis sumber daya tersebut setelah didukung.

Untuk mengkonfigurasi layanan yang digunakan AWS Backup

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pada halaman keikutsertaan Layanan, pilih Konfigurasi sumber daya.
4. Gunakan sakelar sakelar untuk mengaktifkan atau menonaktifkan layanan yang digunakan. AWS Backup

   > **Important**
   >
   > RDS, Aurora, Neptune, dan DocumentDB berbagi Amazon Resource Name (ARN) yang sama. Memilih untuk mengelola salah satu jenis sumber daya ini dengan AWS Backup memilih semuanya saat menetapkannya ke paket cadangan. Terlepas dari itu, kami sarankan Anda memilih semuanya untuk secara akurat mewakili status keikutsertaan Anda.
5. Pilih Konfirmasi.

Bekerja dengan data Amazon S3

AWS Backup menawarkan pencadangan dan pemulihan yang dikelola sepenuhnya untuk cadangan Amazon S3. Untuk mempelajari selengkapnya, lihat Cadangan Amazon S3.

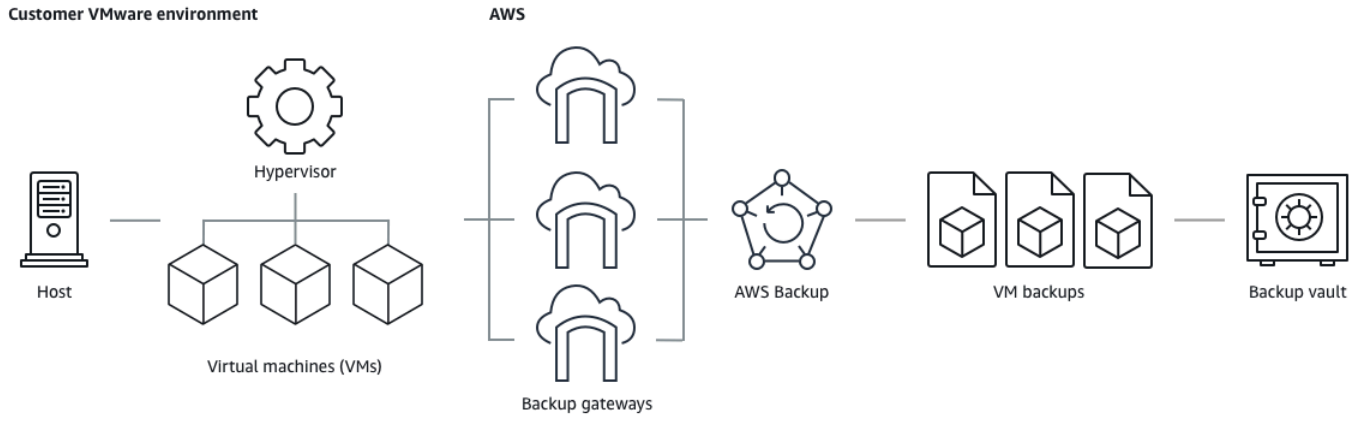
- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan data Amazon S3 menggunakan: AWS BackupMemulihkan data S3

Untuk informasi rinci tentang data S3, lihat dokumentasi Amazon S3.

Bekerja dengan mesin virtual VMware

AWS Backup mendukung perlindungan data terpusat dan otomatis untuk mesin virtual VMware (VM) lokal bersama dengan VM di VMware Cloud™ (VMC) aktif. AWS Anda dapat membuat cadangan dari tempat Anda dan mesin virtual VMC ke. AWS Backup Kemudian, Anda dapat memulihkan dari AWS Backup baik di tempat atau VMC.

Backup gateway adalah AWS Backup perangkat lunak yang dapat diunduh yang Anda gunakan ke VM VMware Anda untuk menghubungkannya. AWS Backup Gateway terhubung ke server manajemen VM Anda untuk menemukan VM, menemukan VM Anda, mengenkripsi data, dan mentransfer data secara efisien. AWS Backup Diagram berikut menggambarkan bagaimana Backup gateway terhubung ke VM Anda:



- Cara membuat cadangan sumber daya: Pencadangan mesin virtual
- Cara mengembalikan sumber daya VM: Memulihkan mesin virtual menggunakan AWS Backup

Bekerja dengan Amazon DynamoDB

AWS Backup mendukung pencadangan dan pemulihan tabel Amazon DynamoDB. DynamoDB adalah layanan database NoSQL yang dikelola sepenuhnya yang memberikan kinerja yang cepat dan dapat diprediksi dengan skalabilitas yang mulus.

Sejak diluncurkan, AWS Backup selalu mendukung DynamoDB. Mulai November 2021, AWS Backup juga memperkenalkan fitur-fitur canggih untuk backup DynamoDB. Fitur-fitur canggih tersebut termasuk menyalin cadangan Anda di seluruh Wilayah AWS dan akun, meningkatkan cadangan ke penyimpanan dingin, dan menggunakan tag untuk izin dan manajemen biaya.

Orientasi AWS Backup pelanggan baru setelah November 2021 akan mengaktifkan fitur cadangan DynamoDB lanjutan secara default.

Kami merekomendasikan semua AWS Backup pelanggan yang ada mengaktifkan fitur-fitur canggih untuk DynamoDB. Tidak ada perbedaan dalam harga penyimpanan cadangan hangat setelah Anda mengaktifkan fitur-fitur canggih, dan Anda dapat menghemat uang dengan meningkatkan cadangan ke penyimpanan dingin dan mengoptimalkan biaya Anda dengan menggunakan tag alokasi biaya.

Untuk daftar lengkap fitur-fitur canggih dan cara mengaktifkannya, lihatCadangan DynamoDB tingkat lanjut.

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan sumber daya DynamoDB: Memulihkan tabel Amazon DynamoDB

Untuk informasi rinci tentang DynamoDB, lihat Apa itu Amazon DynamoDB? di Panduan Pengembang Amazon DynamoDB.

Bekerja dengan sistem file Amazon FSx

AWS Backup mendukung pencadangan dan pemulihan sistem file Amazon FSx. Amazon FSx menyediakan sistem file pihak ketiga yang dikelola sepenuhnya dengan kompatibilitas asli dan set fitur untuk beban kerja. AWS Backup menggunakan fungsionalitas cadangan bawaan Amazon FSx. Jadi cadangan yang diambil dari AWS Backup konsol memiliki tingkat konsistensi dan kinerja sistem file yang sama, dan opsi pemulihan yang sama dengan cadangan yang diambil melalui konsol Amazon FSx.

Jika Anda menggunakannya AWS Backup untuk mengelola cadangan ini, Anda mendapatkan fungsionalitas tambahan, seperti opsi retensi tak terbatas, dan kemampuan untuk membuat cadangan terjadwal sesering setiap jam. Selain itu, AWS Backup pertahankan cadangan Anda bahkan setelah sistem file sumber dihapus. Hal ini melindungi dari penghapusan yang tidak disengaja atau berbahaya.

Gunakan AWS Backup untuk melindungi sistem file Amazon FSx jika Anda ingin mengonfigurasi kebijakan pencadangan dan memantau tugas pencadangan dari konsol cadangan pusat yang juga memperluas dukungan untuk layanan lain. AWS

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan sumber daya Amazon FSx: Memulihkan sistem file FSX

Untuk informasi rinci tentang sistem file Amazon FSx, lihat dokumentasi Amazon FSx.

Bekerja dengan Amazon EC2

AWS Backup mendukung instans Amazon EC2.

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan sumber daya Amazon EC2: Memulihkan instans Amazon EC2

Anda dapat menjadwalkan atau melakukan pekerjaan pencadangan sesuai permintaan yang mencakup seluruh instans EC2, termasuk volume Amazon EBS-nya. Oleh karena itu, Anda dapat memulihkan seluruh instans Amazon EC2 dari satu titik pemulihan, termasuk volume root, volume data, dan beberapa pengaturan konfigurasi instans, seperti jenis instans dan key pair.

Anda juga dapat mencadangkan dan memulihkan aplikasi Microsoft Windows berkemampuan VSS Anda. Anda dapat menjadwalkan pencadangan yang konsisten dengan aplikasi, menentukan kebijakan siklus hidup, dan melakukan pemulihan yang konsisten sebagai bagian dari pencadangan sesuai permintaan atau rencana pencadangan terjadwal. Untuk informasi selengkapnya, lihat Membuat cadangan Windows VSS.

AWS Backup tidak me-reboot instans EC2 Anda kapan saja.

Gambar dan snapshot

Saat mencadangkan instans Amazon EC2 AWS Backup , ambil snapshot dari volume penyimpanan Amazon EBS root, konfigurasi peluncuran, dan semua volume EBS terkait. AWS Backup menyimpan parameter konfigurasi tertentu dari instans EC2, termasuk jenis instans, grup keamanan, Amazon VPC, konfigurasi pemantauan, dan tag. Data cadangan disimpan sebagai Amazon Machine Image (AMI) yang didukung volume Amazon EBS.

Jika Anda menghapus snapshot Amazon Machine Image (AMI) atau Amazon EBS yang dikelola dengan AWS Backup menggunakan AWS Backup dan tempat sampah Amazon EC2 telah

dikonfigurasi, gambar atau snapshot mungkin dikenakan biaya sesuai kebijakan recycle bin Amazon EC2. Snapshot dan gambar di recycle bin Amazon EC2 tidak lagi dikelola AWS Backup oleh dan tidak akan dikelola AWS Backup oleh kebijakan jika Anda memulihkannya dari recycle bin.

AWS Backup snapshot Amazon EBS terkelola dan snapshot yang terkait dengan AWS Backup Amazon EC2 AMI terkelola yang menerapkan Amazon EBS Snapshot Lock mungkin tidak dihapus sebagai bagian dari siklus hidup titik pemulihan jika durasi kunci snapshot melebihi siklus hidup pencadangan. Sebaliknya, titik pemulihan ini akan berstatus`EXPIRED`. Poin pemulihan ini dapat dihapus secara manual jika Anda memilih untuk menghapus kunci snapshot Amazon EBS terlebih dahulu.

AWS Backup dapat mengenkripsi snapshot EBS yang terkait dengan cadangan Amazon EC2. Ini mirip dengan cara mengenkripsi snapshot EBS. AWS Backup menggunakan enkripsi yang sama yang diterapkan pada volume EBS yang mendasarinya saat membuat snapshot Amazon EC2 AMI, dan parameter konfigurasi instans asli dipertahankan dalam metadata pemulihan.

Sebuah snapshot memperoleh enkripsi dari volume, dan enkripsi yang sama diterapkan ke snapshot yang sesuai. Cuplikan EBS dari AMI yang disalin selalu dienkripsi. Jika Anda menentukan kunci KMS selama penyalinan, kunci yang ditentukan diterapkan. Jika Anda tidak menentukan kunci KMS, kunci KMS default diterapkan.

Untuk informasi selengkapnya, lihat instans Amazon EC2 di Panduan Pengguna Amazon EC2 dan enkripsi Amazon EBS di Panduan Pengguna Amazon EBS.

Bekerja dengan Amazon EFS

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

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan sumber daya Amazon EFS: Memulihkan sistem file Amazon EFS

Untuk informasi rinci tentang sistem file Amazon EFS, lihat Apa itu Amazon Elastic File System? di Panduan Pengguna Amazon Elastic File System.

Bekerja dengan Amazon EBS

AWS Backup mendukung volume Amazon Elastic Block Store (Amazon EBS).

AWS Backup snapshot Amazon EBS terkelola dan snapshot yang terkait dengan AWS Backup Amazon EC2 AMI terkelola yang menerapkan Amazon EBS Snapshot Lock mungkin tidak dihapus

sebagai bagian dari siklus hidup titik pemulihan jika durasi kunci snapshot melebihi siklus hidup pencadangan. Sebaliknya, titik pemulihan ini akan berstatus`EXPIRED`. Poin pemulihan ini dapat dihapus secara manual jika Anda memilih untuk menghapus kunci snapshot Amazon EBS terlebih dahulu.

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan volume Amazon EBS: Memulihkan volume Amazon EBS

Untuk informasi selengkapnya, lihat volume Amazon EBS di Panduan Pengguna Amazon EBS.

Bekerja dengan Amazon RDS dan Aurora

AWS Backup mendukung mesin database Amazon RDS dan cluster Aurora.

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan sumber daya Amazon RDS: Memulihkan database RDS
- Cara mengembalikan cluster Aurora: Memulihkan cluster Amazon Aurora

Untuk informasi selengkapnya tentang Amazon RDS, lihat Apa itu Amazon Relational Database Service? di Panduan Pengguna Amazon RDS.

Untuk informasi rinci tentang Aurora, lihat Apa itu Amazon Aurora? di Panduan Pengguna Amazon Aurora.

> **Note**
>
> Jika Anda memulai pekerjaan pencadangan dari konsol Amazon RDS, ini dapat bertentangan dengan pekerjaan pencadangan klaster Aurora, menyebabkan kesalahan Pekerjaan Backup berakhir sebelum selesai. Jika ini terjadi, konfigurasikan jendela cadangan yang lebih panjang di AWS Backup.

> **Note**
>
> Kustom RDS untuk SQL Server dan RDS Kustom untuk Oracle saat ini tidak didukung oleh. AWS Backup

> **Note**
>
> AWS tidak mengenakan biaya untuk snapshot Aurora yang disimpan di dalam brankas cadangan selama Aurora mengaktifkan pencadangan otomatis dan periode retensi untuk pencadangan otomatis Aurora lebih dari periode retensi snapshot Aurora. Setiap snapshot dalam brankas cadangan akan dikenakan biaya jika database snapshot dihapus (penghapusan dapat terjadi secara tidak sengaja atau selama penerapan biru/hijau). Snapshot besar dan backup yang sering dari database yang dihapus dapat mengakibatkan biaya penyimpanan yang signifikan. Kunjungi AWS Backup kalkulator untuk memperkirakan AWS Backup biaya potensial.

Bekerja dengan AWS BackInt

AWS Backup bekerja dengan AWS Backint untuk mendukung pencadangan dan pemulihan basis data SAP HANA pada instans Amazon EC2.

- Petunjuk untuk mencadangkan dan memulihkan sumber daya SAP HANA: SAP HANA Amazon EC2 Instans backup dan restore
- Mengatur AWS Backint Agent AWS : Backint Agent untuk SAP HANA

Bekerja dengan AWS Storage Gateway

AWS Backup mendukung Storage Gateway Volume Gateway. Anda juga dapat memulihkan snapshot Amazon EBS sebagai volume Storage Gateway.

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan sumber daya Storage Gateway:Memulihkan volume Storage Gateway.

Bekerja dengan Amazon DocumentDB

AWS Backup mendukung cluster Amazon DocumentDB.

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan sumber daya Amazon DocumentDB:. Memulihkan cluster DocumentDB

Bekerja dengan Amazon Neptunus

AWS Backup mendukung cluster Amazon Neptunus.

- Cara membuat cadangan sumber daya: Memulai dengan AWS Backup
- Cara mengembalikan cluster Amazon Neptunus:. Memulihkan cluster Neptunus

Bekerja dengan Amazon Timestream

AWS Backup mendukung tabel Amazon Timestream.

- Cara membuat cadangan tabel Timestream.
- Cara mengembalikan tabel Timestream.

Bekerja dengan AWS Organizations

AWS Backup bekerja dengan AWS Organizations untuk menyederhanakan pemantauan dan manajemen lintas akun

- Buat akun manajemen di Organizations.
- Aktifkan manajemen lintas akun.
- Tentukan akun administrator yang didelegasikan dan kebijakan delegasi.

Bekerja dengan AWS CloudFormation

AWS Backup AWS CloudFormation template dukungan dan tumpukan aplikasi

- AWS CloudFormation cadangan tumpukan

Bekerja dengan AWS BackInt, AWS Systems Manager untuk SAP, dan SAP HANA

AWS Backup bekerja dengan AWS BackInt dan dengan SSM untuk SAP untuk mendukung fungsi pencadangan dan pemulihan SAP HANA.

- Database SAP HANA di Amazon EC2 membuat cadangan instans

- Memulai dengan AWS Systems Manager SAP
- AWS Backint Agent untuk SAP HANA

Bagaimana AWS layanan mendukung sumber daya mereka sendiri

Anda dapat merujuk ke dokumentasi teknis untuk proses pencadangan dan pemulihan AWS layanan tertentu, terutama ketika, selama pemulihan, Anda perlu mengonfigurasi instance baru dari AWS layanan tersebut. Berikut ini adalah daftar dokumentasi:

- Layanan Terkait Amazon EC2
- Menggunakan AWS Backup dengan Amazon EFS
- Backup dan Restore Sesuai Permintaan untuk DynamoDB
- Cuplikan Amazon EBS
- Mencadangkan dan Memulihkan Instans Amazon RDS DB
  - Ikhtisar Mencadangkan dan Memulihkan Cluster Aurora DB
- Menggunakan AWS Backup dengan FSx for Windows File Server
- Menggunakan AWS Backup dengan FSx for Lustre
- Mencadangkan Volume Anda di AWS Storage Gateway
- Mencadangkan dan Memulihkan di Amazon DocumentDB
- Mencadangkan dan Memulihkan Cluster Amazon Neptunus

Pengukuran, biaya, dan penagihan

AWS Backup harga

AWS Backup Harga saat ini tersedia dengan AWS Backup harga.

> **Important**
>
> Untuk menghindari biaya tambahan, konfigurasikan kebijakan penyimpanan Anda dengan durasi penyimpanan hangat minimal satu minggu.
> Misalnya, asumsikan Anda mengambil cadangan harian dan menyimpannya selama satu hari. Selanjutnya, asumsikan bahwa sumber daya yang dilindungi Anda begitu besar sehingga dibutuhkan sepanjang hari untuk menyelesaikan cadangan Anda. AWS Backup mengimplementasikan periode retensi Anda satu hari dan menghapus cadangan Anda dari

penyimpanan hangat saat pekerjaan pencadangan Anda selesai. Keesokan harinya, AWS Backup tidak dapat membuat cadangan tambahan karena Anda tidak memiliki cadangan di penyimpanan hangat. Karena periode retensi ini tidak mengikuti praktik terbaik, Anda menghadapi risiko dan biaya untuk membuat cadangan penuh setiap hari.
Hubungi AWS Support untuk bantuan lebih lanjut.

AWS Backup penagihan

Ketika jenis sumber daya mendukung AWS Backup manajemen penuh, biaya untuk AWS Backup aktivitas (termasuk penyimpanan, transfer data, pemulihan, dan penghapusan awal) muncul di bagian “Cadangan” pada tagihan Anda. Amazon Web Services Untuk daftar layanan yang mendukung AWS Backup manajemen penuh, lihat bagian AWS Backup Manajemen lengkap dalam Ketersediaan fitur berdasarkan sumber daya tabel.

Ketika jenis sumber daya tidak mendukung AWS Backup manajemen penuh, beberapa AWS Backup aktivitas Anda seperti biaya penyimpanan untuk cadangan Anda, memiliki penagihan yang tercermin oleh layanan masing-masing. AWS

Salin kegagalan pekerjaan

Anda hanya akan dikenakan biaya setelah titik pemulihan dibuat di brankas tujuan. Tidak ada biaya ketika pekerjaan salinan gagal dan tidak ada titik pemulihan yang dibuat.

Tag alokasi biaya

Anda dapat menggunakan tag alokasi biaya untuk melacak dan mengoptimalkan AWS Backup biaya pada tingkat terperinci, dan melihat dan memfilter tag tersebut menggunakan AWS Cost Explorer.

Untuk menggunakan tag alokasi biaya, lihat Mengotomatiskan pencadangan dan mengoptimalkan biaya cadangan untuk Amazon EFS menggunakan AWS Backup dan Menggunakan Tag Alokasi Biaya.

AWS Backup Harga Audit Manager

AWS Backup Audit Manager mengenakan biaya untuk penggunaan berdasarkan jumlah evaluasi kontrol. Evaluasi kontrol adalah evaluasi satu sumber daya terhadap satu kontrol. Biaya evaluasi kontrol muncul di AWS Backup tagihan Anda. Untuk harga evaluasi kontrol saat ini, lihat AWS Backup harga.

Untuk menggunakan kontrol AWS Backup Audit Manager, Anda harus mengaktifkan AWS Config perekaman untuk melacak aktivitas pencadangan Anda. AWS Config biaya untuk setiap item konfigurasi yang dicatat, dan biaya ini muncul di AWS Config tagihan Anda. Untuk penetapan harga item konfigurasi saat ini, lihat AWS Config harga.

Harga Amazon Aurora

Selama periode retensi yang dikonfigurasi untuk pencadangan berkelanjutan Aurora (hingga 35 hari), snapshot tidak dikenakan biaya penyimpanan. Snapshot yang disimpan melewati jendela ini dibebankan sebagai cadangan penuh.

AWS Backup blog, video, tutorial, dan sumber daya lainnya

Untuk informasi selengkapnya AWS Backup, lihat berikut ini:

- Cadangkan dan pulihkan mesin virtual VMware lokal menggunakan. AWS Backup Dengan Olumuyiwa Koya dan Yehezkiel Oyerinde (Juni 2022).
- Menggunakan AWS Backup untuk melindungi database Amazon Aurora. Bersama Chris Hendon, Brandon Rubadou, dan Thomas Liddle (Mei 2022).
- Melindungi instans Amazon RDS terenkripsi dengan pencadangan lintas akun dan lintas wilayah. Dengan Evan Peck dan Sabith Venkitachalapathy (Mei 2022).
- Otomatiskan dan tingkatkan postur keamanan Anda menggunakan AWS Backup dan AWS PrivateLink. Bersama Bilal Alam (April 2022).
- Dapatkan pelaporan AWS Backup multi-wilayah lintas akun harian agregat. Dengan Wali Akbari dan Sabith Venkitachalapathy (Februari 2022).
- Otomatiskan visibilitas temuan cadangan menggunakan AWS Backup dan. AWS Security Hub Dengan Kanishk Mahajan (Januari 2022).
- 10 praktik terbaik keamanan teratas untuk mengamankan cadangan di. AWS Dengan Ibukun Oyewumi (Januari 2022).
- Mengoptimalkan SAS Grid AWS dengan FSx for Lustre (dan mengoptimalkan pemulihan bencana menggunakan). AWS Backup Dengan Matt Saeger dan Shea Lutton (Januari 2022).
- Memusatkan perlindungan dan kepatuhan data di Amazon AWS Backup Neptunus dengan. Dengan Brian O'Keefe (November 2021).
- Kelola pencadangan dan pemulihan Amazon DocumentDB (dengan kompatibilitas MongoDB) dengan. AWS Backup Dengan Karthik Vijayraghavan (November 2021).

- Sederhanakan audit kebijakan perlindungan data Anda dengan AWS Backup Audit Manager. Bersama Jordan Bjorkman dan Harshitha Putta (November 2021).
- Tingkatkan postur keamanan cadangan Anda dengan AWS Backup Vault Lock. Dengan Rolland Miller (Oktober 2021).
- Cara mempertahankan tag sumber daya dalam AWS Backup memulihkan pekerjaan. Dengan Ibukun Oyewumi, Amee Shah, dan Sabith Venkitachalapathy (Sep. 2021).
- Mengelola akses ke cadangan menggunakan kebijakan kontrol layanan dengan. AWS Backup Dengan Sabith Venkitachalapathy dan Ibukun Oyewumi (Agustus 2021).
- Otomatiskan pencadangan terpusat pada skala di seluruh AWS layanan yang menggunakan. AWS Backup Dengan Ibukun Oyewumi dan Sabith Venkitachalapathy (Juli 2021).
- Blog: Cara menyederhanakan backup Microsoft SQL Server menggunakan AWS Backup dan VSS. Bersama Siavash Irani dan Sepehr Samiei (Juli 2021).
- Otomatiskan validasi pemulihan data dengan. AWS Backup Dengan Mahanth Jayadeva (Juni 2021).
- Mengkonfigurasi notifikasi untuk memantau AWS Backup pekerjaan. Dengan Virgil Ennes (Juni 2021).
- Mengotomatiskan pencadangan dan mengoptimalkan biaya pencadangan untuk Amazon EFS menggunakan. AWS Backup Dengan Prachi Gupta dan Rohit Verma (Juni 2021).
- Kelola biaya cadangan Amazon EFS: AWS Backup dukungan untuk tag alokasi biaya. Dengan Aditya Maruvada (Mei 2021).
- Buat dan bagikan cadangan terenkripsi di seluruh akun dan Wilayah menggunakan. AWS Backup Dengan Prachi Gupta (Mei 2021).
- AWS Backup sekarang FedRAMP High disetujui untuk kepatuhan dan kebutuhan perlindungan data Anda. Dengan Andy Grimes (Mei 2021).
- ZS Associates meningkatkan efisiensi pencadangan dengan. AWS Backup Bersama Mitesh Naik, Hiranand Mulchandani, dan Sushant Jadhav (Mei 2021).
- Tutorial: Amazon EBS Backup dan Restore menggunakan AWS Backup. Dengan Fathima Kamal (April 2021).
- Video Tutorial: Mengelola Salinan Cadangan Lintas Wilayah. Dengan David DeLuca (April 2021).
- Hapus beberapa titik AWS Backup pemulihan menggunakan AWS Alat untuk PowerShell. Dengan Sherif Talaat (April 2021).
- Pencadangan lintas wilayah dan lintas akun untuk Amazon FSx menggunakan. AWS Backup Dengan Adam Hunter dan Fathima Kamal (April 2021).

- CloudWatch Acara dan Metrik Amazon untuk AWS Backup. Dengan Rolland Miller (Maret 2021).
- Tutorial: Amazon Relational Database Service (RDS) Backup and Restore menggunakan. AWS Backup Dengan Fathima Kamal (Maret 2021).
- oint-in-time Pemulihan P dan pencadangan berkelanjutan untuk Amazon RDS dengan AWS Backup. Dengan Kelly Griffin (Maret 2021).
- Otomatisasi AWS Backup dengan AWS Service Catalog. dengan John Husemoller (Januari 2021).
- Pemulihan data aman dengan pencadangan lintas akun dan salinan Lintas Wilayah menggunakan. AWS Backup Dengan Cher Simon (Januari 2021).
- AWS Re: Invent recap: Perlindungan data dan kepatuhan dengan. AWS Backup Dengan Nancy Wang (Desember 2020).
- AWS Backup menyediakan perlindungan data terpusat di seluruh AWS sumber daya Anda. Dengan Nancy Wang (November 2020).
- Tech Talk: Perlindungan data dalam skala besar dengan AWS Backup. Dengan Kareem Behairy (Sep. 2020).
- Manajemen lintas akun terpusat dengan menggunakan salinan lintas wilayah. AWS Backup Dengan Cher Simon (Sep. 2020).
- Video Tutorial: Mengelola backup dalam skala yang Anda AWS Organizations gunakan. AWS Backup Dengan Ildar Sharafeev (Juli 2020).
- Mengelola cadangan dalam skala besar dalam penggunaan Anda AWS Organizations. AWS Backup Bersama Nancy Wang, Avi Drabkin, Ganesh Sundaresan, dan Vikas Shah (Juni 2020).
- Pulihkan file dan folder Amazon EFS dengan file AWS Backup. Bersama Abrar Hussain dan Gurudath Pai (Mei 2020).
- Menjadwalkan pencadangan otomatis menggunakan Amazon EFS dan. AWS Backup Bersama Rob Barnes (Desember 2019).
- Re: Invent Recording: AWS Re:Invent 2019: Menyelam jauh di ft. AWS Backup Ruang rak. Bersama Nancy Wang dan Jason Pavao (Desember 2019).
- Melindungi data Anda dengan AWS Backup Dengan Anthony Fiore (Juli 2019).
- Video Pemasaran: Memperkenalkan AWS Backup. Januari 2019.
- Video: Pengantar AWS Backup. Dengan AWS Pelatihan dan Sertifikasi.

Menyiapkan AWS untuk pertama kalinya

Sebelum Anda menggunakan AWS Backup untuk pertama kalinya, selesaikan tugas-tugas berikut:

1. Mendaftar untuk AWS
2. Mmebuat pengguna IAM
3. Membuat peran IAM

Mendaftar untuk AWS

Ketika Anda mendaftar ke Amazon Web Services (AWS), Anda Akun AWS secara otomatis mendaftar untuk semua layanan AWS, termasuk AWS Backup. Anda hanya membayar biaya layanan yang Anda gunakan.

Untuk informasi selengkapnya tentang tarif AWS Backup penggunaan, lihat halaman AWS Backup Harga.

Jika Anda Akun AWS sudah memiliki, lompat ke tugas berikutnya. Jika Anda belum memiliki akun AWS , gunakan prosedur berikut untuk membuatnya.

Untuk membuat Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

Catat Akun AWS nomor Anda, karena Anda akan membutuhkannya untuk tugas berikutnya.

Mmebuat pengguna IAM

Layanan di AWS, seperti AWS Backup, mengharuskan Anda memberikan kredensyal saat Anda mengaksesnya, sehingga layanan dapat menentukan apakah Anda memiliki izin untuk mengakses sumber dayanya. AWS merekomendasikan agar Anda tidak menggunakan pengguna Akun AWS root untuk membuat permintaan. Sebagai gantinya, buat pengguna IAM, dan berikan akses penuh kepada pengguna tersebut. Kami menyebut pengguna ini sebagai pengguna administrator. Anda dapat menggunakan kredensyal pengguna admin, bukan kredensyal pengguna Akun AWS root, untuk berinteraksi AWS dan melakukan tugas, seperti membuat bucket, membuat pengguna, dan memberi mereka izin. Untuk informasi selengkapnya, lihat Kredensyal Pengguna Akun AWS Root vs. Kredensyal Pengguna IAM di Referensi AWS Umum dan Praktik Terbaik IAM dalam Panduan Pengguna IAM.

Jika Anda mendaftar AWS tetapi belum membuat pengguna IAM untuk diri Anda sendiri, Anda dapat membuatnya menggunakan konsol IAM.

Untuk membuat pengguna administrator, pilih salah satu opsi berikut.

Pilih salah satu cara untuk mengelola administrator Anda	Untuk	Oleh	Anda juga bisa
Di Pusat Identitas IAM (Direkomendasikan)	Gunakan kredensyal jangka pendek untuk mengakses. AWS Ini sejalan dengan praktik terbaik keamanan. Untuk informasi tentang praktik terbaik, lihat Praktik terbaik	Mengikuti petunjuk di Memulai di Panduan AWS IAM Identity Center Pengguna.	Konfigurasikan akses terprogram dengan Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center dalam AWS Command Line Interface Panduan Pengguna.

Pilih salah satu cara untuk mengelola administrator Anda	Untuk	Oleh	Anda juga bisa
	keamanan di IAM di Panduan Pengguna IAM.		
Di IAM (Tidak direkomendasikan)	Gunakan kredensyal jangka panjang untuk mengakses. AWS	Mengikuti petunjuk dalam Membuat pengguna admin IAM pertama Anda dan grup pengguna di Panduan Pengguna IAM.	Konfigurasikan akses terprogram dengan Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Untuk masuk sebagai pengguna IAM baru ini, keluar dari. AWS Management Console Kemudian gunakan URL berikut, di mana your_aws_account_id adalah Akun AWS nomor Anda tanpa tanda hubung (misalnya, jika nomor Anda, ID Anda adalah): Akun AWS `1234-5678-9012` Akun AWS `123456789012`

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

Masukkan nama pengguna dan kata sandi IAM yang baru saja Anda buat. Saat Anda masuk, bilah navigasi menampilkan your_user_name@your_aws_account_id.

Jika Anda tidak ingin URL untuk halaman login Anda berisi Akun AWS ID Anda, Anda dapat membuat alias akun. Dari dasbor IAM, klik Buat Alias Akun dan masukkan alias, seperti nama perusahaan Anda. Untuk masuk setelah membuat alias akun, gunakan URL berikut:

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

Untuk memverifikasi tautan masuk untuk pengguna IAM untuk akun Anda, buka konsol IAM dan periksa di Alias Akun AWS di dasbor.

Membuat peran IAM

Anda dapat menggunakan konsol IAM untuk membuat peran IAM yang memberikan AWS Backup izin untuk mengakses sumber daya yang didukung. Setelah Anda membuat peran IAM, Anda akan membuat dan melampirkan kebijakan ke peran tersebut.

Untuk membuat peran IAM dengan konsol

1. Masuk ke Konsol AWS Manajemen dan buka konsol IAM.
2. Di konsol IAM, pilih Peran di panel navigasi, dan pilih Buat peran.
3. Pilih Peran AWS Layanan, lalu pilih Pilih untuk AWS Backup. Pilih Berikutnya: Izin.
4. Pada halaman Lampirkan kebijakan izin, periksa keduanya`AWSBackupServiceRolePolicyForBackup`, dan`AWSBackupServiceRolePolicyForRestores`. Kebijakan AWS terkelola ini memberikan AWS Backup izin untuk mencadangkan dan memulihkan semua AWS sumber daya yang didukung. Untuk mempelajari selengkapnya tentang kebijakan terkelola dan melihat contoh, lihat Kebijakan Terkelola.

   Kemudian, pilih Berikutnya: Tag.
5. Pilih Berikutnya: Tinjau.
6. Untuk Nama Peran, ketikkan nama yang menjelaskan tujuan peran ini. Nama peran harus unik di dalam diri Anda Akun AWS. Karena berbagai entitas mungkin mereferensikan peran, Anda tidak dapat mengedit nama peran setelah Anda membuatnya.

   Pilih Buat peran.
7. Pada halaman Peran, pilih peran yang Anda buat untuk membuka halaman detailnya.

Memulai dengan AWS Backup

Tutorial ini menunjukkan langkah-langkah umum untuk menggunakan AWS Backup fitur dan fungsionalitas. Seperti halnya bagian mana pun dari dokumentasi teknis ini, Anda harus mengikuti Konsol AWS Manajemen di jendela lain.

Anda juga dapat mempelajari cara menggunakan AWS Backup dengan layanan tertentu dengan membaca tutorial ini:

- Amazon Relational Database Service (Amazon RDS) Backup dan Restore menggunakan AWS Backup
- Tutorial: Amazon EBS Backup dan Restore menggunakan AWS Backup

Topik

Prasyarat

Sebelum Anda mulai, pastikan Anda memiliki yang berikut:

- Sebuah Akun AWS. Untuk informasi selengkapnya, lihat Menyiapkan AWS untuk pertama kalinya.
- Setidaknya satu sumber daya yang didukung oleh AWS Backup.
- Anda harus terbiasa dengan AWS layanan dan sumber daya yang Anda cadangkan. Lihat daftar AWS sumber daya yang didukung dan aplikasi pihak ketiga.

Ketika AWS layanan baru tersedia, memungkinkan AWS Backup untuk menggunakan layanan tersebut.

Untuk mengkonfigurasi AWS layanan yang akan digunakan AWS Backup

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pada halaman keikutsertaan Layanan, pilih Konfigurasi sumber daya.
4. Pada halaman Konfigurasi sumber daya, gunakan sakelar sakelar untuk mengaktifkan atau menonaktifkan layanan yang digunakan. AWS Backup Pilih Konfirmasi saat layanan Anda dikonfigurasi. Pastikan bahwa AWS layanan yang Anda pilih tersedia di Anda Wilayah AWS.

Lihat Menetapkan sumber daya ke rencana cadangan untuk informasi tambahan. AWS Backup Konsol memungkinkan pengguna untuk menetapkan jenis sumber daya ke paket cadangan; ini akan disertakan bahkan jika keikutsertaan tidak diaktifkan untuk layanan tertentu.

- Pastikan bahwa sumber daya yang Anda cadangkan semuanya sama Wilayah AWS.

Untuk menyelesaikan tutorial ini, Anda dapat menggunakan pengguna Akun AWS root Anda untuk masuk ke file AWS Management Console. Namun, AWS Identity and Access Management (IAM) merekomendasikan agar Anda tidak menggunakan pengguna Akun AWS root. Sebagai gantinya, buat administrator di akun Anda dan gunakan kredensyal tersebut untuk mengelola sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Menyiapkan AWS untuk pertama kalinya.

AWS Backup Konsol menyediakan opsi berbeda untuk mencadangkan sumber daya Anda. Anda dapat membuat cadangan sesuai permintaan, menjadwalkan, dan mengonfigurasi cara Anda ingin sumber daya dicadangkan, atau mengonfigurasi sumber daya untuk dicadangkan secara otomatis saat sumber daya dibuat.

Memulai 1: Layanan Opt-in

AWS Backup Konsol memiliki dua cara untuk menyertakan jenis sumber daya dalam rencana cadangan: secara eksplisit menetapkan jenis sumber daya dalam rencana cadangan atau menyertakan semua sumber daya. Lihat poin di bawah ini untuk memahami cara kerja pilihan ini dengan layanan opt in.

- Jika penetapan sumber daya hanya didasarkan pada tag, maka pengaturan keikutsertaan layanan diterapkan.
- Jika jenis sumber daya secara eksplisit ditetapkan ke rencana cadangan, itu akan disertakan dalam cadangan meskipun keikutsertaan tidak diaktifkan untuk layanan tertentu. Ini tidak berlaku untuk Aurora, Neptunus, dan Amazon DocumentDB. Agar layanan ini disertakan, keikutsertaan harus diaktifkan.
- Jika kedua jenis sumber daya dan tag ditentukan dalam penetapan sumber daya, jenis sumber daya yang ditentukan difilter terlebih dahulu, lalu tag lebih lanjut memfilter sumber daya tersebut.

  Pengaturan keikutsertaan layanan diabaikan untuk sebagian besar jenis sumber daya. Namun Aurora, Neptunus, dan Amazon DocumentDB memerlukan layanan opt-in.
- Untuk Amazon FSx untuk NetApp ONTAP, saat menggunakan pemilihan sumber daya berbasis tag, terapkan tag ke volume individual alih-alih seluruh sistem file.

Pilihan keikutsertaan berlaku untuk akun tertentu dan Wilayah AWS. Saat akun menggunakan AWS Backup (membuat brankas cadangan atau paket cadangan) di Wilayah, akun secara otomatis dipilih ke semua jenis sumber daya yang didukung oleh AWS Backup di Wilayah pada saat itu. Layanan yang didukung yang ditambahkan ke Wilayah tersebut di kemudian hari tidak akan secara otomatis disertakan dalam paket cadangan. Anda dapat memilih untuk memilih jenis sumber daya tersebut setelah didukung.

Karena AWS Backup mendukung semakin banyak AWS layanan dan aplikasi pihak ketiga, Anda mungkin perlu meninjau kembali langkah ini untuk ikut serta dalam sumber daya yang baru didukung tersebut.

AWS Backup tidak mengatur atau mengelola cadangan yang diambil di AWS lingkungan selain. AWS Backup

Untuk ikut serta dalam penggunaan AWS Backup untuk melindungi semua jenis sumber daya yang didukung

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Di bawah Keikutsertaan layanan, pilih Konfigurasi sumber daya.
4. Pilih semua Sumber Daya yang AWS Backup didukung dengan memindahkan semua sakelar ke kanan.

5. Pilih Konfirmasi.

Langkah selanjutnya

Untuk membuat cadangan sesuai permintaan menggunakan AWS Backup, lanjutkan keMemulai 2: Buat cadangan sesuai permintaan.

Memulai 2: Buat cadangan sesuai permintaan

Di AWS Backup konsol, halaman Sumber daya yang dilindungi mencantumkan sumber daya yang telah dicadangkan AWS Backup setidaknya sekali. Jika Anda menggunakan AWS Backup untuk pertama kalinya, tidak ada sumber daya apa pun, seperti volume Amazon EBS atau database Amazon RDS, yang tercantum di halaman ini. Ini benar bahkan jika sumber daya itu ditetapkan ke rencana cadangan jika rencana cadangan itu belum menjalankan pekerjaan pencadangan terjadwal setidaknya sekali.

Pada langkah pertama ini, Anda membuat cadangan sesuai permintaan dari salah satu sumber daya Anda. Anda kemudian akan melihat sumber daya ini terdaftar di halaman Sumber daya yang dilindungi.

Untuk membuat cadangan sesuai permintaan

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Menggunakan panel navigasi, pilih Sumber daya yang dilindungi, lalu Buat cadangan sesuai permintaan.
3. Pada halaman Buat cadangan sesuai permintaan, pilih jenis sumber daya yang ingin Anda cadangkan; misalnya, pilih DynamoDB untuk tabel Amazon DynamoDB.
4. Pilih nama atau ID sumber daya yang ingin Anda lindungi. Pastikan sumber daya yang Anda pilih adalah yang Anda inginkan.

> **Note**
>
> Untuk jenis penerapan Amazon FSx for Lustre, Persistent dan Persistent_2 didukung.

5. Pastikan bahwa Buat cadangan sekarang dipilih. Ini segera memulai pencadangan dan memungkinkan Anda melihat sumber daya yang disimpan lebih cepat di halaman Sumber daya yang dilindungi.
6. Tentukan transisi ke nilai penyimpanan dingin (jika sesuai) dan nilai kedaluwarsa.

> **Note**
>
> - Untuk melihat daftar sumber daya yang dapat Anda transisi ke penyimpanan dingin, lihat bagian “Siklus Hidup ke penyimpanan dingin” pada Ketersediaan fitur berdasarkan sumber daya tabel. Semua jenis sumber daya lainnya disimpan ke penyimpanan hangat, dan abaikan transisi ke ekspresi penyimpanan dingin. Nilai kedaluwarsa berlaku untuk semua jenis sumber daya.
> - Saat pencadangan kedaluwarsa dan ditandai untuk dihapus sebagai bagian dari kebijakan siklus hidup Anda, AWS Backup hapus cadangan pada titik yang dipilih secara acak selama 8 jam berikutnya. Jendela ini membantu memastikan kinerja yang konsisten.

7. Pilih brankas cadangan yang ada. Memilih Buat brankas cadangan baru membuka halaman baru untuk membuat brankas dan kemudian mengembalikan Anda ke halaman Buat cadangan sesuai permintaan setelah Anda selesai.
8. Di bawah peran IAM, pilih Peran default.

> **Note**
>
> Jika peran AWS Backup default tidak ada di akun Anda, peran dibuat untuk Anda dengan izin yang benar.

9. Jika Anda ingin menetapkan satu atau beberapa tag ke cadangan sesuai permintaan, masukkan kunci dan nilai opsional, lalu pilih Tambah tag.

> **Note**
>
> - Untuk sumber daya Amazon EC2, AWS Backup secara otomatis menyalin tag sumber daya grup dan individu yang ada, selain tag apa pun yang Anda tambahkan ke cadangan ini. Untuk informasi selengkapnya, lihat Menyalin tag ke cadangan.

- Saat membuat paket cadangan berbasis tag, jika Anda memilih peran selain peran Default, pastikan bahwa ia memiliki izin yang diperlukan untuk mencadangkan semua sumber daya yang ditandai. AWS Backup mencoba memproses semua sumber daya dengan tag yang dipilih. Jika menemukan sumber daya yang tidak memiliki izin untuk mengaksesnya, paket cadangan gagal.

10. Pilih Buat cadangan sesuai permintaan. Ini membawa Anda ke halaman Pekerjaan, di mana Anda akan melihat daftar pekerjaan.
11. Jika jenis sumber daya Anda adalah EC2, bagian Pengaturan cadangan lanjutan akan muncul. Pilih Windows VSS jika instans EC2 Anda menjalankan Microsoft Windows. Ini memungkinkan Anda untuk mengambil cadangan Windows VSS yang konsisten dengan aplikasi.

> **Note**
>
> AWS Backup saat ini mendukung pencadangan sumber daya yang konsisten aplikasi yang berjalan di Amazon EC2 saja. Tidak semua jenis instans atau aplikasi didukung untuk cadangan Windows VSS. Untuk informasi selengkapnya, lihat Membuat cadangan Windows VSS.

12. Pilih ID pekerjaan Backup untuk sumber daya yang Anda pilih untuk dicadangkan untuk melihat detail pekerjaan itu.

Langkah selanjutnya

Untuk mengotomatiskan aktivitas pencadangan Anda, lanjutkan keMemulai 3: Buat cadangan terjadwal.

Memulai 3: Buat cadangan terjadwal

Pada langkah AWS Backup tutorial ini, Anda membuat rencana cadangan, menetapkan sumber daya untuk itu, dan kemudian membuat brankas cadangan.

Sebelum Anda mulai, pastikan Anda memiliki prasyarat yang diperlukan. Untuk informasi selengkapnya, lihat Memulai dengan AWS Backup.

Topik

- Langkah 1: Buat rencana cadangan berdasarkan yang sudah ada

- Langkah 2: Tetapkan sumber daya ke rencana cadangan
- Langkah 3: Buat brankas cadangan
- Langkah selanjutnya

Langkah 1: Buat rencana cadangan berdasarkan yang sudah ada

Rencana cadangan adalah ekspresi kebijakan yang menentukan kapan dan bagaimana Anda ingin mencadangkan AWS sumber daya Anda, seperti tabel Amazon DynamoDB atau sistem file Amazon Elastic File System (Amazon EFS). Anda menetapkan sumber daya ke rencana cadangan, dan AWS Backup kemudian secara otomatis mencadangkan dan mempertahankan cadangan untuk sumber daya tersebut sesuai dengan rencana cadangan. Untuk informasi selengkapnya, lihat Mengelola cadangan menggunakan rencana cadangan.

Ada dua cara untuk membuat rencana cadangan baru: Anda dapat membuat satu dari awal atau membuat satu berdasarkan rencana cadangan yang ada. Contoh ini menggunakan AWS Backup konsol untuk membuat rencana cadangan dengan memodifikasi rencana cadangan yang ada.

Untuk membuat rencana cadangan dari yang sudah ada

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Dari dasbor, pilih Kelola paket Cadangan. Atau, menggunakan panel navigasi, pilih Paket Backup dan pilih Buat paket Backup.
3. Pilih Mulai dengan templat, pilih paket dari daftar (misalnya,`Daily-Monthly-1yr-Retention`), dan masukkan nama di kotak Nama paket Backup.

   > **Note**
   >
   > Jika Anda mencoba membuat rencana cadangan yang identik dengan rencana yang ada, Anda mendapatkan `AlreadyExistsException` kesalahan.

4. Pada halaman ringkasan paket, pilih aturan cadangan yang Anda inginkan, lalu pilih Edit.
5. Tinjau dan pilih nilai yang Anda inginkan untuk aturan Anda (lihat Opsi dan konfigurasi paket Backup opsi aturan).
6. Untuk brankas cadangan, pilih Default atau pilih Create new Backup vault untuk membuat brankas baru.

7. (Opsional) - pilih Wilayah AWS dari daftar di Wilayah tujuan untuk menyalin cadangan ke Wilayah yang berbeda. Untuk menambahkan lebih banyak Wilayah, pilih Tambahkan salinan.
8. Setelah selesai mengedit aturan, pilih Save Backup rule.

Pada halaman Ringkasan, pilih Tetapkan sumber daya untuk mempersiapkan bagian berikutnya.

Langkah 2: Tetapkan sumber daya ke rencana cadangan

Setelah Anda membuat rencana cadangan, Anda harus menetapkan AWS sumber daya Anda ke rencana cadangan itu. Untuk informasi selengkapnya tentang menetapkan sumber daya, lihatMenetapkan sumber daya ke rencana cadangan.

Jika Anda belum memiliki AWS sumber daya yang ingin Anda tetapkan ke rencana cadangan, buat beberapa sumber daya baru untuk digunakan untuk latihan ini. Buat satu atau dua sumber daya menggunakan sumber AWS daya yang didukung dan aplikasi pihak ketiga.

Untuk menetapkan sumber daya ke rencana cadangan

1. Langkah-langkah sebelumnya seharusnya membawa Anda ke halaman Tetapkan sumber daya.
2. Ketik nama tugas Sumber Daya.
3. Untuk peran IAM, pilih Peran default. Jika Anda memilih peran lain, itu harus memiliki izin untuk mencadangkan semua sumber daya yang Anda tetapkan.
4. Di bagian Tetapkan sumber daya, pilih Sertakan semua jenis sumber daya. Jenis sumber daya adalah AWS layanan yang AWS Backup didukung atau aplikasi pihak ketiga. Paket cadangan ini sekarang akan melindungi semua jenis sumber daya yang telah Anda pilih untuk dilindungi AWS Backup
5. Pilih Tetapkan sumber daya.

Anda kembali ke halaman Ringkasan rencana cadangan. Pilih Buat rencana cadangan untuk menerapkan rencana cadangan pertama Anda!

Langkah 3: Buat brankas cadangan

Alih-alih menggunakan brankas cadangan default yang dibuat secara otomatis untuk Anda di AWS Backup konsol, Anda dapat membuat brankas cadangan khusus untuk menyimpan dan mengatur grup cadangan di brankas yang sama.

Untuk informasi selengkapnya tentang brankas cadangan, lihat. Brankas cadangan

Untuk membuat brankas cadangan

1. Di AWS Backup konsol, di panel navigasi, pilih Backup vaults.

   > **Note**
   >
   > Jika panel navigasi tidak terlihat di sisi kiri, Anda dapat membukanya dengan memilih ikon menu di sudut kiri atas konsol. AWS Backup

2. Pilih Buat brankas cadangan.
3. Masukkan nama untuk brankas cadangan Anda. Anda dapat memberi nama brankas Anda untuk mencerminkan apa yang akan Anda simpan di dalamnya, atau untuk membuatnya lebih mudah untuk mencari cadangan yang Anda butuhkan. Misalnya, Anda bisa menamainya**`FinancialBackups`**.
4. Pilih tombol AWS Key Management Service (AWS KMS). Anda dapat menggunakan salah satu kunci yang sudah Anda buat, atau pilih kunci AWS Backup KMS default.

   > **Note**
   >
   > AWS KMS Kunci yang ditentukan di sini hanya berlaku untuk cadangan layanan yang mendukung enkripsi AWS Backup independen. Untuk melihat daftar jenis sumber daya yang mendukung enkripsi AWS Backup independen, lihat bagian “ AWS Backup Manajemen penuh” pada Ketersediaan fitur berdasarkan sumber daya tabel.

5. Secara opsional, tambahkan tag yang akan membantu Anda mencari dan mengidentifikasi brankas cadangan Anda. Misalnya, Anda bisa menambahkan **`BackupType:Financial`** tag.
6. Pilih Buat brankas Cadangan.
7. Di panel navigasi, pilih Backup vaults, dan verifikasi bahwa brankas cadangan Anda telah ditambahkan.

> **Note**
>
> Anda sekarang dapat mengedit aturan cadangan di salah satu rencana cadangan Anda untuk menyimpan cadangan yang dibuat oleh aturan itu di brankas cadangan yang baru saja Anda buat.

Langkah selanjutnya

Untuk mencadangkan sistem file Amazon EFS secara khusus, lanjutkan keMemulai 4: Buat cadangan otomatis Amazon EFS.

Memulai 4: Buat cadangan otomatis Amazon EFS

Saat Anda membuat sistem file Amazon Elastic File System (Amazon EFS) menggunakan konsol Amazon EFS, pencadangan otomatis diaktifkan secara default. Jika Anda ingin secara otomatis mencadangkan sistem file Amazon EFS yang ada, Anda dapat melakukannya menggunakan konsol Amazon EFS, API, atau CLI.

Untuk secara otomatis mencadangkan sistem file Amazon EFS yang ada menggunakan konsol

1. Buka konsol Amazon EFS dihttps://console.aws.amazon.com/efs.
2. Pada halaman Sistem file, pilih sistem file untuk mengaktifkan backup otomatis.
3. Pilih Edit di panel Pengaturan umum.
4. Untuk mengaktifkan pencadangan otomatis, pilih Aktifkan pencadangan otomatis.

Pengaturan paket cadangan default adalah`daily backups, 35-day retention`. Jendela cadangan default (kerangka waktu saat pencadangan akan berjalan) diatur untuk dimulai pada pukul 5 pagi UTC (Waktu Universal Terkoordinasi) dan berlangsung 8 jam.

> **Note**
>
> Brankas cadangan otomatis Amazon EFS hanya `aws/efs/automatic-backup-vault` disediakan untuk pencadangan otomatis tersebut.
> Vault ini tidak boleh digunakan untuk membuat salinan lintas akun atau sebagai tujuan pencadangan yang dibuat oleh paket cadangan non-otomatis lainnya. Jika Anda menggunakannya sebagai tujuan untuk paket cadangan lainnya, Anda akan menerima kesalahan “hak istimewa yang tidak memadai”.

AWS Backup membuat peran terkait layanan atas nama Anda di akun Anda. Peran ini memiliki izin yang diperlukan untuk melakukan backup Amazon EFS. Untuk informasi terperinci tentang peran terkait layanan, lihat. Menggunakan peran terkait layanan untuk AWS Backup

Untuk step-by-step petunjuk tentang cara mengaktifkan atau menonaktifkan pencadangan otomatis menggunakan konsol, API, atau CLI Amazon EFS, lihat Pencadangan otomatis di Panduan Pengguna Amazon Elastic File System.

Langkah selanjutnya

Untuk melihat cadangan yang telah Anda buat, lanjutkan ke. Memulai 5: Lihat pekerjaan cadangan dan titik pemulihan

Memulai 5: Lihat pekerjaan cadangan dan titik pemulihan

Dengan AWS Backup, Anda dapat melihat status dan detail lain dari aktivitas pencadangan dan pemulihan di seluruh AWS layanan yang Anda gunakan.

Di AWS Backup dasbor, Anda dapat mengelola rencana cadangan, membuat cadangan sesuai permintaan, memulihkan cadangan, dan melihat status pencadangan dan pemulihan pekerjaan.

Topik

Lihat status pekerjaan cadangan

Gunakan AWS Backup dasbor untuk melihat status aktivitas pencadangan dan pemulihan Anda dengan cepat.

Untuk melihat status pekerjaan cadangan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Dasbor.
3. Untuk melihat status pekerjaan cadangan Anda, pilih Detail pekerjaan Backup. Ini akan membawa Anda ke halaman Backup jobs, di mana Anda dapat melihat tabel yang berisi pekerjaan cadangan dan memulihkan pekerjaan.

4. Anda dapat memfilter pekerjaan yang ditampilkan berdasarkan waktu. Misalnya, pekerjaan dibuat dalam 24 jam terakhir, minggu terakhir, atau 30 hari terakhir. Anda juga dapat mengatur jumlah pekerjaan yang akan ditampilkan per halaman dengan memilih ikon roda gigi.

Lihat semua cadangan di brankas

Ikuti langkah-langkah ini untuk melihat cadangan yang dibuat di brankas tertentu di. AWS Backup

Untuk melihat semua cadangan di brankas

1. Di AWS Backup konsol, di panel navigasi, pilih Backup vaults.
2. Pilih brankas yang Anda gunakan saat membuat cadangan sesuai permintaan atau terjadwal, dan lihat semua cadangan yang dibuat di brankas ini.

> **Note**
>
> Setiap cadangan memiliki Status, yang biasanya Selesai. Jika karena alasan tertentu tidak AWS Backup dapat menghapus cadangan sesuai dengan konfigurasi siklus hidupnya, itu menandai cadangan ini sebagai Kedaluwarsa. Anda ditagih untuk penyimpanan yang dikonsumsi cadangan kedaluwarsa dan harus menghapusnya.

Lihat detail sumber daya yang dilindungi

Di halaman Sumber daya yang dilindungi, Anda dapat menjelajahi detail sumber daya yang dicadangkan AWS Backup.

Untuk melihat sumber daya yang dilindungi

1. Di AWS Backup konsol, di panel navigasi, pilih Sumber daya yang dilindungi.
2. Lihat AWS sumber daya yang sedang didukung. Pilih sumber daya dalam daftar untuk menjelajahi cadangan Anda untuk sumber daya tersebut.

Langkah selanjutnya

Untuk mengembalikan titik pemulihan yang telah Anda lihat, lanjutkan keMemulai 6: Kembalikan cadangan.

Memulai 6: Kembalikan cadangan

Setelah sumber daya telah dicadangkan setidaknya sekali, itu dianggap dilindungi dan tersedia untuk dipulihkan menggunakan AWS Backup. Ikuti langkah-langkah ini untuk memulihkan sumber daya menggunakan AWS Backup konsol.

Untuk informasi tentang memulihkan parameter untuk layanan tertentu, atau memulihkan cadangan menggunakan AWS CLI atau AWS Backup API, lihat Memulihkan Cadangan.

Untuk memulihkan sumber daya

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi dan ID sumber daya yang ingin Anda pulihkan.
3. Daftar titik pemulihan Anda, termasuk jenis sumber daya, ditampilkan oleh ID Sumber Daya. Pilih sumber daya untuk membuka halaman Detail sumber daya.
4. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.
5. Tentukan parameter pemulihan. Parameter pemulihan yang ditampilkan khusus untuk jenis sumber daya yang dipilih.

   > **Note**
   >
   > Jika Anda hanya menyimpan satu cadangan, Anda hanya dapat mengembalikan ke keadaan sistem file pada saat Anda mengambil cadangan itu. Anda tidak dapat mengembalikan ke backup inkremental sebelumnya.

   Untuk petunjuk tentang cara memulihkan sumber daya tertentu, lihat Memulihkan cadangan.
6. Untuk Memulihkan peran, pilih Peran default.

   > **Note**
   >
   > Jika peran AWS Backup default tidak ada di akun Anda, peran dibuat untuk Anda dengan izin yang benar.
7. Pilih Pulihkan cadangan.

Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.

> **Note**
>
> Saat Anda melakukan pemulihan untuk memulihkan item tertentu dalam instans Amazon EFS, Anda dapat memulihkan item tersebut ke sistem file baru atau yang sudah ada. Jika Anda mengembalikan item ke sistem file yang ada, AWS Backup buat direktori Amazon EFS baru dari direktori root untuk memuat item. Hirarki penuh dari item yang ditentukan dipertahankan dalam direktori pemulihan. Misalnya, jika direktori A berisi subdirektori B, C, dan D, AWS Backup mempertahankan struktur hierarkis ketika A, B, C, dan D dipulihkan. Terlepas dari apakah Anda melakukan pemulihan sebagian Amazon EFS ke sistem file yang ada atau ke sistem file baru, setiap upaya pemulihan membuat direktori pemulihan baru dari direktori root untuk berisi file yang dipulihkan. Jika Anda mencoba beberapa pemulihan untuk jalur yang sama, beberapa direktori yang berisi item yang dipulihkan mungkin ada.

Untuk memulihkan instans Amazon EFS

Jika Anda memulihkan instans Amazon EFS, Anda dapat melakukan Pemulihan penuh, yang memulihkan seluruh sistem file. Atau, Anda dapat memulihkan file dan direktori tertentu menggunakan pemulihan tingkat Item (pemulihan tingkat item memiliki batas. Lihat Memulihkan sistem file EFS untuk informasi selengkapnya). Untuk informasi tentang memulihkan jenis sumber daya lainnya, lihat Memulihkan cadangan.

> **Note**
>
> Untuk memulihkan instans Amazon EFS, Anda harus “Izinkan”`backup:startrestorejob`.

Untuk informasi rinci tentang memulihkan cadangan, lihatMemulihkan cadangan.

Langkah selanjutnya

Dengan AWS Backup Audit Manager, Anda dapat mengaudit aktivitas dan sumber daya pencadangan Anda. Anda juga dapat membuat laporan yang dapat Anda gunakan sebagai bukti

pencadangan, pemulihan, dan penyalinan pekerjaan Anda. Untuk membuat laporan, lihatMemulai 7: Buat laporan audit.

Memulai 7: Buat laporan audit

DiMemulai 5: Lihat pekerjaan cadangan dan titik pemulihan, Anda mengamati aktivitas pencadangan di tampilan AWS Backup Dasbor, Brankas Cadangan, dan Sumber Daya yang Dilindungi. Namun, tampilan ini dinamis dan akan diperbarui tergantung pada saat Anda mengunjunginya. Pandangan ini belum tentu merupakan bukti terbaik dari kepatuhan berkelanjutan terhadap persyaratan dan kontrol perlindungan data organisasi Anda sepanjang waktu.

Pada langkah ini, Anda akan membuat laporan pekerjaan cadangan sesuai permintaan menggunakan AWS Backup Audit Manager.

AWS Backup Audit Manager memberikan berbagai laporan audit dalam format CSV, JSON, atau keduanya setiap hari dan sesuai permintaan ke bucket Amazon S3 Anda. Anda dapat mengaudit kepatuhan aktivitas pencadangan dan sumber daya Anda terhadap sejumlah kontrol yang dapat disesuaikan. Anda dapat menerima laporan tentang pencadangan, menyalin, dan memulihkan pekerjaan Anda. Laporan pekerjaan cadangan adalah bukti bahwa pekerjaan cadangan Anda terjadi.

Berikut ini adalah contoh rencana cadangan.


```
{
  "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"
    }
  ]
}
```

Untuk membuat laporan cadangan (termasuk laporan cadangan sesuai permintaan), pertama-tama Anda membuat rencana laporan untuk mengotomatiskan laporan dan mengirimkannya ke bucket Amazon S3.

Paket laporan mengharuskan Anda memiliki bucket Amazon S3 untuk menerima laporan Anda. Untuk petunjuk cara menyiapkan bucket S3 baru, lihat Langkah 1: Membuat bucket S3 pertama Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk membuat rencana laporan

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Laporan.
3. Pilih Buat rencana laporan.
4. Pilih Backup job report dari daftar dropdown.
5. Untuk nama paket Laporan, masukkan**`TestBackupJobReport`**.
6. Untuk format File, pilih CSV dan JSON.
7. Untuk nama bucket S3, pilih tujuan laporan Anda dari daftar tarik-turun.
8. Pilih Buat rencana laporan.

Selanjutnya, Anda harus mengizinkan bucket S3 Anda untuk menerima laporan dari AWS Backup. AWS Backup Audit Manager secara otomatis membuat kebijakan akses S3 untuk Anda.

Untuk melihat dan menerapkan kebijakan akses ini

1. Di panel navigasi kiri, pilih Laporan.
2. Di bawah nama paket Laporan, pilih nama rencana laporan Anda (`TestBackupJobReport`).
3. Pilih Edit.
4. Pilih Lihat kebijakan akses untuk bucket S3.

5. Pilih Salin izin.
6. Pilih Edit kebijakan bucket untuk mengedit kebijakan bucket S3 tujuan agar dapat menerima laporan pekerjaan cadangan.
7. Salin atau tambahkan izin ke kebijakan bucket S3 tujuan.

Selanjutnya, buat laporan pekerjaan cadangan pertama Anda.

Untuk membuat laporan cadangan sesuai permintaan

1. Di panel navigasi kiri, pilih Laporan.
2. Di bawah nama paket Laporan, pilih nama rencana laporan Anda (`TestBackupJobReport`).
3. Pilih Buat laporan sesuai permintaan.

Terakhir, lihat laporan Anda.

Untuk melihat laporan Anda

1. Di panel navigasi kiri, pilih Laporan.
2. Di bawah nama paket Laporan, pilih nama rencana laporan Anda (`TestBackupJobReport`).
3. Di bagian Laporkan pekerjaan, pilih tautan S3. Melakukan hal itu membawa Anda ke ember S3 tujuan Anda.
4. Pilih Unduh.
5. Buka laporan menggunakan program yang Anda gunakan untuk bekerja dengan file CSV atau JSON.

Langkah selanjutnya

Untuk membersihkan sumber daya awal Anda dan menghindari biaya yang tidak diinginkan, lanjutkan keMemulai 8: Bersihkan sumber daya.

Memulai 8: Bersihkan sumber daya

Setelah Anda melakukan semua tugasMemulai dengan AWS Backup, Anda mungkin ingin membersihkan apa yang telah Anda buat untuk menghindari biaya yang tidak perlu.

Topik

Langkah 1: Hapus AWS sumber daya yang dipulihkan

Untuk menghapus AWS sumber daya yang dipulihkan dari titik pemulihan, seperti volume Amazon Elastic Block Store (Amazon EBS) atau tabel Amazon DynamoDB, Anda menggunakan konsol untuk layanan tersebut. Misalnya, untuk menghapus sistem file Amazon Elastic File System (Amazon EFS), gunakan konsol Amazon EFS.

> **Note**
>
> Informasi ini mengacu pada sumber daya yang dipulihkan, bukan ke titik pemulihan yang disimpan dalam brankas cadangan.

Langkah 2: Hapus paket cadangan

Jika Anda tidak ingin membuat cadangan terjadwal, Anda harus menghapus rencana cadangan Anda. Sebelum Anda dapat menghapus rencana cadangan, Anda harus menghapus semua penetapan sumber daya ke rencana cadangan itu.

Ikuti langkah-langkah berikut untuk menghapus paket cadangan:

Untuk menghapus rencana cadangan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Rencana cadangan.
3. Pada halaman Backup plan, pilih paket cadangan yang ingin Anda hapus. Ini membawa Anda ke halaman detail untuk cadangan itu.
4. Untuk menghapus penetapan sumber daya untuk paket Anda, pilih tombol radio di sebelah nama penetapan, lalu pilih Hapus.

5. Untuk menghapus paket cadangan, pilih Hapus di sudut kanan atas halaman.
6. Pada halaman konfirmasi, masukkan nama paket, dan pilih Hapus paket.

Langkah 3: Hapus titik pemulihan

Selanjutnya, Anda dapat menghapus titik pemulihan cadangan yang ada di brankas cadangan Anda.

Untuk menghapus poin pemulihan

1. Di AWS Backup konsol, di panel navigasi, pilih Backup vaults.
2. Pada halaman Backup vaults, pilih brankas cadangan tempat Anda menyimpan cadangan.
3. Periksa titik pemulihan dan pilih Hapus.
4. Jika Anda menghapus lebih dari satu titik pemulihan, ikuti langkah-langkah berikut:

    a. Jika daftar Anda berisi cadangan berkelanjutan, pilih apakah akan menyimpan atau menghapus data cadangan berkelanjutan Anda.

    b. Untuk menghapus semua titik pemulihan yang terdaftar, ketik**`delete`**, lalu pilih Hapus titik pemulihan.

    Biarkan tab browser Anda tetap terbuka sampai Anda melihat spanduk sukses hijau di bagian atas halaman. Menutup tab ini sebelum waktunya akan mengakhiri proses penghapusan dan mungkin meninggalkan beberapa titik pemulihan yang ingin Anda hapus. Untuk informasi selengkapnya, lihat Menghapus cadangan.

Langkah 4: Hapus brankas cadangan

Brankas cadangan default biasanya tidak dapat dihapus. Namun, jika satu atau beberapa brankas lain ada di Wilayah, brankas cadangan default di Wilayah tersebut dapat dihapus menggunakan. AWS CLI

Anda dapat menghapus brankas non-default lainnya setelah semua cadangan (titik pemulihan) di dalamnya telah dihapus. Untuk melakukan ini, pilih Hapus di brankas kosong.

Langkah 5: Hapus rencana laporan

Rencana laporan Anda secara otomatis mengirimkan laporan baru setiap hari. Untuk mencegah hal ini, hapus rencana laporan.

Untuk menghapus rencana laporan

1. Di AWS Backup konsol, di panel navigasi, pilih Laporan.
2. Di bawah nama paket Laporan, pilih nama rencana laporan Anda.
3. Pilih Hapus.
4. Masukkan nama rencana laporan Anda, dan pilih Hapus rencana laporan.

Langkah 6: Hapus laporan

Anda dapat menghapus laporan dengan mengikuti petunjuk untuk Menghapus satu objek untuk setiap laporan Anda. Jika Anda tidak lagi membutuhkan bucket S3 tujuan Anda, setelah menghapus semua objek dari bucket, Anda dapat menghapus bucket dengan mengikuti petunjuk untuk Menghapus ember.

Mengelola cadangan menggunakan rencana cadangan

Di AWS Backup, rencana cadangan adalah ekspresi kebijakan yang menentukan kapan dan bagaimana Anda ingin mencadangkan AWS sumber daya Anda, seperti tabel Amazon DynamoDB atau sistem file Amazon Elastic File System (Amazon EFS). Anda dapat menetapkan sumber daya ke rencana cadangan, dan AWS Backup secara otomatis mencadangkan dan mempertahankan cadangan untuk sumber daya tersebut sesuai dengan rencana cadangan. Anda dapat membuat beberapa paket cadangan jika Anda memiliki beban kerja dengan persyaratan pencadangan yang berbeda. Secara default, jendela cadangan dioptimalkan oleh AWS Backup. Anda dapat menyesuaikan jendela cadangan di konsol atau secara terprogram.

AWS Backup secara efisien menyimpan cadangan berkala Anda secara bertahap. Cadangan pertama AWS sumber daya mencadangkan salinan lengkap data Anda. Untuk setiap pencadangan inkremental berturut-turut, hanya perubahan pada AWS sumber daya Anda yang dicadangkan. Pencadangan tambahan memungkinkan Anda mendapatkan keuntungan dari perlindungan data dari pencadangan yang sering sekaligus meminimalkan biaya penyimpanan.

AWS Backup juga mengelola siklus hidup paket cadangan Anda dengan mulus berdasarkan pengaturan retensi Anda, yang memungkinkan Anda memulihkan saat diperlukan.

Bagian berikut memberikan dasar-dasar mengelola strategi cadangan Anda di AWS Backup.

Topik

Membuat rencana cadangan

Anda dapat membuat paket cadangan menggunakan AWS Backup konsol, API, CLI, SDK, atau templat. AWS CloudFormation

Topik

- Membuat rencana cadangan menggunakan AWS CLI
- Opsi dan konfigurasi paket Backup
- AWS CloudFormation template untuk rencana cadangan

Membuat paket cadangan menggunakan AWS Backup konsol

Buka AWS Backup konsol di https://console.aws.amazon.com/backup. Dari dasbor, pilih Kelola paket Cadangan. Atau, menggunakan panel navigasi, pilih Paket Backup dan pilih Buat paket Backup.

Opsi mulai

Anda memiliki tiga pilihan untuk paket cadangan baru Anda:

- Langkah 1: Buat rencana cadangan berdasarkan yang sudah ada
- Bangun rencana baru
- Membuat rencana cadangan menggunakan AWS CLI

Dalam tutorial ini, kita akan memilih Build a new plan. Setiap bagian dari konfigurasi memiliki tautan ke bagian yang diperluas lebih jauh di halaman tempat Anda dapat menavigasi untuk detail lebih lanjut.

1. Masukkan nama paket di Nama paket Backup. Anda tidak dapat mengubah nama rencana setelah dibuat.

   Jika Anda mencoba membuat rencana cadangan yang identik dengan paket yang ada, Anda menerima `AlreadyExistsException` kesalahan.
2. Secara opsional, Anda dapat menambahkan tag ke paket cadangan Anda.
3. Konfigurasi aturan cadangan: Di bagian konfigurasi aturan cadangan, Anda akan mengatur jadwal cadangan, jendela, dan siklus hidup.
4. Jadwal:

   a. Masukkan nama aturan cadangan di bidang teks.

   b. Di menu tarik-turun backup vault, pilih Default atau pilih Create new Backup vault untuk membuat brankas baru.

   c. Di menu tarik-turun frekuensi cadangan, pilih seberapa sering Anda ingin paket ini membuat cadangan.

5. Jendela Backup:

    a. Waktu mulai default ke 12:30 (00:30 dalam waktu 24 jam) di zona waktu lokal sistem Anda.

    b. Mulai dalam default hingga 8 jam. Anda dapat mengubah ini untuk menentukan jendela waktu untuk memulai pencadangan.

    c. Selesaikan dalam default hingga 7 hari.

6. Pencadangan dan point-in-time pemulihan berkelanjutan (PITR): Anda dapat memilih Aktifkan cadangan berkelanjutan untuk point-in-time pemulihan (PITR). Untuk memverifikasi sumber daya mana yang didukung untuk jenis cadangan ini, lihat Ketersediaan fitur berdasarkan sumber daya matriks.

7. Siklus hidup

    a. Penyimpanan dingin: Pilih kotak ini untuk memungkinkan jenis sumber daya yang memenuhi syarat bertransisi ke penyimpanan dingin sesuai dengan jadwal yang Anda tentukan dalam periode retensi total. Untuk menggunakan cold storage, Anda harus memiliki periode retensi total 90 hari atau lebih.

    b. Penyimpanan dingin untuk Amazon EBS adalah Amazon EBS Snapshots Archive. Snapshot yang dialihkan ke tingkat penyimpanan arsip akan ditampilkan di konsol sebagai tingkat dingin. Jika penyimpanan dingin diaktifkan, dan jika frekuensi cadangan Anda bulanan atau lebih jarang, Anda dapat memiliki snapshot EBS transisi rencana cadangan Anda.

    c. Periode retensi total adalah jumlah hari Anda menyimpan sumber daya Anda AWS Backup. Ini adalah jumlah total hari penyimpanan hangat ditambah penyimpanan dingin.

8. (Opsional) Gunakan Salin ke tujuan untuk membuat salinan lintas wilayah dari sumber daya yang memenuhi syarat jika Anda ingin menyimpan salinan cadangan di tempat lain Wilayah AWS.

9. (Opsional) Tag ditambahkan ke titik pemulihan.

10. Ketika semua bagian disetel ke spesifikasi Anda, pilih aturan Simpan Cadangan.

Membuat rencana cadangan menggunakan AWS CLI

Anda juga dapat menentukan paket cadangan Anda dalam dokumen JSON dan menyediakannya menggunakan AWS Backup konsol atau AWS CLI. Dokumen JSON berikut berisi contoh rencana cadangan yang membuat cadangan harian pada pukul 1:00 waktu Pasifik (waktu setempat menyesuaikan dengan kondisi siang hari, standar, atau musim panas jika berlaku). Secara otomatis menghapus cadangan setelah satu tahun.

```
{
  "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
        }
      }
    ]
  }
}
```

Anda dapat menyimpan dokumen JSON Anda dengan nama yang Anda pilih. Perintah CLI berikut menunjukkan `create-backup-plan`dengan JSON bernama: `test-backup-plan.json`

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

Perhatikan bahwa sementara beberapa sistem memberi nomor hari dalam seminggu dari 0 hingga 6, kami memberi nomor dari 1 hingga 7. Untuk informasi selengkapnya, lihat Ekspresi cron. Untuk informasi selengkapnya tentang zona waktu, lihat TimeZonedi referensi Amazon Location Service API.

Opsi dan konfigurasi paket Backup

Saat Anda menentukan paket cadangan di AWS Backup konsol, Anda mengonfigurasi opsi berikut:

Nama paket Backup

Anda harus memberikan nama paket cadangan yang unik.

Jika Anda memilih nama yang identik dengan nama paket yang ada, Anda akan menerima pesan kesalahan.

Aturan Backup

Paket Backup terdiri dari satu atau lebih aturan cadangan. Untuk menambahkan aturan cadangan ke rencana cadangan, atau mengedit aturan yang ada dalam rencana cadangan:

1. Dari AWS Backup konsol, di panel navigasi kiri, pilih Backup plan.
2. Di bawah nama paket Backup, pilih paket cadangan.
3. Di bawah bagian Aturan Backup:
   - Untuk menambahkan aturan cadangan, pilih Tambahkan aturan cadangan.
   - Untuk mengedit aturan cadangan yang ada, pilih aturan, lalu pilih Edit.

> **Note**
>
> Jika Anda memiliki rencana cadangan dengan beberapa aturan dan kerangka waktu dari dua aturan tumpang tindih, AWS Backup optimalkan cadangan dan ambil cadangan untuk aturan dengan waktu retensi yang lebih lama. Optimalisasi memperhitungkan jendela mulai penuh, tidak hanya ketika cadangan harian diambil.

Setiap aturan cadangan terdiri dari elemen-elemen berikut.

Nama aturan Backup

Nama aturan Backup peka huruf besar/kecil. Mereka harus berisi dari 1 hingga 50 karakter alfanumerik atau tanda hubung.

Frekuensi Backup

Frekuensi cadangan menentukan seberapa sering AWS Backup membuat cadangan snapshot. Menggunakan konsol, Anda dapat memilih frekuensi setiap jam, 12 jam, harian, mingguan, atau bulanan. Anda juga dapat membuat ekspresi cron yang membuat cadangan snapshot sesering per jam. Menggunakan AWS Backup CLI, Anda dapat menjadwalkan cadangan snapshot sesering per jam.

Jika Anda memilih mingguan, Anda dapat menentukan hari mana dalam seminggu Anda ingin backup diambil. Jika Anda memilih bulanan, Anda dapat memilih hari tertentu dalam sebulan.

Anda juga dapat memeriksa kotak centang Aktifkan pencadangan berkelanjutan untuk sumber daya yang didukung untuk membuat aturan pencadangan berkelanjutan yang diaktifkan point-in-time pemulihan (PITR). Tidak seperti cadangan snapshot, pencadangan berkelanjutan memungkinkan Anda melakukan pemulihan. point-in-time Untuk mempelajari lebih lanjut tentang pencadangan berkelanjutan, lihat Pemulihan Point-in-Time.

Periode pencadangan

Jendela cadangan terdiri dari waktu di mana jendela cadangan dimulai dan durasi jendela dalam jam. Pekerjaan Backup dimulai dalam jendela ini. Pengaturan default di konsol adalah:

- 12:30 lokal ke zona waktu sistem Anda (0:30 dalam sistem 24 jam)
- Mulai dalam 8 jam
- Selesai dalam 7 hari

  (lengkap dalam parameter tidak berlaku untuk sumber daya Amazon FSx)

Anda dapat menyesuaikan frekuensi cadangan dan waktu mulai jendela cadangan menggunakan ekspresi cron. Untuk melihat enam bidang ekspresi AWS cron, lihat Ekspresi Cron di Panduan Pengguna CloudWatch Acara Amazon. Dua contoh ekspresi AWS cron adalah `15 * ? * * *` (ambil cadangan setiap jam pada 15 menit melewati satu jam) dan `0 12 * * ? *` (ambil cadangan setiap hari pada 12 siang UTC). Untuk tabel contoh, klik tautan sebelumnya dan gulir ke bawah halaman.

AWS Backup mengevaluasi ekspresi cron antara 00:00 dan 23:59. Jika Anda membuat aturan cadangan untuk “setiap 12 jam” tetapi memberikan waktu mulai lebih dari 11:59, itu hanya akan berjalan sekali per hari.

Pencadangan dan point-in-time pemulihan berkelanjutan (PITR) merujuk perubahan yang direkam selama periode waktu tertentu; oleh karena itu, mereka tidak dapat dijadwalkan dengan ekspresi waktu atau cron.

> **Note**
>
> Secara umum, layanan AWS database tidak dapat memulai pencadangan 1 jam sebelum atau selama jendela pemeliharaannya dan Amazon FSx tidak dapat memulai pencadangan 4 jam sebelum atau selama jendela pemeliharaan atau jendela pencadangan otomatis (Amazon Aurora dibebaskan dari pembatasan jendela pemeliharaan ini). Pencadangan snapshot yang dijadwalkan selama waktu itu akan gagal.

Pengecualian terjadi ketika Anda memilih AWS Backup untuk menggunakan snapshot dan backup berkelanjutan untuk layanan yang didukung. AWS Backup akan menjadwalkan jendela cadangan secara otomatis untuk menghindari konflik. Lihat Point-in-Time Recovery untuk daftar layanan yang didukung dan petunjuk tentang cara menggunakan AWS Backup untuk melakukan backup berkelanjutan.

Aturan cadangan yang tumpang tindih

Kadang-kadang, rencana cadangan mungkin berisi beberapa aturan yang tumpang tindih. Ketika jendela awal dari aturan yang berbeda tumpang tindih, AWS Backup pertahankan cadangan di bawah aturan dengan periode retensi yang lebih lama. Misalnya, pertimbangkan rencana cadangan dengan dua aturan:

1. Backup per jam, dengan jendela mulai 1 jam, dan simpan selama 1 hari.
2. Backup setiap 12 jam, dengan jendela mulai 8 jam, dan simpan selama 1 minggu.

Setelah 24 jam, aturan kedua membuat dua cadangan (karena memiliki periode retensi yang lebih lama). Aturan pertama membuat delapan cadangan (karena jendela mulai 8 jam aturan kedua mencegah lebih banyak cadangan per jam berjalan). Secara khusus:

Selama Jendela Mulai ini	Aturan Ini Membuat 1 Backup
Tengah malam sampai jam 8 pagi	12 jam
8 hingga 9	Per Jam
9 hingga 10	Per Jam
10 hingga 11	Per Jam
11 hingga Siang Hari	Per Jam
Siang sampai jam 8 malam	12 jam
8 hingga 9	Per Jam
9 hingga 10	Per Jam

Selama Jendela Mulai ini	Aturan Ini Membuat 1 Backup
10 hingga 11	Per Jam
11 hingga Tengah Malam	Per Jam

Selama jendela mulai, status pekerjaan cadangan tetap dalam `CREATED` status sampai berhasil dimulai atau sampai waktu jendela mulai habis. Jika dalam waktu jendela mulai AWS Backup menerima kesalahan yang memungkinkan pekerjaan untuk dicoba lagi, secara otomatis AWS Backup akan mencoba lagi untuk memulai pekerjaan setidaknya setiap 10 menit sampai pencadangan berhasil dimulai (status pekerjaan berubah menjadi`RUNNING`) atau sampai status pekerjaan berubah menjadi `EXPIRED` (yang diharapkan terjadi ketika waktu jendela mulai selesai).

Siklus hidup dan tingkatan penyimpanan

Cadangan disimpan untuk jumlah hari yang Anda tentukan, yang dikenal sebagai siklus hidup cadangan. Cadangan dapat dipulihkan hingga akhir siklus hidupnya.

Ini ditetapkan sebagai periode retensi total di bagian siklus hidup konfigurasi aturan cadangan di AWS Backup konsol.

Jika Anda menggunakan AWS CLI, ini diatur menggunakan parameter `DeleteAfterDays`. Periode retensi untuk snapshot dapat berkisar antara 1 hari dan 100 tahun (atau tanpa batas waktu jika Anda tidak memasukkannya), sedangkan periode retensi untuk pencadangan berkelanjutan dapat berkisar dari 1 hari hingga 35 hari. Tanggal pembuatan cadangan adalah tanggal pekerjaan pencadangan dimulai, bukan tanggal penyelesaiannya. Jika pekerjaan cadangan Anda tidak selesai pada tanggal yang sama saat dimulai, gunakan tanggal di mana ia mulai membantu menghitung periode retensi.

Cadangan dipertahankan dalam tingkat penyimpanan. Setiap tingkat menimbulkan biaya yang berbeda untuk penyimpanan dan pemulihan, seperti yang diuraikan oleh harga.AWS Backup Setiap cadangan dibuat dan disimpan dalam penyimpanan hangat. Tergantung pada berapa lama Anda memilih untuk menyimpan cadangan Anda, Anda mungkin ingin mentransisikan cadangan Anda ke tingkat biaya lebih rendah yang disebut penyimpanan dingin. Ketersediaan fitur berdasarkan sumber dayamenampilkan sumber daya mana yang memiliki fitur opsional ini.

Console

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.

2. Buat atau edit rencana cadangan.
3. Di bagian siklus hidup konfigurasi aturan cadangan, centang kotak Pindahkan cadangan dari penyimpanan hangat ke penyimpanan dingin.
4. (opsional) Jika Amazon EBS adalah salah satu sumber daya yang Anda cadangkan dan frekuensi pencadangan Anda bulanan atau kurang sering, Anda dapat mentransisikannya ke tingkat dingin menggunakan arsip snapshot EBS.
5. Masukkan nilai (dalam beberapa hari) yang Anda inginkan cadangan Anda tetap dalam penyimpanan hangat. AWS Backup merekomendasikan setidaknya 8 hari.
6. Masukkan nilai (dalam hari) untuk periode retensi total. Perbedaan antara periode retensi total dan waktu dalam penyimpanan hangat adalah jumlah hari cadangan tetap dalam penyimpanan dingin.

AWS CLI

1. Gunakan `create-backup-plan`atau `update-backup-plan`.
2.
3. Sertakan parameter Boolean `OptInToArchiveForSupportedResources`untuk sumber daya EBS.
4. Sertakan parameternya `MoveToColdStorageAfterdays`.
5. Gunakan parameter `DeleteAfterDays`. Nilai ini harus 90 (hari) ditambah nilai yang Anda masukkan`MoveToColdStorageAfterDays`.

Penyimpanan dingin saat ini tersedia untuk jenis sumber daya berikut:

Jenis sumber daya	Cadangan tambahan atau penuh dalam penyimpanan dingin
AWS CloudFormation	Inkremental
DynamoDB dengan fitur-fitur canggih	Penuh; tidak ada cadangan tambahan di tingkat mana pun
Amazon EBS (menggunakan Arsip Snapshot EBS)	Penuh; Cadangan tambahan akan menjadi Penuh setelah transisi.

Jenis sumber daya	Cadangan tambahan atau penuh dalam penyimpanan dingin
Amazon EFS	Inkremental
Database SAP HANA berjalan pada instans Amazon EC2	Inkremental
Amazon Timestream	Inkremental
Mesin virtual VMware	Inkremental

Setelah Anda mengaktifkan transisi ke penyimpanan dingin melalui konsol atau baris perintah, kondisi berikut berlaku untuk cadangan di penyimpanan dingin (atau arsip):

- Cadangan yang dialihkan harus disimpan dalam penyimpanan dingin selama minimal 90 hari, selain waktu dalam penyimpanan hangat. AWS Backup mengharuskan retensi diatur selama 90 hari lebih lama dari pengaturan “transisi ke dingin setelah hari”. Anda tidak dapat mengubah pengaturan “transisi ke dingin setelah berhari-hari” setelah cadangan dialihkan ke dingin.
- Beberapa layanan mendukung pencadangan tambahan. Untuk pencadangan tambahan, Anda harus memiliki setidaknya satu cadangan penuh hangat. AWS Backup merekomendasikan agar Anda mengatur pengaturan siklus hidup Anda untuk tidak memindahkan cadangan Anda ke penyimpanan dingin sampai setelah setidaknya 8 hari. Jika cadangan penuh dialihkan ke penyimpanan dingin terlalu cepat (misalnya, transisi ke penyimpanan dingin setelah 1 hari), AWS Backup akan membuat cadangan penuh hangat lainnya.
- Untuk tipe sumber daya yang mendukung pencadangan tambahan, AWS Backup transisi data dari penyimpanan hangat ke penyimpanan dingin jika data yang ditransisi tidak lagi direferensikan oleh backup hangat. Data dalam cadangan yang disimpan dalam cold storage yang hanya direferensikan oleh cold backup lainnya ditagih dengan harga tingkat cold storage. Pencadangan lainnya berlanjut dengan harga tingkat penyimpanan hangat.

Brankas cadangan

Brankas cadangan adalah wadah untuk mengatur cadangan Anda. Cadangan yang dibuat oleh aturan cadangan diatur dalam brankas cadangan yang Anda tentukan dalam aturan pencadangan. Anda dapat menggunakan brankas cadangan untuk menyetel kunci enkripsi AWS Key Management Service (AWS KMS) yang digunakan untuk mengenkripsi cadangan di brankas cadangan dan

untuk mengontrol akses ke cadangan di brankas cadangan. Anda juga dapat menambahkan tag ke brankas cadangan untuk membantu Anda mengaturnya. Jika Anda tidak ingin menggunakan brankas default, Anda dapat membuatnya sendiri. Untuk step-by-step petunjuk membuat brankas cadangan, lihatLangkah 3: Buat brankas cadangan.

Salin ke Wilayah

Sebagai bagian dari rencana cadangan Anda, Anda dapat secara opsional membuat salinan cadangan di yang lain Wilayah AWS. Untuk informasi selengkapnya tentang salinan cadangan, lihat Membuat salinan cadangan di seluruh Wilayah AWS.

Saat Anda menentukan salinan cadangan, Anda mengonfigurasi opsi berikut:

Wilayah Tujuan

Wilayah tujuan untuk salinan cadangan.

(Pengaturan Lanjutan) Brankas cadangan

Brankas cadangan tujuan untuk salinan.

(Pengaturan Lanjutan) Peran IAM

Peran IAM yang AWS Backup digunakan saat membuat salinan. Peran tersebut juga harus AWS Backup terdaftar sebagai entitas tepercaya, yang memungkinkan AWS Backup untuk mengambil peran. Jika Anda memilih Default dan peran AWS Backup default tidak ada di akun Anda, peran akan dibuat untuk Anda dengan izin yang benar.

(Pengaturan Lanjutan) Siklus Hidup

Menentukan kapan harus transisi salinan cadangan ke cold storage dan kapan harus kedaluwarsa (menghapus) salinan. Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Anda tidak dapat mengubah nilai ini setelah salinan dialihkan ke penyimpanan dingin.

Kedaluwarsa menentukan jumlah hari setelah pembuatan bahwa salinan dihapus. Ini harus lebih besar dari 90 hari di luar nilai Transisi ke penyimpanan dingin.

Tag ditambahkan ke titik pemulihan

Tag yang Anda cantumkan di sini secara otomatis ditambahkan ke cadangan saat dibuat.

Tag ditambahkan ke rencana cadangan

Tag ini dikaitkan dengan rencana cadangan itu sendiri untuk membantu Anda mengatur dan melacak rencana cadangan Anda.

Pengaturan cadangan lanjutan

Mengaktifkan pencadangan konsisten aplikasi untuk aplikasi pihak ketiga yang berjalan di instans Amazon EC2. Saat ini, AWS Backup mendukung cadangan Windows VSS. AWS Backup mengecualikan jenis instans Amazon EC2 tertentu dari cadangan Windows VSS. Untuk informasi selengkapnya, lihat Membuat cadangan Windows VSS.

AWS CloudFormation template untuk rencana cadangan

Kami menyediakan dua contoh AWS CloudFormation template untuk referensi Anda. Template pertama membuat rencana cadangan sederhana. Template kedua memungkinkan cadangan VSS dalam rencana cadangan.

> **Note**
>
> Jika Anda menggunakan peran layanan default, ganti *peran layanan* dengan. `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
```

Menetapkan sumber daya ke rencana cadangan

Penugasan sumber daya menentukan sumber daya mana yang AWS Backup akan dilindungi menggunakan rencana cadangan Anda. AWS Backup memberi Anda pengaturan default sederhana dan kontrol halus untuk menetapkan sumber daya ke paket cadangan Anda. Setiap kali paket cadangan Anda berjalan, ia memindai semua sumber daya yang sesuai dengan kriteria penetapan sumber daya Anda. Akun AWS Tingkat otomatisasi ini memungkinkan Anda untuk menentukan rencana cadangan dan penugasan sumber daya tepat sekali. AWS Backup mengabstraksikan pekerjaan menemukan dan mencadangkan sumber daya baru yang sesuai dengan tugas sumber daya yang Anda tentukan sebelumnya.

Anda dapat menetapkan semua jenis sumber daya yang AWS Backup didukung yang telah Anda pilih untuk AWS Backup dikelola. Untuk petunjuk tentang cara memilih jenis sumber daya yang AWS Backup didukung lainnya, lihat Memulai 1: Keikutsertaan Layanan.

AWS Backup Konsol memiliki dua cara untuk menyertakan jenis sumber daya dalam rencana cadangan: secara eksplisit menetapkan jenis sumber daya dalam rencana cadangan atau menyertakan semua sumber daya. Lihat poin di bawah ini untuk memahami cara kerja pilihan ini dengan layanan opt in.

- Jika penetapan sumber daya hanya didasarkan pada tag, maka pengaturan keikutsertaan layanan diterapkan.
- Jika jenis sumber daya secara eksplisit ditetapkan ke rencana cadangan, itu akan disertakan dalam cadangan meskipun keikutsertaan tidak diaktifkan untuk layanan tertentu. Ini tidak berlaku untuk Aurora, Neptunus, dan Amazon DocumentDB. Agar layanan ini disertakan, keikutsertaan harus diaktifkan.
- Jika kedua jenis sumber daya dan tag ditentukan dalam penetapan sumber daya, jenis sumber daya yang ditentukan difilter terlebih dahulu, lalu tag lebih lanjut memfilter sumber daya tersebut.

  Pengaturan keikutsertaan layanan diabaikan untuk sebagian besar jenis sumber daya. Namun Aurora, Neptunus, dan Amazon DocumentDB memerlukan layanan opt-in.
- Saat akun menggunakan AWS Backup (membuat brankas cadangan atau paket cadangan) di Wilayah, akun secara otomatis dipilih ke semua jenis sumber daya yang didukung oleh AWS Backup di Wilayah pada saat itu. Layanan yang didukung yang ditambahkan ke Wilayah tersebut di kemudian hari tidak akan secara otomatis disertakan dalam paket cadangan. Anda dapat memilih untuk memilih jenis sumber daya tersebut setelah didukung.
- Untuk Amazon FSx untuk NetApp ONTAP, saat menggunakan pemilihan sumber daya berbasis tag, terapkan tag ke volume individual alih-alih seluruh sistem file.

Penetapan sumber daya Anda dapat menyertakan (atau mengecualikan) jenis sumber daya dan sumber daya.

- Jenis sumber daya mencakup setiap instance atau sumber daya dari AWS layanan yang AWS Backup didukung atau aplikasi pihak ketiga. Misalnya, jenis sumber daya DynamoDB mengacu pada semua tabel DynamoDB Anda.
- Sumber daya adalah contoh tunggal dari jenis sumber daya, seperti salah satu tabel DynamoDB Anda. Anda dapat menentukan sumber daya menggunakan ID sumber daya uniknya.

Anda dapat lebih menyempurnakan penetapan sumber daya Anda menggunakan tag dan operator bersyarat.

Topik

- Menetapkan sumber daya menggunakan konsol
- Menetapkan sumber daya secara terprogram
- Menetapkan sumber daya menggunakan AWS CloudFormation

- Kuota pada penugasan sumber daya

Menetapkan sumber daya menggunakan konsol

Untuk menavigasi ke halaman Tetapkan sumber daya:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pilih Paket Backup.
3. Pilih Buat paket Cadangan.
4. Pilih template apa pun di daftar tarik-turun Pilih template, lalu pilih Buat rencana.
5. Ketik nama paket Backup.
6. Pilih Buat paket.
7. Pilih Tetapkan sumber daya.

Untuk memulai tugas sumber daya Anda, di bagian Umum:

1. Ketik nama tugas Sumber Daya.
2. Pilih peran Default atau Pilih peran IAM.

> **Note**
>
> Jika Anda memilih peran IAM, verifikasi bahwa ia memiliki izin untuk mencadangkan semua sumber daya yang akan Anda tetapkan. Jika peran Anda menemukan sumber daya yang tidak memiliki izin untuk dicadangkan, paket cadangan Anda akan gagal.

Untuk menetapkan sumber daya Anda, di bagian Tetapkan sumber daya, pilih salah satu dari dua opsi di bawah Tentukan pemilihan sumber daya:

- Sertakan semua jenis sumber daya. Opsi ini mengonfigurasi paket cadangan Anda untuk melindungi semua sumber daya yang AWS Backup didukung saat ini dan masa depan yang ditetapkan ke paket cadangan Anda. Gunakan opsi ini untuk melindungi data estate Anda dengan cepat dan mudah.

  Ketika Anda memilih opsi ini, Anda dapat secara opsional Memperbaiki pilihan menggunakan tag sebagai langkah berikutnya.

- Sertakan jenis sumber daya tertentu. Ketika Anda memilih opsi ini, Anda harus Pilih jenis sumber daya tertentu dengan langkah-langkah berikut:

  1. Menggunakan menu tarik-turun Pilih jenis sumber daya, tetapkan satu atau beberapa jenis sumber daya.

     > **Important**
     >
     > RDS, Aurora, Neptune, dan DocumentDB berbagi Amazon Resource Name (ARN) yang sama. Memilih untuk mengelola salah satu jenis sumber daya ini dengan AWS Backup memilih semuanya saat menetapkannya ke paket cadangan. Untuk menyempurnakan pilihan Anda, gunakan tag dan operator bersyarat.

     Setelah selesai, AWS Backup menyajikan daftar jenis sumber daya yang Anda pilih dan pengaturan defaultnya, yaitu untuk melindungi semua sumber daya untuk setiap jenis sumber daya yang dipilih.

  2. Secara opsional, jika Anda ingin mengecualikan sumber daya tertentu dari jenis sumber daya yang Anda pilih:

     1. Gunakan menu tarik-turun Pilih sumber daya dan batalkan pilihan opsi default.
     2. Pilih sumber daya spesifik yang akan ditetapkan ke paket cadangan Anda.

  3. Secara opsional, Anda dapat Mengecualikan ID sumber daya tertentu dari jenis sumber daya yang dipilih. Gunakan opsi ini jika Anda ingin mengecualikan satu atau beberapa sumber daya dari banyak sumber daya, karena melakukannya mungkin lebih cepat daripada memilih banyak sumber daya selama langkah sebelumnya. Anda harus menyertakan jenis sumber daya sebelum dapat mengecualikan sumber daya dari jenis sumber daya tersebut. Kecualikan ID sumber daya menggunakan langkah-langkah berikut:

     1. Di bawah Kecualikan ID sumber daya tertentu dari jenis sumber daya yang dipilih, pilih satu atau beberapa jenis sumber daya yang Anda sertakan menggunakan Pilih jenis sumber daya.
     2. Untuk setiap jenis sumber daya, gunakan menu Pilih sumber daya untuk memilih satu atau beberapa sumber daya yang akan dikecualikan.

Selain pilihan Anda sebelumnya, Anda dapat membuat pilihan yang lebih terperinci menggunakan pilihan Perbaiki opsional menggunakan fitur tag. Fitur ini memungkinkan Anda untuk

menyempurnakan pilihan Anda saat ini untuk menyertakan subset sumber daya Anda menggunakan tag.

Tag adalah pasangan nilai kunci yang dapat Anda tetapkan ke sumber daya tertentu untuk membantu Anda mengidentifikasi, mengatur, dan memfilter sumber daya Anda. Tag peka terhadap huruf besar dan kecil. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya di Referensi AWS Umum.

Ketika Anda memperbaiki pilihan Anda menggunakan dua atau lebih tag, efeknya adalah kondisi AND. Misalnya, jika Anda menyempurnakan pilihan menggunakan dua tag, `env: prod` dan`role: application`, Anda hanya menetapkan sumber daya dengan KEDUA tag ke paket cadangan Anda.

Untuk menyempurnakan pilihan Anda menggunakan tag:

1. Di bawah Perbaiki pilihan menggunakan tag, pilih Kunci dari daftar dropdown.
2. Pilih Kondisi untuk nilai dari daftar dropdown.
   - Nilai mengacu pada input berikutnya, nilai pasangan kunci-nilai Anda.
   - Kondisi dapat berupa`Equals`,`Contains`,`Begins with`, atau`Ends with`, atau kebalikannya:`Does not equal`,, `Does not contain`Does not begin with, atauDoes not end with`.
3. Pilih Nilai dari daftar dropdown.
4. Untuk menyempurnakan lebih lanjut menggunakan tag lain, pilih Tambah tag.

Menetapkan sumber daya secara terprogram

Anda dapat menentukan penetapan sumber daya dalam dokumen JSON. *Contoh penetapan sumber daya ini menetapkan semua instans Amazon EC2 ke paket cadangan 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/*"
    ]
  }
```

```
}
```

Dengan asumsi JSON ini disimpan sebagai`backup-selection.json`, Anda dapat menetapkan sumber daya ini ke rencana cadangan Anda menggunakan perintah CLI berikut:

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

Berikut ini adalah contoh tugas sumber daya, bersama dengan dokumen JSON yang sesuai. Untuk membuat tabel ini lebih mudah bagi Anda untuk membaca, contoh menghilangkan bidang`"BackupPlanId"`,`"SelectionName"`, dan`"IamRoleArn"`. Wildcard `*` mewakili nol atau lebih karakter non-spasi.

Example Contoh: Pilih semua sumber daya di akun saya

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

Example Contoh: Pilih semua sumber daya di akun saya, tetapi kecualikan volume EBS

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

Example Contoh: Pilih semua sumber daya yang ditandai dengan`"backup":"true"`, tetapi kecualikan volume EBS

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

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

Example Contoh: Pilih semua volume EBS dan instans RDS DB yang ditandai dengan keduanya dan "backup":"true""stage":"prod"

Aritmatika Boolean mirip dengan yang ada dalam kebijakan IAM, dengan yang "Resources" digabungkan menggunakan Boolean OR dan yang dikombinasikan dengan Boolean AND. `"Conditions"`

`"Resources"`Ekspresi `"arn:aws:rds:*:*:db:*"` hanya memilih instans RDS DB karena tidak ada sumber daya Aurora, Neptunus, atau DocumentDB yang sesuai.

```
{
  "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 Contoh: Pilih semua volume EBS dan instans RDS yang ditandai dengan tetapi tidak "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 Contoh: Pilih semua sumber daya yang ditandai dengan "key1" dan nilai yang dimulai dengan "include" tetapi tidak dengan "key2" dan nilai yang berisi kata "exclude"

Anda dapat menggunakan karakter wildcard di awal, akhir, dan tengah string. Perhatikan penggunaan karakter wildcard (*) di dalam `include*` dan `*exclude*` dalam contoh di atas. Anda juga dapat menggunakan karakter wildcard di tengah string seperti yang ditunjukkan pada contoh sebelumnya,`arn:aws:rds:*:*:db:*`.

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

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

Example Contoh: Pilih semua sumber daya yang ditandai dengan "backup":"true" kecuali sistem file FSx dan sumber daya RDS, Aurora, Neptunus, dan DocumentDB

Item dalam `NotResources` digabungkan menggunakan Boolean OR.

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

Example Contoh: Pilih semua sumber daya yang ditandai dengan tag "backup" dan nilai apa pun

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

Example Contoh: Pilih semua sistem file FSx, cluster Aurora, dan semua sumber daya yang ditandai dengan"my-aurora-cluster", kecuali untuk sumber daya yang ditandai dengan "backup":"true""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 Contoh: Pilih semua sumber daya yang ditandai dengan tag **"backup":"true"** kecuali untuk volume EBS yang ditandai dengan **"stage":"test"**

Gunakan dua perintah CLI untuk membuat dua pilihan untuk memilih kelompok sumber daya ini. Pilihan pertama berlaku untuk semua sumber daya kecuali untuk volume EBS. Pilihan kedua berlaku untuk volume 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"
        }
      ]
    }
  }
}
```

Menetapkan sumber daya menggunakan AWS CloudFormation

end-to-end AWS CloudFormation Template ini membuat penetapan sumber daya, rencana cadangan, dan brankas cadangan tujuan:

- Sebuah brankas cadangan bernama *`CloudFormationTestBackupVault`*.
- Rencana cadangan bernama *`CloudFormationTestBackupPlan`*. Rencana ini akan menjalankan dua berisi dua aturan cadangan, yang keduanya mengambil cadangan setiap hari pada 12 siang UTC dan menyimpannya selama 210 hari.
- Sebuah pilihan sumber daya bernama *`BackupSelectionName`*.
- • Penugasan sumber daya mencadangkan sumber daya berikut:
  - Sumber daya apa pun yang ditandai dengan pasangan kunci-nilai. `backupplan:dsi-sandbox-daily`
  - Setiap sumber daya yang ditandai dengan nilai `prod` atau nilai yang dimulai dengan`prod/`.
- Penugasan sumber daya tidak mencadangkan sumber daya berikut:
  - Kluster RDS, Aurora, Neptunus, atau DocumentDB apa pun.
  - Setiap sumber daya yang ditandai dengan nilai `test` atau nilai yang dimulai dengan`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/*
```

Kuota pada penugasan sumber daya

Kuota berikut berlaku untuk penugasan sumber daya tunggal:

- 500 Nama Sumber Daya Amazon (ARN) tanpa wildcard
- 30 ARN dengan ekspresi wildcard
- 30 kondisi
- 30 tag per penetapan sumber daya (dan jumlah sumber daya per tag yang tidak terbatas)

Menghapus paket cadangan

Anda dapat menghapus paket cadangan hanya setelah semua pilihan sumber daya yang terkait telah dihapus. Pilihan ini juga dikenal sebagai tugas sumber daya. Jika ini belum dihapus sebelum penghapusan paket cadangan, konsol akan menampilkan kesalahan: “Pilihan paket cadangan terkait harus dihapus sebelum penghapusan rencana cadangan.” Gunakan konsol atau gunakan `DeleteBackupSelection`.

Menghapus paket cadangan akan menghapus versi paket saat ini. Versi saat ini dan sebelumnya, jika ada, masih ada, tetapi tidak lagi terdaftar di konsol di bawah paket Backup.

> **Note**
>
> Ketika rencana cadangan dihapus, cadangan yang ada tidak dihapus. Untuk menghapus cadangan yang ada, hapus dari brankas cadangan menggunakan langkah-langkah dalam Menghapus cadangan.

Untuk menghapus paket cadangan menggunakan AWS Backup konsol

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi di sebelah kiri, pilih Backup plan.
3. Pilih paket cadangan Anda dalam daftar.
4. Pilih tugas sumber daya apa pun yang terkait dengan rencana cadangan.
5. Pilih Hapus.

Memperbarui rencana cadangan

Setelah membuat rencana cadangan, Anda dapat mengedit rencana—misalnya, Anda dapat menambahkan tag, atau menambahkan, mengedit, atau menghapus aturan pencadangan. Setiap perubahan yang Anda buat pada rencana cadangan tidak berpengaruh pada cadangan yang ada yang dibuat oleh paket cadangan. Perubahan hanya berlaku untuk backup yang dibuat di masa depan.

Misalnya, saat Anda memperbarui periode retensi dalam aturan pencadangan, periode penyimpanan cadangan yang dibuat sebelum Anda membuat pembaruan tetap sama. Pencadangan apa pun yang dibuat oleh aturan tersebut ke depan mencerminkan periode retensi yang diperbarui.

Anda tidak dapat mengubah nama rencana setelah dibuat.

Untuk mengedit paket cadangan menggunakan AWS Backup konsol

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Rencana cadangan.
3. Di bawah panel kedua, Backup plan, back plan yang ada akan ditampilkan. Pilih tautan yang digarisbawahi di kolom Nama rencana cadangan untuk melihat detail paket cadangan yang dipilih.

4. Anda dapat mengedit aturan cadangan, melihat penetapan sumber daya, melihat pekerjaan cadangan, mengelola tag, atau mengubah pengaturan Windows VSS.
5. Untuk memperbarui aturan cadangan, pilih nama aturan cadangan.

   Pilih Kelola tag untuk menambah atau menghapus tag.

   Pilih Edit di samping Pengaturan cadangan lanjutan untuk mengaktifkan atau menonaktifkan Windows VSS.
6. Ubah pengaturan yang Anda inginkan, lalu pilih Simpan.

Brankas cadangan

> **Note**
>
> Mulai 9 Agustus 2023, AWS Backup menawarkan pratinjau untuk menggunakan brankas yang memiliki celah udara secara logis. Untuk mendaftar di pratinjau ini, kirim permintaan melalui email ke <aws-backup-vault-preview@amazon .com>.
> Fitur dapat berubah atau disesuaikan selama dan setelah periode pratinjau. Ketika layanan menjadi Generally Available (GA), data dan konfigurasi yang disediakan selama pratinjau tidak akan lagi tersedia. AWS merekomendasikan penggunaan data uji alih-alih data produksi dengan pratinjau.

Di AWS Backup, brankas cadangan adalah wadah yang menyimpan dan mengatur cadangan Anda.

Saat membuat brankas cadangan, Anda harus menentukan kunci enkripsi AWS Key Management Service (AWS KMS) yang mengenkripsi beberapa cadangan yang ditempatkan di brankas ini. Enkripsi untuk backup lainnya dikelola oleh layanan sumber AWS mereka. Untuk informasi selengkapnya tentang enkripsi, lihat bagan di Enkripsi untuk pencadangan di. AWS

Akun Anda akan selalu memiliki brankas cadangan default. Jika Anda memerlukan kunci enkripsi atau kebijakan akses yang berbeda untuk grup cadangan yang berbeda, Anda dapat membuat beberapa brankas cadangan.

Bagian ini memberikan ikhtisar tentang cara mengelola brankas cadangan Anda. AWS Backup

Topik

Kubah yang memiliki lubang udara secara logis (pratinjau)

> **Note**
>
> Mulai 9 Agustus 2023, AWS Backup menawarkan pratinjau untuk menggunakan brankas yang memiliki celah udara secara logis. Untuk mendaftar di pratinjau ini, kirim permintaan melalui email ke <aws-backup-vault-preview@amazon .com>.
> Fitur dapat berubah atau disesuaikan selama dan setelah periode pratinjau. Ketika layanan menjadi Generally Available (GA), data dan konfigurasi yang disediakan selama pratinjau tidak akan lagi tersedia. AWS merekomendasikan penggunaan data uji alih-alih data produksi dengan pratinjau.

Gambaran Umum

AWS Backup mempratinjau jenis brankas sekunder yang dapat menyimpan salinan cadangan di brankas lain. Vault yang memiliki celah udara secara logis adalah brankas khusus yang menawarkan peningkatan fitur keamanan selain dari brankas cadangan serta kemampuan untuk berbagi akses brankas ke akun dan organisasi lain sehingga waktu pemulihan (RTO) dapat lebih cepat dan lebih fleksibel jika terjadi insiden yang membutuhkan pemulihan sumber daya yang cepat.

Kubah celah udara secara logis dilengkapi dengan fitur perlindungan tambahan: masing-masing brankas ini dienkripsi dengan kunci yang AWS dimiliki, dan setiap brankas memiliki kunci brankas yang diatur dalam mode kepatuhan.

Anda dapat memilih untuk berbagi brankas dengan celah udara secara logis di seluruh organisasi dan akun sehingga cadangan yang disimpan di dalamnya dapat dipulihkan dari akun yang digunakan untuk berbagi brankas, jika diperlukan.

Tidak ada biaya tambahan untuk penyimpanan di brankas yang memiliki celah udara secara logis selama periode pratinjau. Pencadangan di brankas cadangan standar dan salinan lintas wilayah masih akan dikenakan biaya dengan tarif yang dipublikasikan (lihat harga) meskipun salinan cadangan tersebut di brankas yang memiliki celah udara secara logis tidak dikenakan biaya.

Kasus penggunaan

Vault yang memiliki celah udara secara logis adalah brankas sekunder yang berfungsi sebagai bagian dari strategi perlindungan data. Vault ini dapat membantu meningkatkan retensi dan pemulihan organisasi Anda saat Anda menginginkan brankas untuk cadangan Anda

- Secara otomatis diatur dengan kunci brankas dalam mode kepatuhan
- Berisi cadangan yang dapat dibagikan dan dipulihkan dari akun yang berbeda dari yang membuat cadangan
- Dilengkapi dienkripsi dengan kunci yang dimiliki AWS

Sumber daya yang didukung dalam brankas yang memiliki celah udara secara logis termasuk

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

Pratinjau kubah celah udara secara logis ini hanya tersedia di Wilayah AS Timur (Virginia N.). Karena fitur ini saat ini hanya ada di satu Wilayah, salinan lintas wilayah tidak didukung selama periode pratinjau ini.

Bandingkan dan kontraskan dengan brankas cadangan standar

Brankas cadangan adalah jenis brankas utama dan standar yang digunakan. AWS Backup Setiap cadangan disimpan dalam brankas cadangan saat cadangan dibuat. Anda dapat menetapkan kebijakan berbasis sumber daya untuk mengelola cadangan yang disimpan di vault, seperti siklus hidup pencadangan yang disimpan di dalam vault.

Vault yang memiliki celah udara secara logis adalah brankas khusus dengan keamanan tambahan dan berbagi fleksibel untuk waktu pemulihan yang lebih cepat (RTO). Vault ini menyimpan salinan cadangan yang awalnya dibuat dan disimpan dalam brankas cadangan standar.

Brankas cadangan dapat dienkripsi dengan kunci, mekanisme keamanan yang membatasi akses ke pengguna yang dituju. Kunci-kunci ini dapat dikelola atau AWS dikelola oleh pelanggan. Selain itu, brankas cadangan bahkan dapat lebih diamankan dengan kunci brankas; secara logis kubah celah udara dilengkapi dengan kunci brankas dalam mode kepatuhan.

Jika AWS KMS kunci tidak diubah atau disetel secara manual sebagai kunci terkelola pelanggan (CMK) pada saat sumber daya awal dibuat, cadangan tidak dapat disalin ke brankas yang memiliki celah udara secara logis.

Fitur	Brankas cadangan	Lemari besi yang memiliki lubang udara secara logis (pratinjau)
Pembuatan Backup	Ketika cadangan dibuat, itu disimpan sebagai titik pemulihan	Cadangan tidak disimpan di brankas ini saat pembuatan
Penyimpanan cadangan	Dapat menyimpan cadangan awal sumber daya dan salinan cadangan	Dapat menyimpan salinan cadangan dari brankas lain
Keamanan	Secara opsional dapat dienkripsi dengan kunci (dikelola atau dikelola pelanggan) AWS Secara opsional dapat dikunci dengan kunci brankas	Dienkripsi dengan kunci yang dimiliki AWS Selalu terkunci dengan kunci brankas dalam mode kepatuhan
Sharabilitas	Akses dapat dikelola melalui kebijakan dan AWS Organizations Tidak kompatibel dengan AWS Resource Access Manager	Secara opsional dapat dibagikan di seluruh akun menggunakan AWS RAM
Restorasi	Cadangan dapat dipulihkan oleh akun yang sama yang memiliki brankas	Cadangan dapat dipulihkan oleh akun yang berbeda dari akun yang memiliki cadangan jika brankas dibagikan dengan akun terpisah itu
Regionalitas	Tersedia di semua Wilayah di mana AWS Backup beroperasi	Tersedia di Wilayah AS Timur (Virginia N.) selama pratinjau
Sumber Daya	Dapat menyimpan cadangan yang berisi semua AWS	Dapat menyimpan cadangan yang berisi data Amazon EC2,

Fitur	Brankas cadangan	Lemari besi yang memiliki lubang udara secara logis (pratinjau)
	Backup sumber daya yang didukung	Amazon EBS, Amazon EFS, Amazon S3, atau Amazon RDS

Buat brankas yang memiliki celah udara secara logis dari konsol

> **Important**
>
> Setelah vault dibuat, nama vault, jenis vault, dan periode retensi minimum dan maksimum tidak dapat diubah; selain itu, kunci vault tidak dapat dihapus.
> Ketika layanan tersedia secara umum, data dan konfigurasi yang disediakan selama pratinjau tidak akan lagi tersedia. AWS merekomendasikan penggunaan data uji alih-alih data produksi dengan pratinjau.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Vaults.
3. Kedua jenis brankas akan ditampilkan. Pilih Buat brankas baru.
4. Masukkan nama untuk brankas cadangan Anda. Anda dapat memberi nama brankas Anda untuk mencerminkan apa yang akan Anda simpan di dalamnya, atau untuk membuatnya lebih mudah untuk mencari cadangan yang Anda butuhkan. Misalnya, Anda bisa menamainya`FinancialBackups`.
5. Pilih tombol radio untuk brankas dengan celah udara secara logis.
6. Tetapkan periode retensi minimum.

   Nilai ini (dalam hari, bulan, atau tahun) adalah jumlah waktu terpendek cadangan dapat disimpan di lemari besi ini. Pencadangan dengan periode retensi yang lebih pendek dari nilai ini tidak dapat disalin ke brankas ini.
7. Atur periode retensi maksimum.

Nilai ini (dalam hari, bulan, atau tahun) adalah jumlah waktu terlama cadangan dapat disimpan di lemari besi ini. Cadangan dengan periode retensi yang lebih besar dari nilai ini tidak dapat disalin ke brankas ini.

8. (Opsional) Tambahkan tag yang akan membantu Anda mencari dan mengidentifikasi brankas Anda yang memiliki celah udara secara logis. Misalnya, Anda bisa menambahkan `BackupType:Financial` tag.
9. Pilih Buat lemari besi.
10. Tinjau pengaturan. Jika semua pengaturan ditampilkan seperti yang Anda inginkan, pilih Buat brankas dengan celah udara secara logis.
11. Konsol akan membawa Anda ke halaman detail brankas baru Anda. Verifikasi detail brankas seperti yang diharapkan.

Lihat detail vault yang memiliki celah udara secara logis di konsol

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pilih Vaults dari navigasi sebelah kiri.
3. Di bawah deskripsi brankas akan ada dua daftar, Vault yang dimiliki oleh akun ini dan Vaults dibagikan dengan akun ini. Pilih tab yang diinginkan untuk melihat brankas.
4. Di bawah nama Vault, klik nama brankas untuk membuka halaman detail. Anda dapat melihat ringkasan, titik pemulihan, sumber daya yang dilindungi, berbagi akun, kebijakan akses, dan detail tag.

Salin dari brankas cadangan standar ke brankas yang memiliki celah udara secara logis di konsol

Logika air-gapped vaults hanya dapat menjadi target tujuan pekerjaan salinan dalam rencana cadangan atau target untuk pekerjaan salinan sesuai permintaan.

Untuk memulai pekerjaan fotokopi, Anda harus memiliki

- Brankas cadangan
- Sebuah lemari besi yang memiliki celah udara secara logis
- Cadangan yang berisi data Amazon EC2, Amazon EBS, Amazon RDS, Amazon S3, atau Amazon EFS

- Izin `kms:CreateGrant`untuk peran yang digunakan untuk membuat salinan.
- Tidak ada cadangan yang dienkripsi dengan kunci AWS terkelola sebagai bagian dari pekerjaan penyalinan Anda ke brankas yang celah udara secara logis

Setelah Anda mengkonfirmasi hal di atas,

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pilih Vaults dari navigasi sebelah kiri.
3. Di halaman detail vault, semua titik pemulihan di dalam brankas itu ditampilkan. Tempatkan tanda centang di sebelah titik pemulihan yang ingin Anda salin.
4. Pilih Tindakan, lalu pilih Salin dari menu tarik-turun.
5. Pada layar berikutnya, masukkan detail tujuan.
   a. Wilayah harus diatur ke AS Timur (Virginia N.)
   b. Menu drop-down vault cadangan tujuan menampilkan brankas tujuan yang memenuhi syarat. Pilih salah satu dengan tipe `logically air-gapped vault`
6. Pilih Salin setelah semua detail diatur ke preferensi Anda.

Pada halaman Pekerjaan di konsol, Anda dapat memilih Salin pekerjaan untuk melihat pekerjaan salinan saat ini.

Untuk informasi selengkapnya, lihat Menyalin cadangan, Pencadangan lintas wilayah, dan Pencadangan lintas akun.

Bagikan brankas yang memiliki celah udara secara logis dari konsol

> **Note**
>
> Hanya akun dengan hak istimewa IAM tertentu yang dapat berbagi dan mengelola berbagi akun.

Anda dapat menggunakan AWS RAM untuk berbagi brankas yang memiliki celah udara secara logis dengan akun lain yang Anda tunjuk. Untuk berbagi menggunakan AWS RAM, pastikan Anda memiliki yang berikut:

- Dua atau lebih akun yang dapat diakses AWS Backup
- Akun yang bermaksud berbagi memiliki izin RAM yang diperlukan. Izin `ram:CreateResourceShare` diperlukan untuk prosedur ini. Kebijakan ini `AWSResourceAccessManagerFullAccess` berisi semua izin terkait RAM yang diperlukan.
- Setidaknya satu lemari besi yang memiliki lubang udara secara logis

Untuk berbagi lemari besi yang memiliki lubang udara secara logis,

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pilih Vaults dari navigasi sebelah kiri.
3. Di bawah deskripsi brankas akan ada dua daftar, Vault yang dimiliki oleh akun ini dan Vaults dibagikan dengan akun ini. Pilih daftar yang diinginkan untuk melihat brankas.
4. Di bawah nama Vault, pilih nama brankas yang memiliki celah udara secara logis untuk membuka halaman detail.
5. Panel berbagi akun menunjukkan dengan akun mana vault sedang dibagikan.
6. Untuk mulai berbagi dengan akun lain atau mengedit akun yang sudah dibagikan, pilih Kelola berbagi.

AWS RAM konsol terbuka saat Kelola berbagi dipilih. Untuk langkah-langkah berbagi sumber daya menggunakan AWS RAM, lihat Membuat pembagian sumber daya di AWS RAM.

Pastikan Anda memiliki izin yang sesuai. Kebijakan IAM Administrator Backup [AWSBackupFullAccess] dan Kebijakan IAM Operator Cadangan [AWSBackupOperatorAccess] berisi izin yang diperlukan untuk melihat akun bersama; namun, peran yang Anda gunakan untuk berbagi memerlukan izin tulis Resource Access Manager untuk membagikan akun dari RAM, seperti. `ram:CreateResourceShare`

Akun yang diundang untuk menerima undangan untuk menerima bagian memiliki 12 jam untuk menerima undangan. Lihat Menerima dan menolak undangan berbagi sumber daya di Panduan Pengguna RAM.AWS

Jika langkah berbagi selesai dan diterima, halaman ringkasan vault akan ditampilkan di bawah Berbagi akun = “Dibagikan - lihat tabel berbagi akun di bawah”.

Pulihkan cadangan dari brankas yang memiliki celah udara secara logis menggunakan konsol

Anda dapat memulihkan cadangan yang disimpan dalam brankas yang memiliki celah udara secara logis baik dari akun yang memiliki brankas atau dari akun mana pun yang digunakan untuk berbagi brankas.

Lihat Memulihkan cadangan untuk informasi tentang cara memulihkan titik pemulihan.

Hapus brankas yang memiliki celah udara secara logis menggunakan konsol

> **Important**
>
> Ketika layanan tersedia secara umum, data dan konfigurasi yang disediakan selama pratinjau tidak akan lagi tersedia. AWS merekomendasikan penggunaan data uji alih-alih data produksi dengan pratinjau.

Lihat menghapus brankas cadangan untuk menghapus vault. Vault tidak dapat dihapus jika masih berisi cadangan (titik pemulihan). Pastikan vault kosong dari cadangan sebelum Anda memulai operasi penghapusan.

Kubah celah udara secara logis melalui CLI/API

Anda dapat menggunakannya AWS CLI untuk melakukan operasi secara terprogram untuk kubah yang memiliki celah udara secara logis. Setiap CLI khusus untuk AWS layanan di mana ia berasal. Perintah yang terkait dengan berbagi ditambahkan dengan`aws ram`; semua perintah lainnya harus ditambahkan dengan. `aws backup`

Buat

Contoh perintah CLI berikut `CreateLogicallyAirGappedBackupVault` dapat dimodifikasi untuk membuat brankas cadangan yang memiliki celah udara secara logis:

```
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
```

Lihat detail

Contoh perintah CLI berikut `DescribeBackupVault` dapat dimodifikasi untuk mendapatkan detail tentang brankas:

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

Bagikan

> **Note**
>
> Hanya akun dengan izin IAM yang memadai yang dapat berbagi dan mengelola berbagi akun.

Anda dapat berbagi brankas dengan celah udara secara logis melalui AWS Resource Access Manager(RAM), layanan yang membantu pengguna berbagi sumber daya.

AWS RAM menggunakan perintah CLI. `create-resource-share` Akses ke perintah ini hanya tersedia untuk akun admin dengan izin yang memadai. Lihat Membuat berbagi sumber daya AWS RAM untuk langkah-langkah CLI.

Langkah 1 hingga 4 dilakukan dengan akun yang memiliki brankas celah udara secara logis. Langkah 5 hingga 8 dilakukan dengan akun yang digunakan untuk berbagi brankas yang memiliki celah udara secara logis.

1. Masuk ke akun pemilik ATAU minta pengguna di organisasi Anda dengan kredensi yang cukup untuk mengakses akun sumber menyelesaikan langkah-langkah ini.

    - Jika pembagian sumber daya sebelumnya dibuat dan Anda ingin menambahkan sumber daya tambahan ke dalamnya, gunakan CLI `associate-resource-share` sebagai gantinya dengan ARN dari brankas baru.

2. Ambil kredensi peran dengan izin yang cukup untuk dibagikan melalui RAM. Masukkan ini ke dalam CLI.

   - Izin `ram:CreateResourceShare` diperlukan untuk prosedur ini. Kebijakan ini AWSResourceAccessManagerFullAccessberisi semua izin terkait RAM.

3. Gunakan create-resource-share.

   a. Sertakan ARN dari brankas yang memiliki celah udara secara logis.

   b. Contoh masukan:

```
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
```

   Contoh output:

```
{
   "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. Salin ARN berbagi sumber daya dalam output (yang diperlukan untuk langkah selanjutnya). Berikan ARN kepada operator akun yang Anda undang untuk menerima bagian.

5. Dapatkan pembagian sumber daya ARN

   a. Jika Anda tidak melakukan langkah 1 sampai 4, dapatkan resourceShareArn dari siapa pun yang melakukannya.

   b. Contoh: `arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543`

6. Dalam CLI, asumsikan kredensi akun penerima.
7. Dapatkan undangan berbagi sumber daya dengan `get-resource-share-invitations`. Untuk informasi selengkapnya, lihat Menerima dan menolak undangan di Panduan Pengguna.AWS RAM
8. Terima undangan di akun tujuan (pemulihan).
    - Gunakan `accept-resource-share-invitation`(bisa juga `reject-resource-share-invitation`).

Daftar

Perintah CLI `ListBackupVaults`dapat dimodifikasi untuk mencantumkan semua brankas yang dimiliki oleh dan hadir di akun:

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

Untuk membuat daftar hanya brankas yang memiliki celah udara secara logis, tambahkan parameternya

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

Untuk membuat daftar vault yang dibagikan dengan akun, gunakan

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

Salin

Vault yang memiliki celah udara secara logis hanya dapat menjadi target untuk pekerjaan penyalinan cadangan, bukan target pekerjaan pencadangan awal. Gunakan `StartCopyJob`untuk menyalin cadangan yang ada di brankas cadangan ke brankas yang memiliki celah udara secara logis.

Peran yang digunakan untuk membuat pekerjaan penyalinan ke brankas yang memiliki celah udara secara logis harus berisi izin. `kms:CreateGrant`

Contoh masukan CLI:

```
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
```

Memulihkan

Setelah cadangan dibagikan dari brankas yang memiliki celah udara secara logis ke akun Anda, Anda dapat menggunakannya `StartRestoreJob`untuk memulihkan cadangan. Contoh masukan CLI:

```
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
```

Hapus

Contoh perintah CLI berikut `DeleteBackupVault`dapat digunakan untuk menghapus vault. Vault hanya dapat dihapus jika tidak ada cadangan (titik pemulihan) di dalam brankas.

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

Opsi program lain yang tersedia meliputi:

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

Buat brankas cadangan

Anda harus membuat setidaknya satu brankas sebelum membuat rencana cadangan atau memulai pekerjaan pencadangan.

Saat pertama kali menggunakan AWS Backup konsol di konsol Wilayah AWS, konsol secara otomatis membuat brankas default.

Namun, jika Anda menggunakan AWS Backup melalui AWS CLI, AWS SDK, atau AWS CloudFormation, vault default tidak dibuat. Anda harus membuat lemari besi Anda sendiri.

Izin yang diperlukan

Anda harus memiliki izin berikut untuk membuat brankas cadangan menggunakan. 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": "*"
    }
  ]
}
```

Membuat brankas cadangan (konsol)

Untuk step-by-step petunjuk membuat brankas cadangan menggunakan AWS Backup konsol, lihat Langkah 3: Buat brankas cadangan di panduan Memulai.

Membuat brankas cadangan (secara terprogram)

AWS Command Line Interface Perintah berikut membuat brankas cadangan:

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

Anda juga dapat menentukan konfigurasi berikut untuk brankas cadangan.

Nama brankas cadangan

Nama brankas cadangan peka huruf besar/kecil. Mereka harus berisi 2 hingga 50 karakter alfanumerik, tanda hubung, atau garis bawah.

AWS KMS kunci enkripsi

Kunci AWS KMS enkripsi melindungi cadangan Anda di brankas cadangan ini. Secara default, AWS Backup membuat kunci KMS dengan alias `aws/backup` untuk Anda. Anda dapat memilih kunci itu atau memilih kunci lain di akun Anda (kunci KMS lintas akun dapat digunakan melalui CLI).

Anda dapat membuat kunci enkripsi baru dengan mengikuti prosedur Creating Keys di Panduan AWS Key Management Service Pengembang.

Setelah membuat brankas cadangan dan menyetel kunci AWS KMS enkripsi, Anda tidak dapat lagi mengedit kunci untuk brankas cadangan tersebut.

Kunci enkripsi yang ditentukan dalam AWS Backup brankas berlaku untuk cadangan jenis sumber daya tertentu. Untuk informasi selengkapnya tentang enkripsi cadangan, lihat Enkripsi untuk backup di AWS Backup di bagian Keamanan. Cadangan semua jenis sumber daya lainnya dicadangkan menggunakan kunci yang digunakan untuk mengenkripsi sumber daya sumber.

Tag brankas cadangan

Tag ini dikaitkan dengan brankas cadangan untuk membantu Anda mengatur dan melacak brankas cadangan Anda.

Tetapkan kebijakan akses pada brankas cadangan

Dengan AWS Backup, Anda dapat menetapkan kebijakan ke brankas cadangan dan sumber daya yang dikandungnya. Menetapkan kebijakan memungkinkan Anda melakukan hal-hal seperti memberikan akses kepada pengguna untuk membuat paket cadangan dan pencadangan sesuai permintaan, tetapi membatasi kemampuan mereka untuk menghapus titik pemulihan setelah dibuat.

Untuk informasi tentang penggunaan kebijakan untuk memberikan atau membatasi akses ke sumber daya, lihat Kebijakan Berbasis Identitas dan Kebijakan Berbasis Sumber Daya di Panduan Pengguna IAM. Anda juga dapat mengontrol akses menggunakan tag.

Anda dapat menggunakan contoh kebijakan berikut sebagai panduan untuk membatasi akses ke sumber daya saat Anda bekerja dengan AWS Backup vault. Tidak seperti kebijakan berbasis IAM lainnya, kebijakan AWS Backup akses tidak mendukung wildcard di kunci. `Action`

Untuk daftar Nama Sumber Daya Amazon (ARN) yang dapat Anda gunakan untuk mengidentifikasi titik pemulihan untuk jenis sumber daya yang berbeda, lihat AWS Backup ARN sumber daya untuk ARN titik pemulihan khusus sumber daya.

Kebijakan akses Vault hanya mengontrol akses pengguna ke AWS Backup API. Beberapa jenis cadangan, seperti snapshot Amazon Elastic Block Store (Amazon EBS) dan Amazon Relational Database Service (Amazon RDS), juga dapat diakses menggunakan API dari layanan tersebut. Anda dapat membuat kebijakan akses terpisah di IAM yang mengontrol akses ke API tersebut untuk sepenuhnya mengontrol akses ke jenis cadangan tersebut.

Terlepas dari kebijakan akses AWS Backup vault, akses lintas akun untuk tindakan apa pun selain `backup:CopyIntoBackupVault` akan ditolak; yaitu, AWS Backup akan menolak permintaan lain dari akun yang berbeda dari akun sumber daya yang direferensikan.

Topik

- Tolak akses ke jenis sumber daya di brankas cadangan
- Tolak akses ke brankas cadangan
- Tolak akses untuk menghapus titik pemulihan di brankas cadangan

Tolak akses ke jenis sumber daya di brankas cadangan

Kebijakan ini menolak akses ke operasi API yang ditentukan untuk semua snapshot Amazon EBS di brankas cadangan.

```
{
    "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/*"]
        }
    ]
}
```

Tolak akses ke brankas cadangan

Kebijakan ini menolak akses ke operasi API tertentu yang menargetkan brankas cadangan.

```
{
    "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"
        }
    ]
}
```

Tolak akses untuk menghapus titik pemulihan di brankas cadangan

Akses ke brankas dan kemampuan untuk menghapus titik pemulihan yang tersimpan di dalamnya ditentukan oleh akses yang Anda berikan kepada pengguna Anda.

Ikuti langkah-langkah berikut untuk membuat kebijakan akses berbasis sumber daya pada brankas cadangan yang mencegah penghapusan cadangan apa pun di brankas cadangan.

Untuk membuat kebijakan akses berbasis sumber daya di brankas cadangan

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi di sebelah kiri, pilih Backup vaults.
3. Pilih brankas cadangan dalam daftar.
4. Di bagian Kebijakan akses, tempel contoh JSON berikut. Kebijakan ini mencegah siapa pun yang bukan prinsipal menghapus titik pemulihan di brankas cadangan target.

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

```
                    "AAAAAAAAAAAAAAAAAAAAA:",
                    "BBBBBBBBBBBBBBBBBBBBB",
                    "112233445566"
                ]
            }
        }
    ]
}
```

Untuk mengizinkan identitas IAM daftar menggunakan ARN mereka, gunakan kunci kondisi `aws:PrincipalArn` global dalam contoh berikut.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Untuk informasi tentang mendapatkan ID unik untuk entitas IAM, lihat Mendapatkan pengenal unik di Panduan Pengguna IAM.

Jika Anda ingin membatasi ini ke jenis sumber daya tertentu, alih-alih`"Resource": "*"`, Anda dapat secara eksplisit menyertakan jenis titik pemulihan untuk ditolak. Misalnya, untuk snapshot Amazon EBS, ubah jenis sumber daya menjadi yang berikut.

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

5. Pilih Lampirkan kebijakan.

AWS Backup Kunci Brankas

> **Note**
>
> AWS Backup Vault Lock telah dinilai oleh Cohasset Associates untuk digunakan di lingkungan yang tunduk pada peraturan SEC 17a-4, CFTC, dan FINRA. Untuk informasi selengkapnya tentang bagaimana AWS Backup Vault Lock berhubungan dengan peraturan ini, lihat Penilaian Kepatuhan Cohasset Associates.

AWS Backup Vault Lock adalah fitur opsional dari brankas cadangan, yang dapat membantu memberi Anda keamanan dan kontrol tambahan atas brankas cadangan Anda. Ketika kunci aktif dalam mode Kepatuhan dan waktu tenggang berakhir, konfigurasi vault tidak dapat diubah atau dihapus oleh pelanggan, pemilik akun/data, atau. AWS Setiap lemari besi dapat memiliki satu kunci brankas di tempatnya.

AWS Backup memastikan bahwa cadangan Anda tersedia untuk Anda sampai mereka mencapai berakhirnya periode retensi mereka. Jika ada pengguna (termasuk pengguna root) yang mencoba menghapus cadangan atau mengubah properti siklus hidup di brankas yang terkunci, AWS Backup akan menolak operasi.

- Vault yang terkunci dalam mode tata kelola dapat menghapus kunci oleh pengguna dengan izin IAM yang memadai.
- Vault yang terkunci dalam mode kepatuhan tidak dapat dihapus setelah periode pendinginan (" waktu tenggang ") berakhir. Selama waktu tenggang, Anda masih dapat menghapus kunci brankas dan mengubah konfigurasi kunci.

Mode kunci lemari besi

Saat membuat kunci vault, Anda memiliki dua pilihan mode: Mode tata kelola atau mode Kepatuhan. Mode tata kelola dimaksudkan untuk memungkinkan brankas dikelola hanya oleh pengguna dengan hak istimewa IAM yang memadai. Mode tata kelola membantu organisasi memenuhi persyaratan tata

kelola, memastikan hanya personel yang ditunjuk yang dapat membuat perubahan pada brankas cadangan. Mode kepatuhan ditujukan untuk brankas cadangan di mana brankas (dan dengan ekstensi, isinya) diharapkan tidak akan pernah dihapus atau diubah hingga periode penyimpanan data selesai. Setelah brankas dalam mode kepatuhan terkunci, itu tidak dapat diubah, artinya kunci tidak dapat dilepas.

Vault yang terkunci dalam mode Tata Kelola dapat dikelola atau dihapus oleh pengguna yang memiliki izin IAM yang sesuai.

Kunci brankas dalam mode Kepatuhan tidak dapat diubah atau dihapus oleh pengguna mana pun atau oleh. AWS Kunci brankas dalam mode kepatuhan memiliki masa tenggang yang Anda atur sebelum terkunci dan menjadi tidak dapat diubah.

Manfaat kunci vault

AWS Backup Vault Lock memberikan beberapa manfaat, antara lain:

- Konfigurasi WORM (tulis-sekali, baca-banyak) untuk semua cadangan yang Anda simpan dan buat di brankas cadangan.
- Lapisan pertahanan tambahan yang melindungi cadangan (titik pemulihan) di brankas cadangan Anda dari penghapusan yang tidak disengaja atau berbahaya.
- Penegakan periode retensi, yang mencegah penghapusan dini oleh pengguna istimewa (termasuk pengguna Akun AWS root), dan memenuhi kebijakan dan prosedur perlindungan data organisasi Anda.

Kunci brankas cadangan menggunakan konsol

Anda dapat menambahkan kunci vault ke AWS Backup Vault menggunakan konsol Backup.

Untuk menambahkan kunci vault ke brankas cadangan Anda:

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, temukan Brankas Cadangan. Klik tautan yang bersarang di bawah Brankas Cadangan yang disebut kunci Vault.
3. Di bawah Cara kerja kunci vault atau kunci Vault, klik + Buat kunci vault.
4. Di panel Detail kunci Vault, pilih brankas mana yang ingin Anda gunakan untuk mengunci.

5. Di bawah mode kunci Vault pilih mode mana Anda ingin brankas Anda terkunci. Untuk informasi selengkapnya tentang memilih mode, lihat Mode kunci Vault sebelumnya di halaman ini.
6. Untuk periode Retensi, pilih periode retensi minimum dan maksimum (periode retensi adalah opsional). Pekerjaan pencadangan dan penyalinan baru yang dibuat di vault akan gagal jika tidak sesuai dengan periode penyimpanan yang Anda tetapkan; periode ini tidak akan berlaku untuk titik pemulihan yang sudah ada di brankas.
7. Jika Anda memilih mode kepatuhan, bagian yang disebut Tanggal mulai kunci Vault akan ditampilkan. Jika Anda memilih mode Tata Kelola, ini tidak akan ditampilkan, dan langkah ini dapat dilewati.

   Dalam mode kepatuhan, kunci brankas memiliki periode pendinginan dari pembuatan kunci lemari besi hingga lemari besi dan kuncinya menjadi tidak dapat diubah dan tidak dapat diubah. Anda memilih durasi periode ini (disebut waktu tenggang), meskipun harus minimal 3 hari (72 jam).

   > **Important**
   >
   > Setelah waktu tenggang berakhir, lemari besi dan kuncinya tidak dapat diubah. Itu tidak dapat diubah atau dihapus oleh pengguna atau oleh AWS.

8. Bila Anda puas dengan pilihan konfigurasi, klik Create vault lock.
9. Untuk mengonfirmasi bahwa Anda ingin membuat kunci ini dalam mode yang dipilih, ketik `confirm` kotak teks, lalu centang kotak yang mengakui konfigurasi sebagaimana dimaksud.

Jika langkah-langkah telah berhasil diselesaikan, spanduk “Sukses” akan muncul di bagian atas konsol.

Kunci brankas cadangan secara terprogram

Untuk mengonfigurasi AWS Backup Vault Lock, gunakan API`PutBackupVaultLockConfiguration`. Parameter yang akan disertakan akan tergantung pada mode kunci vault mana yang Anda inginkan. Jika Anda ingin membuat kunci brankas dalam mode tata kelola, jangan sertakan. `ChangeableForDays` Jika parameter ini disertakan, kunci vault akan dibuat dalam mode kepatuhan.

Berikut adalah contoh CLI dari pembuatan kunci vault mode kepatuhan:

```
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
```

Berikut adalah contoh CLI dari pembuatan kunci brankas mode tata kelola:

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

Anda dapat mengkonfigurasi empat opsi.

1. **`BackupVaultName`**

   Nama lemari besi untuk dikunci.

2. **`ChangeableForDays`**(termasuk hanya untuk mode kepatuhan)

   Parameter ini menginstruksikan AWS Backup untuk membuat kunci vault dalam mode kepatuhan. Hilangkan parameter ini jika Anda bermaksud membuat kunci dalam mode tata kelola.

   Nilai ini dinyatakan dalam beberapa hari. Itu harus angka tidak kurang dari 3 dan tidak lebih dari 36.500; jika tidak, kesalahan akan kembali.

   Dari pembuatan kunci brankas ini hingga berakhirnya tanggal yang ditentukan, kunci vault dapat dihapus dari lemari besi menggunakan. `DeleteBackupVaultLockConfiguration` Atau, selama waktu ini, Anda dapat mengubah konfigurasi menggunakan`PutBackupVaultLockConfiguration`.

   Pada dan setelah tanggal yang ditentukan ditentukan oleh parameter ini, brankas cadangan akan tidak dapat diubah dan tidak dapat diubah atau dihapus.

3. **`MaxRetentionDays`**(opsional)

   Ini adalah nilai numerik yang dinyatakan dalam hari. Ini adalah periode retensi maksimum dimana brankas mempertahankan titik pemulihannya.

   Kerangka waktu retensi maksimum yang Anda pilih harus selaras dengan kebijakan organisasi Anda untuk menyimpan data. Jika organisasi Anda menginstruksikan data untuk disimpan selama suatu periode, nilai ini dapat diatur ke periode tersebut (dalam beberapa hari). Misalnya, data

keuangan atau perbankan mungkin diperlukan untuk disimpan selama 7 tahun (sekitar 2.557 hari, tergantung pada tahun kabisat).

Jika tidak ditentukan, AWS Backup Vault Lock tidak akan memberlakukan periode retensi maksimum. Jika ditentukan, cadangan dan salin pekerjaan ke vault ini dengan periode retensi siklus hidup yang lebih lama dari periode retensi maksimum akan gagal. Titik pemulihan yang sudah disimpan di brankas sebelum pembuatan kunci vault tidak terpengaruh. Periode retensi maksimum terpanjang yang dapat Anda tentukan adalah 36500 hari (sekitar 100 tahun).

4. **`MinRetentionDays`**(opsional; diperlukan untuk CloudFormation)

   Ini adalah nilai numerik yang dinyatakan dalam hari. Ini adalah periode retensi minimum dimana vault mempertahankan titik pemulihannya. Pengaturan ini harus diatur ke jumlah waktu organisasi Anda diperlukan untuk memelihara data. Misalnya, jika peraturan atau undang-undang mengharuskan data disimpan setidaknya selama tujuh tahun, nilainya dalam hari akan menjadi sekitar 2.557, tergantung pada tahun kabisat.

   Jika tidak ditentukan, AWS Backup Vault Lock tidak akan memberlakukan periode retensi minimum. Jika ditentukan, cadangan dan salin pekerjaan ke vault ini dengan periode retensi siklus hidup yang lebih pendek dari periode retensi minimum akan gagal. Titik pemulihan yang sudah disimpan di brankas sebelum AWS Backup Vault Lock tidak terpengaruh. Periode retensi minimum terpendek yang dapat Anda tentukan adalah 1 hari.

Tinjau brankas cadangan untuk konfigurasi AWS Backup Vault Lock

Anda dapat meninjau detail AWS Backup Vault Lock di vault kapan saja dengan menelepon `DescribeBackupVault` atau `ListBackupVaults` API.

Untuk menentukan apakah Anda menerapkan kunci vault ke brankas cadangan, hubungi `DescribeBackupVault` dan periksa properti. `Locked` Jika`"Locked": true`, seperti contoh berikut, Anda telah menerapkan AWS Backup Vault Lock ke brankas cadangan Anda.

```
{
    "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"
}
```

Output sebelumnya mengkonfirmasi opsi berikut:

1. `Locked`adalah Boolean yang menunjukkan apakah Anda telah menerapkan AWS Backup Vault Lock ke brankas cadangan ini. `True`berarti bahwa AWS Backup Vault Lock menyebabkan operasi penghapusan atau pembaruan ke titik pemulihan yang disimpan di brankas gagal (terlepas dari apakah Anda masih dalam masa tenggang waktu pendinginan).
2. `LockDate`adalah tanggal dan waktu UTC ketika masa tenggang pendinginan Anda berakhir. Setelah waktu ini, Anda tidak dapat menghapus atau mengubah kunci Anda di brankas ini. Gunakan konverter waktu yang tersedia untuk umum untuk mengonversi string ini ke waktu lokal Anda.

Jika`"Locked":false`, seperti contoh berikut, Anda belum menerapkan kunci vault (atau yang sebelumnya telah dihapus).

```
{
    "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
}
```

Penghapusan kunci brankas selama waktu tenggang (Mode kepatuhan)

Untuk menghapus kunci vault Anda selama waktu tenggang (waktu setelah mengunci brankas tetapi sebelum Anda`LockDate`) menggunakan konsol, AWS Backup

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.

2. Di navigasi kiri di bawah Akun saya, klik Backup vaults, lalu klik Backup Vault Lock.
3. Klik kunci vault yang ingin Anda hapus, lalu klik Kelola kunci vault.
4. Klik Hapus kunci brankas.
5. Kotak peringatan akan muncul, meminta Anda mengonfirmasi maksud Anda untuk menghapus kunci vault. Ketik `confirm` ke dalam kotak teks, lalu klik konfirmasi.

Setelah semua langkah berhasil diselesaikan, spanduk Sukses akan muncul di bagian atas layar konsol.

Untuk menghapus kunci vault Anda selama waktu tenggang menggunakan perintah CLI, `DeleteBackupVaultLockConfiguration` gunakan contoh CLI seperti ini:

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

Akun AWS penutupan dengan lemari besi terkunci

Ketika Anda menutup sebuah Akun AWS yang berisi brankas cadangan, AWS dan AWS Backup menangguhkan akun Anda selama 90 hari dengan cadangan Anda utuh. Jika Anda tidak membuka kembali akun selama 90 hari tersebut, AWS menghapus konten brankas cadangan Anda, meskipun AWS Backup Vault Lock sudah terpasang.

Pertimbangan keamanan tambahan

AWS Backup Vault Lock menambahkan lapisan keamanan tambahan ke pertahanan perlindungan data Anda secara mendalam. Kunci vault dapat dikombinasikan dengan fitur keamanan lainnya:

- Enkripsi untuk titik pemulihan Anda
- AWS Backup kebijakan akses vault dan titik pemulihan, yang memungkinkan Anda memberikan atau menolak izin di tingkat vault,
- AWS Backup praktik terbaik keamanan, termasuk pustaka kebijakan terkelola pelanggan yang memungkinkan Anda memberikan atau menolak izin pencadangan dan pemulihan oleh layanan yang AWS didukung, dan
- AWS Backup Audit Manager, yang memungkinkan Anda mengotomatiskan pemeriksaan kepatuhan untuk cadangan Anda terhadap daftar kontrol yang Anda tentukan.

Anda dapat bekerja Membuat kerangka kerja menggunakan API AWS Backup untuk kontrol Cadangan dilindungi oleh AWS Backup Vault Lock dengan AWS Backup Audit Manager untuk membantu memastikan bahwa sumber daya yang Anda inginkan dilindungi dengan kunci vault.

- Mekanisme yang membuat sumber daya tidak aktif dapat memengaruhi kemampuan untuk memulihkannya. Meskipun masih tidak dapat dihapus di brankas yang terkunci, mereka dapat berada dalam keadaan selain aktif. Misalnya, pengaturan Amazon Elastic Compute Cloud yang memungkinkan Anda menonaktifkan AMI dapat memblokir sementara kemampuan untuk memulihkan cadangan instans EC2. Ini memengaruhi semua titik pemulihan EC2, bahkan cadangan yang dipengaruhi oleh kunci brankas atau penahanan hukum.

  Jika cadangan EC2 dinonaktifkan, Anda dapat mengaktifkan kembali AMI yang dinonaktifkan. Setelah diaktifkan kembali, itu memenuhi syarat untuk dipulihkan. Untuk memblokir fitur nonaktifkan AMI, Anda dapat menggunakan kebijakan IAM untuk tidak mengizinkan`ec2:DisableImage`.

> **Note**
>
> AWS Backup Vault Lock bukan fitur yang sama dengan Amazon S3 Glacier Vault Lock, yang hanya kompatibel dengan S3 Glacier.

Hapus brankas cadangan

Untuk mencegah penghapusan massal yang tidak disengaja atau berbahaya, Anda dapat menghapus brankas cadangan AWS Backup hanya setelah Anda menghapus (atau siklus hidup paket cadangan) semua titik pemulihan di brankas cadangan Anda. Untuk menghapus titik pemulihan secara manual, lihat Membersihkan sumber daya.

Saat Anda menghapus brankas cadangan, perbarui paket cadangan Anda untuk menunjuk ke brankas cadangan baru. Paket cadangan yang mengarah ke brankas cadangan yang dihapus akan menyebabkan pembuatan cadangan gagal.

> **Note**
>
> Anda tidak dapat menghapus dua brankas cadangan: brankas cadangan AWS Backup default dan brankas cadangan otomatis Amazon EFS.

Untuk menghapus brankas cadangan menggunakan konsol AWS Backup

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih nama brankas cadangan untuk membuka halaman detailnya.
4. Pilih dan hapus cadangan apa pun yang terkait dengan brankas cadangan.
5. Pilih Hapus brankas. Saat diminta konfirmasi, masukkan nama vault lalu pilih Delete Backup vault.

Menggunakan cadangan

Pencadangan, atau titik pemulihan, mewakili konten sumber daya, seperti volume Amazon Elastic Block Store (Amazon EBS) atau tabel Amazon DynamoDB, pada waktu yang ditentukan. Titik pemulihan adalah istilah yang umumnya mengacu pada cadangan yang berbeda dalam AWS layanan, seperti snapshot Amazon EBS dan cadangan DynamoDB. Istilah titik pemulihan dan cadangan digunakan secara bergantian.

AWS Backup menyimpan poin pemulihan di brankas cadangan, yang dapat Anda atur sesuai dengan kebutuhan bisnis Anda. Misalnya, Anda dapat menyimpan satu set sumber daya yang berisi informasi keuangan untuk tahun fiskal 2020. Saat Anda perlu memulihkan sumber daya, Anda dapat menggunakan AWS Backup konsol atau AWS Command Line Interface (AWS CLI) untuk menemukan dan memulihkan sumber daya yang Anda butuhkan.

Setiap titik pemulihan memiliki ID unik. ID unik ada di akhir Amazon Resource Name (ARN) titik pemulihan. Untuk contoh ARN titik pemulihan dan ID unik, lihat tabel diSumber daya dan operasi.

> **Important**
>
> Untuk menghindari biaya tambahan, konfigurasikan kebijakan penyimpanan Anda dengan durasi penyimpanan hangat minimal satu minggu. Untuk informasi selengkapnya, lihat Pengukuran, biaya, dan penagihan.

Bagian berikut memberikan gambaran umum tentang tugas-tugas manajemen cadangan dasar di AWS Backup.

Topik

- Membuat cadangan
- Salin cadangan
- Menghapus cadangan
- Mengedit cadangan
- Memulihkan cadangan
- Kembalikan pengujian
- Melihat daftar backup

Membuat cadangan

Dengan AWS Backup, Anda dapat membuat cadangan secara otomatis menggunakan paket cadangan atau secara manual dengan memulai pencadangan sesuai permintaan.

Membuat backup otomatis

Ketika cadangan dibuat secara otomatis oleh rencana cadangan, mereka dikonfigurasi dengan pengaturan siklus hidup yang ditentukan dalam paket cadangan. Mereka diatur dalam brankas cadangan yang ditentukan dalam rencana cadangan. Mereka juga diberi tag yang tercantum dalam rencana cadangan. Untuk informasi selengkapnya tentang paket cadangan, lihatMengelola cadangan menggunakan rencana cadangan.

Membuat cadangan sesuai permintaan

Saat Anda membuat cadangan sesuai permintaan, Anda dapat mengonfigurasi pengaturan ini untuk cadangan yang sedang dibuat. Ketika cadangan dibuat baik secara otomatis atau manual, pekerjaan cadangan dimulai. Untuk cara membuat cadangan sesuai permintaan, lihatMembuat cadangan sesuai permintaan menggunakan AWS Backup.

Catatan: Pencadangan sesuai permintaan membuat pekerjaan cadangan; pekerjaan cadangan akan bertransisi dalam keadaan `Running` dalam waktu satu jam (atau bila ditentukan). Anda dapat memilih cadangan sesuai permintaan jika Anda ingin membuat cadangan pada waktu selain waktu yang dijadwalkan yang ditentukan dalam rencana cadangan. Cadangan sesuai permintaan dapat digunakan, misalnya, untuk menguji cadangan dan fungsionalitas kapan saja.

Pencadangan sesuai permintaan tidak dapat digunakan dengan point-in-time pemulihan (PITR) karena cadangan sesuai permintaan mempertahankan sumber daya dalam keadaan saat pencadangan diambil, sedangkan PITR menggunakan cadangan berkelanjutan yang mencatat perubahan selama periode waktu tertentu.

Status pekerjaan Backup

Setiap pekerjaan cadangan memiliki ID unik. Misalnya, `D48D8717-0C9D-72DF-1F56-14E703BF2345`.

Anda dapat melihat status pekerjaan cadangan di halaman Pekerjaan AWS Backup konsol. Status pekerjaan Backup meliputi`CREATED`,`PENDING`,,`RUNNING`,`ABORTING`,`ABORTED`,`COMPLETED`, `FAILEDEXPIRED`, dan`PARTIAL`.

Cara kerja pencadangan tambahan

Banyak sumber daya mendukung pencadangan tambahan dengan AWS Backup. Daftar lengkap tersedia di bagian cadangan tambahan dari Ketersediaan fitur berdasarkan sumber daya tabel.

Meskipun setiap cadangan setelah yang pertama bersifat inkremental (artinya hanya menangkap perubahan dari cadangan sebelumnya), semua cadangan yang dibuat dengan AWS Backup mempertahankan data referensi yang diperlukan untuk memungkinkan pemulihan penuh. Ini benar bahkan jika cadangan asli (penuh) telah mencapai akhir siklus hidupnya dan telah dihapus.

Misalnya, jika cadangan hari 1 (penuh) Anda dihapus karena kebijakan siklus hidup 3 hari, Anda masih dapat melakukan pemulihan penuh dengan pencadangan dari hari ke 2 dan 3. AWS Backup memelihara data referensi yang diperlukan dari hari pertama untuk melakukannya.

Akses ke sumber daya sumber

AWS Backup membutuhkan akses ke sumber daya sumber Anda untuk mendukungnya. Sebagai contoh:

- Untuk mencadangkan instans Amazon EC2, instans dapat berada di `stopped` negara bagian `running` atau, tetapi tidak dalam status. `terminated` Ini karena sebuah `running` atau `stopped` instance dapat berkomunikasi dengan AWS Backup, tetapi sebuah `terminated` instance tidak bisa.
- Untuk membuat cadangan mesin virtual, hypervisornya harus memiliki status gateway Backup. `ONLINE` Untuk informasi selengkapnya, lihat Memahami status hypervisor.
- Untuk mencadangkan database Amazon RDS, Amazon Aurora, atau Amazon DocumentDB cluster, sumber daya tersebut harus memiliki status. `AVAILABLE`
- Untuk mencadangkan Amazon Elastic File System (Amazon EFS), itu harus memiliki status`AVAILABLE`.
- Untuk mencadangkan sistem file Amazon FSx, itu harus memiliki status. `AVAILABLE` Jika statusnya`UPDATING`, permintaan cadangan diantrian sampai sistem file menjadi. `AVAILABLE`

  FSx untuk ONTAP tidak mendukung pencadangan jenis volume tertentu, termasuk volume DP (perlindungan data), volume LS (berbagi beban), volume penuh, atau volume pada sistem file yang penuh. Untuk informasi lebih lanjut, silakan lihat FSx untuk ONTAP Bekerja dengan cadangan.

AWS Backup mempertahankan cadangan yang dibuat sebelumnya sesuai dengan kebijakan siklus hidup Anda, terlepas dari kesehatan sumber daya sumber Anda.

Topik

Membuat cadangan sesuai permintaan menggunakan AWS Backup

Di AWS Backup konsol, halaman Sumber daya yang dilindungi mencantumkan sumber daya yang telah dicadangkan AWS Backup setidaknya sekali. Jika Anda menggunakan AWS Backup untuk pertama kalinya, tidak ada sumber daya apa pun (seperti volume Amazon EBS atau database Amazon RDS) yang tercantum di halaman ini. Ini benar bahkan jika sumber daya ditugaskan ke rencana cadangan dan rencana cadangan itu belum menjalankan pekerjaan pencadangan terjadwal setidaknya sekali.

Catatan: Pencadangan sesuai permintaan mulai membuat cadangan sumber daya Anda segera. Anda dapat memilih cadangan sesuai permintaan jika Anda ingin membuat cadangan pada waktu selain waktu yang dijadwalkan yang ditentukan dalam rencana cadangan. Cadangan sesuai permintaan dapat digunakan, misalnya, untuk menguji cadangan dan fungsionalitas kapan saja.

Pencadangan sesuai permintaan tidak dapat digunakan dengan point-in-time pemulihan (PITR) karena cadangan sesuai permintaan mempertahankan sumber daya dalam keadaan saat pencadangan diambil, sedangkan PITR menggunakan cadangan berkelanjutan yang mencatat perubahan selama periode waktu tertentu.

Pertimbangan

- Jika peran AWS Backup default tidak ada di akun Anda, peran tersebut dibuat untuk Anda dengan izin yang benar.
- Saat pencadangan kedaluwarsa dan ditandai untuk dihapus sebagai bagian dari kebijakan siklus hidup Anda, AWS Backup hapus cadangan pada titik yang dipilih secara acak selama 8 jam berikutnya. Jendela ini membantu memastikan kinerja yang konsisten.
- Untuk sumber daya Amazon EC2, AWS Backup secara otomatis menyalin tag sumber daya grup dan individu yang ada, selain tag apa pun yang Anda tambahkan di langkah ini.
- AWS Backup mengambil cadangan EC2 dengan “no reboot” sebagai perilaku default. AWS Backup saat ini mendukung sumber daya yang berjalan di Amazon EC2, dan jenis instans tertentu tidak didukung. Untuk informasi selengkapnya, lihat Membuat cadangan Windows VSS.

Untuk membuat cadangan sesuai permintaan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di dasbor, pilih Buat cadangan sesuai permintaan. Atau, di panel navigasi, pilih Sumber daya yang dilindungi lalu pilih Buat cadangan sesuai permintaan.
3. Untuk halaman Jenis sumber daya, pilih jenis sumber daya yang ingin Anda cadangkan. Misalnya, pilih DynamoDB untuk tabel Amazon DynamoDB.
4. Pilih nama atau ID sumber daya yang akan dilindungi. Misalnya, pilih nama tabel DynamoDB untuk Amazon DynamoDB.
5. Pastikan bahwa Buat cadangan sekarang dipilih.
6. Jika jenis sumber daya mendukung transisi ke penyimpanan dingin, penyimpanan dingin hadir. Untuk informasi selengkapnya, lihat kolom Siklus Hidup ke penyimpanan dingin dalam tabel Ketersediaan fitur menurut sumber daya.

   Untuk menentukan kapan cadangan ini masuk ke penyimpanan dingin, pilih Pindahkan cadangan dari penyimpanan hangat ke penyimpanan dingin lalu tentukan waktu dalam penyimpanan hangat.
7. Untuk Periode retensi total, tentukan jumlah hari. Jika Anda menentukan waktu dalam penyimpanan dingin, periode retensi dibagi antara penyimpanan hangat dan dingin.
8. Pilih brankas Cadangan yang ada atau buat yang baru. Memilih Create new Backup vault membuka halaman baru untuk membuat vault dan kemudian mengembalikan Anda ke halaman Buat cadangan sesuai permintaan setelah Anda selesai.

9. Untuk peran IAM, pilih peran default atau peran yang Anda buat.
10. Untuk menetapkan tag ke cadangan sesuai permintaan Anda, perluas Tag yang ditambahkan ke titik pemulihan, pilih Tambahkan tag baru, dan masukkan kunci tag dan nilai tag.
11. Jika jenis sumber daya adalah EC2, pengaturan cadangan lanjutan hadir. Untuk mengambil snapshot yang konsisten dengan aplikasi menggunakan Windows Volume Shadow Copy Service (VSS), pilih Windows VSS.
12. Pilih Buat cadangan sesuai permintaan. Ini membuka halaman Pekerjaan, di mana Anda dapat melihat daftar pekerjaan dan melihat status pekerjaan.

Pencadangan dan point-in-time pemulihan berkelanjutan (PITR)

Topik

Untuk beberapa sumber daya, AWS Backup mendukung pencadangan dan point-in-time pemulihan berkelanjutan (PITR) selain cadangan snapshot.

Dengan pencadangan berkelanjutan, Anda dapat memulihkan sumber daya yang AWS Backup didukung dengan memutarnya kembali ke waktu tertentu yang Anda pilih, dalam waktu 1 detik presisi (kembali maksimal 35 hari). Pencadangan berkelanjutan bekerja dengan terlebih dahulu membuat cadangan penuh sumber daya Anda, dan kemudian terus-menerus mencadangkan log transaksi sumber daya Anda. PITR restore bekerja dengan mengakses cadangan penuh Anda dan memutar ulang log transaksi ke waktu yang Anda minta AWS Backup untuk memulihkan.

Atau, cadangan snapshot dapat diambil sesering setiap jam. Cadangan snapshot dapat disimpan hingga maksimal 100 tahun. Snapshot dapat dengan disalin untuk cadangan penuh atau tambahan.

Karena pencadangan berkelanjutan dan snapshot menawarkan keuntungan yang berbeda, kami menyarankan Anda melindungi sumber daya Anda dengan aturan pencadangan berkelanjutan dan snapshot.

Catatan: Pencadangan sesuai permintaan mulai membuat cadangan sumber daya Anda segera. Anda dapat memilih cadangan sesuai permintaan jika Anda ingin membuat cadangan pada waktu selain waktu yang dijadwalkan yang ditentukan dalam rencana cadangan. Cadangan sesuai permintaan dapat digunakan, misalnya, untuk menguji cadangan dan fungsionalitas kapan saja.

Pencadangan sesuai permintaan tidak dapat digunakan dengan point-in-time pemulihan (PITR) karena cadangan sesuai permintaan mempertahankan sumber daya dalam keadaan saat pencadangan diambil, sedangkan PITR menggunakan cadangan berkelanjutan yang mencatat perubahan selama periode waktu tertentu.

Anda dapat ikut serta dalam pencadangan berkelanjutan untuk sumber daya yang didukung saat membuat paket cadangan AWS Backup menggunakan AWS Backup konsol atau API.

Untuk mengaktifkan pencadangan berkelanjutan menggunakan konsol

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Backup plan, lalu pilih Buat paket Backup.
3. Di bawah Aturan Backup, pilih Aturan Tambahkan Cadangan.
4. Di bagian Konfigurasi aturan Backup, pilih Aktifkan pencadangan berkelanjutan untuk sumber daya yang didukung.

Layanan yang didukung untuk pencadangan berkelanjutan/point in time restore (PITR)

AWS Backup mendukung pencadangan dan point-in-time pemulihan berkelanjutan untuk layanan dan aplikasi berikut:

Amazon S3

Untuk mengaktifkan PITR untuk cadangan S3, pencadangan berkelanjutan perlu menjadi bagian dari rencana pencadangan.

Meskipun cadangan asli dari bucket sumber ini dapat mengaktifkan PITR, salinan tujuan lintas wilayah atau lintas akun tidak akan memiliki PITR, dan memulihkan dari salinan ini akan dikembalikan

ke waktu pembuatannya (salinannya akan berupa salinan snapshot) alih-alih memulihkan ke titik waktu tertentu.

RDS

Jadwal Backup: Ketika sebuah AWS Backup rencana membuat snapshot Amazon RDS dan backup berkelanjutan, AWS Backup akan dengan cerdas menjadwalkan jendela cadangan Anda untuk berkoordinasi dengan jendela pemeliharaan Amazon RDS untuk mencegah konflik. Untuk mencegah konflik lebih lanjut, konfigurasi manual jendela pencadangan otomatis Amazon RDS tidak tersedia. RDS mengambil snapshot sekali sehari terlepas dari apakah rencana cadangan memiliki frekuensi untuk cadangan snapshot selain sekali per hari.

Pengaturan: Setelah menerapkan aturan pencadangan AWS Backup berkelanjutan ke instans Amazon RDS, Anda tidak dapat membuat atau mengubah pengaturan pencadangan berkelanjutan ke instance tersebut di Amazon RDS; modifikasi harus dilakukan melalui AWS Backup konsol atau CLI AWS Backup .

Kontrol transisi pencadangan berkelanjutan untuk instans Amazon RDS kembali ke Amazon RDS:

Console

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Rencana cadangan.
3. Hapus semua paket cadangan Amazon RDS dengan pencadangan berkelanjutan yang melindungi sumber daya tersebut.
4. Pilih Brankas Cadangan. Hapus titik pemulihan cadangan berkelanjutan dari brankas cadangan Anda. Atau, tunggu sampai periode retensi mereka berlalu, AWS Backup menyebabkan secara otomatis menghapus titik pemulihan.

   Setelah Anda menyelesaikan langkah-langkah ini, AWS Backup akan transisi kontrol cadangan berkelanjutan sumber daya Anda kembali ke Amazon RDS.

AWS CLI

Panggil operasi `DisassociateRecoveryPoint` API.

Untuk mempelajari selengkapnya, lihat DisassociateRecoveryPoint.

Izin IAM diperlukan untuk pencadangan berkelanjutan Amazon RDS

- Untuk digunakan AWS Backup untuk mengonfigurasi pencadangan berkelanjutan untuk database Amazon RDS Anda, verifikasi bahwa izin API `rds:ModifyDBInstance` ada dalam peran IAM yang ditentukan oleh konfigurasi paket cadangan Anda. Untuk memulihkan backup berkelanjutan Amazon RDS, Anda harus menambahkan izin `rds:RestoreDBInstanceToPointInTime` ke peran IAM yang Anda kirimkan untuk pekerjaan pemulihan. Anda dapat menggunakan `AWS Backup default service role` untuk melakukan backup dan mengembalikan.
- Untuk menggambarkan rentang waktu yang tersedia untuk point-in-time pemulihan, AWS Backup panggilan`rds:DescribeDBInstanceAutomatedBackupsAPI`. Di AWS Backup konsol, Anda harus memiliki izin `rds:DescribeDBInstanceAutomatedBackups` API dalam kebijakan terkelola AWS Identity and Access Management (IAM) Anda. Anda dapat menggunakan `AWSBackupFullAccess` atau kebijakan yang `AWSBackupOperatorAccess` dikelola. Kedua kebijakan memiliki semua izin yang diperlukan. Untuk informasi selengkapnya, lihat Kebijakan Terkelola.

Periode retensi: Ketika Anda mengubah periode retensi PITR Anda, AWS Backup panggilan `ModifyDBInstance` dan menerapkan perubahan itu segera. Jika Anda memiliki pembaruan konfigurasi lain yang menunggu jendela pemeliharaan berikutnya, mengubah periode retensi PITR Anda juga akan segera menerapkan pembaruan konfigurasi tersebut. Untuk informasi selengkapnya, lihat `ModifyDBInstance`di Referensi API Amazon Relational Database Service.

Salinan cadangan berkelanjutan Amazon RDS:

- Proses pekerjaan penyalinan snapshot tambahan lebih cepat daripada pekerjaan penyalinan snapshot penuh. Menyimpan salinan snapshot sebelumnya hingga pekerjaan penyalinan baru selesai dapat mengurangi durasi pekerjaan penyalinan. Jika Anda memilih untuk menyalin snapshot dari instance database RDS, penting untuk dicatat bahwa menghapus salinan sebelumnya terlebih dahulu akan menyebabkan salinan snapshot penuh dibuat (bukan inkremental). Untuk informasi selengkapnya tentang mengoptimalkan penyalinan, lihat Penyalinan snapshot tambahan di Panduan Pengguna Amazon RDS
- Membuat salinan cadangan berkelanjutan Amazon RDS - Anda tidak dapat membuat salinan cadangan berkelanjutan Amazon RDS karena AWS Backup untuk Amazon RDS tidak mengizinkan menyalin log transaksi. Sebagai gantinya, AWS Backup buat snapshot dan salin dengan frekuensi yang ditentukan dalam paket cadangan.

Memulihkan: Anda dapat melakukan point-in-time pemulihan menggunakan salah satu AWS Backup atau Amazon RDS. Untuk petunjuk AWS Backup konsol, lihat Memulihkan Database Amazon RDS. Untuk petunjuk Amazon RDS, lihat Memulihkan Instans DB ke waktu yang ditentukan dalam Panduan Pengguna Amazon RDS.

> **Tip**
>
> Instans database multi AZ (zona ketersediaan) yang disetel ke `Always On` seharusnya tidak memiliki retensi cadangan yang disetel ke nol. Jika terjadi kesalahan, gunakan AWS CLI perintah `disassociate-recovery-point` alih-alih`delete-recovery-point`, lalu ubah pengaturan retensi ke 1 di pengaturan Amazon RDS Anda.

Untuk informasi umum tentang bekerja dengan Amazon RDS, lihat Panduan Pengguna Amazon RDS.

Aurora

Untuk mengaktifkan pencadangan berkelanjutan sumber daya Aurora Anda, lihat langkah-langkah di bagian pertama halaman ini.

Prosedur untuk mengembalikan cluster Aurora ke titik waktu adalah variasi dari langkah-langkah untuk memulihkan snapshot dari cluster aurora.

Saat Anda melakukan pemulihan titik waktu, konsol menampilkan bagian waktu pemulihan. Lihat Memulihkan cadangan berkelanjutan lebih jauh di halaman ini di Bekerja dengan pencadangan Berkelanjutan.

SAP HANA pada instans Amazon EC2

Anda dapat membuat backup berkelanjutan, yang dapat digunakan dengan point-in-time restore (PITR) (perhatikan bahwa on-demand backup menyimpan sumber daya dalam keadaan di mana mereka diambil; sedangkan PITR menggunakan backup berkelanjutan yang mencatat perubahan selama periode waktu tertentu).

Dengan pencadangan berkelanjutan, Anda dapat memulihkan database SAP HANA Anda pada instans EC2 dengan memutarnya kembali ke waktu tertentu yang Anda pilih, dalam waktu 1 detik presisi (kembali maksimal 35 hari). Pencadangan berkelanjutan bekerja dengan terlebih dahulu membuat cadangan penuh sumber daya Anda, dan kemudian terus-menerus mencadangkan log

transaksi sumber daya Anda. PITR restore bekerja dengan mengakses cadangan penuh Anda dan memutar ulang log transaksi ke waktu yang Anda minta AWS Backup untuk memulihkan.

Anda dapat ikut serta dalam pencadangan berkelanjutan saat membuat paket cadangan AWS Backup menggunakan AWS Backup konsol atau API.

Untuk mengaktifkan pencadangan berkelanjutan menggunakan konsol

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Backup plan, lalu pilih Buat paket Backup.
3. Di bawah Aturan Backup, pilih Aturan Tambahkan Cadangan.
4. Di bagian Konfigurasi aturan Backup, pilih Aktifkan pencadangan berkelanjutan untuk sumber daya yang didukung.

Setelah Anda menonaktifkan PITR (point-in-timerestore) untuk backup database SAP HANA, log akan terus dikirim AWS Backup sampai titik pemulihan berakhir (status sama. `EXPIRED`) Anda dapat mengubah ke lokasi cadangan log alternatif di SAP HANA untuk menghentikan transmisi log ke AWS Backup.

Titik pemulihan berkelanjutan dengan status `STOPPED` menunjukkan bahwa titik pemulihan berkelanjutan telah terputus; yaitu, log yang ditransmisikan dari SAP HANA ke AWS Backup yang menunjukkan perubahan tambahan ke database memiliki celah. Titik pemulihan yang terjadi dalam jeda jangka waktu ini memiliki status. `STOPPED`.

Untuk masalah yang mungkin Anda temui selama memulihkan pekerjaan pencadangan berkelanjutan (titik pemulihan), lihat bagian pemecahan masalah SAP HANA Restore dari panduan ini.

Menemukan cadangan berkelanjutan

Anda dapat menggunakan AWS Backup konsol untuk menemukan cadangan berkelanjutan Anda.

Untuk menemukan cadangan berkelanjutan menggunakan AWS Backup konsol

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Backup vaults, lalu pilih brankas cadangan Anda dalam daftar.
3. Di bagian Backup, di kolom Jenis Backup, urutkan untuk titik pemulihan berkelanjutan. Anda juga dapat mengurutkan berdasarkan ID titik Pemulihan untuk awalan kontinu.

Memulihkan cadangan berkelanjutan

Untuk memulihkan cadangan berkelanjutan menggunakan AWS Backup konsol

- Selama proses pemulihan PITR, AWS Backup konsol menampilkan bagian Waktu pemulihan. Di bagian ini, lakukan salah satu hal berikut:
  - Pilih untuk mengembalikan ke waktu restorable terbaru.
  - Pilih Tentukan tanggal dan waktu untuk memasukkan tanggal dan waktu Anda sendiri dalam periode retensi Anda.

Untuk memulihkan cadangan berkelanjutan menggunakan AWS Backup API

1. Untuk Amazon S3, lihat Menggunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan S3.
2. Untuk Amazon RDS lihat Menggunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Amazon RDS.

Menghentikan atau menghapus cadangan berkelanjutan

Anda dapat menghentikan pembuatan cadangan berkelanjutan atau Anda dapat menghapus cadangan tertentu (atau poin PITR)point-in-time-recovery .

Jika Anda ingin menghentikan pencadangan berkelanjutan, Anda harus menghapus aturan pencadangan berkelanjutan dari rencana pencadangan Anda. Jika Anda ingin menghentikan pencadangan berkelanjutan untuk satu atau lebih sumber daya tetapi tidak untuk semua sumber daya, buat rencana cadangan baru dengan aturan pencadangan berkelanjutan untuk sumber daya yang masih ingin Anda dukung terus menerus. Jika Anda hanya menghapus titik pemulihan cadangan berkelanjutan dari brankas cadangan, paket cadangan Anda akan tetap menjalankan aturan pencadangan berkelanjutan, membuat titik pemulihan baru.

Namun, bahkan setelah Anda menghapus aturan pencadangan berkelanjutan, AWS Backup mengingat periode retensi dari aturan pencadangan yang sekarang dihapus. Ini akan secara otomatis menghapus titik pemulihan cadangan berkelanjutan Anda dari brankas cadangan Anda berdasarkan periode retensi yang Anda tentukan.

Saat menghapus poin pemulihan Amazon RDS, pertimbangkan:

- Instans database multi AZ (zona ketersediaan) yang disetel ke `Always On` seharusnya tidak memiliki retensi cadangan yang disetel ke nol. Jika terjadi kesalahan, gunakan AWS CLI perintah `disassociate-recovery-point` alih-alih`delete-recovery-point`, lalu ubah pengaturan retensi ke 1 di pengaturan Amazon RDS Anda.
- Ketika titik point-in-time pemulihan (cadangan yang dibuat oleh pencadangan berkelanjutan) untuk Amazon RDS dihapus, reboot database dipicu dan log biner dinonaktifkan. Untuk detail lebih lanjut, lihat Periode retensi cadangan di Panduan Pengguna Amazon RDS.

Saat menghapus poin pemulihan Aurora, pertimbangkan:

Jika ini dipilih untuk titik pemulihan Amazon Aurora, AWS Backup atur periode retensi menjadi 1 hari. Cadangan Aurora tidak dapat sepenuhnya dihapus sampai cluster sumber juga telah dihapus.

Menyalin cadangan berkelanjutan

Jika aturan pencadangan berkelanjutan juga menentukan salinan lintas akun atau lintas wilayah, AWS Backup ambil snapshot pencadangan berkelanjutan dan salinan snapshot tersebut ke brankas tujuan. Untuk mempelajari lebih lanjut tentang menyalin titik pemulihan Anda di seluruh akun dan Wilayah, lihat Menyalin cadangan.

Pencadangan berkelanjutan membuat cadangan berkala sesuai dengan frekuensi yang ditetapkan dalam aturan rencana cadangan di akun tujuan dan/atau Wilayah.

AWS Backup tidak mendukung salinan cadangan berkelanjutan sesuai permintaan.

Mengubah periode retensi Anda

Anda dapat menggunakan AWS Backup untuk menambah atau mengurangi periode retensi untuk aturan pencadangan berkelanjutan yang ada. Periode retensi minimum adalah 1 hari. Periode retensi maksimum adalah 35 hari.

Jika Anda meningkatkan periode retensi Anda, efeknya langsung. Jika Anda mengurangi periode retensi Anda, AWS Backup akan menunggu sampai cukup waktu berlalu sebelum menerapkan perubahan untuk melindungi terhadap kehilangan data. Misalnya, jika Anda mengurangi periode retensi Anda dari 35 hari menjadi 20, AWS Backup akan terus mempertahankan 35 hari pencadangan terus menerus hingga 15 hari telah berlalu. Desain ini melindungi 15 hari terakhir pencadangan Anda pada saat Anda melakukan perubahan.

Menghapus satu-satunya aturan pencadangan berkelanjutan dari rencana cadangan

Saat Anda membuat rencana cadangan dengan aturan pencadangan berkelanjutan dan kemudian Anda menghapus aturan itu, AWS Backup mengingat periode retensi dari aturan yang sekarang dihapus. Ini akan menghapus cadangan berkelanjutan dari brankas cadangan Anda ketika periode retensi berlalu.

Pencadangan berkelanjutan yang tumpang tindih pada sumber daya yang sama

Secara umum, Anda harus melindungi setiap sumber daya dengan tidak lebih dari satu aturan pencadangan berkelanjutan. Ini karena cadangan berkelanjutan tambahan berlebihan. Namun, saat Anda meningkatkan cadangan estat Anda, dimungkinkan untuk beberapa rencana cadangan, aturan, dan brankas untuk tumpang tindih pada satu sumber daya. AWS Backup menangani tumpang tindih ini sebagai berikut.

Jika Anda menyertakan sumber daya yang sama di lebih dari satu paket cadangan dengan aturan pencadangan berkelanjutan, hanya AWS Backup akan membuat cadangan berkelanjutan untuk rencana cadangan pertama yang dievaluasi. Ini akan membuat cadangan snapshot untuk semua rencana cadangan lainnya.

Jika Anda menyertakan beberapa aturan pencadangan berkelanjutan dalam satu paket cadangan:

- Jika aturan Anda mengarah ke brankas cadangan yang sama, AWS Backup hanya membuat cadangan berkelanjutan untuk aturan dengan periode retensi terlama. Ini mengabaikan semua aturan lainnya.
- Jika aturan Anda mengarah ke brankas cadangan yang berbeda, AWS Backup tolak paket sebagai tidak valid.

Pertimbangan oint-in-time pemulihan P

Waspadai pertimbangan berikut untuk point-in-time pemulihan:

- Fallback otomatis ke snapshot - Jika AWS Backup tidak dapat melakukan pencadangan berkelanjutan, ia mencoba melakukan cadangan snapshot sebagai gantinya.
- Tidak ada dukungan untuk pencadangan berkelanjutan sesuai permintaan - AWS Backup tidak mendukung pencadangan berkelanjutan sesuai permintaan karena cadangan berdasarkan permintaan mencatat titik waktu, sedangkan catatan pencadangan berkelanjutan berubah selama periode waktu tertentu.

- Tidak ada dukungan untuk transisi ke penyimpanan dingin - Pencadangan berkelanjutan tidak mendukung transisi ke penyimpanan dingin karena transisi ke dingin memerlukan periode transisi minimum 90 hari, sedangkan pencadangan berkelanjutan memiliki periode retensi maksimum 35 hari.
- Memulihkan aktivitas terbaru - Aktivitas Amazon RDS memungkinkan pemulihan hingga aktivitas 5 menit terakhir; Amazon S3 memungkinkan pemulihan hingga aktivitas 15 menit terakhir.

Cadangan Amazon S3

AWS Backup mendukung pencadangan terpusat dan pemulihan aplikasi yang menyimpan data di S3 sendiri atau bersama AWS layanan lain untuk database, penyimpanan, dan komputasi. Banyak fitur yang tersedia untuk backup S3, termasuk Backup Audit Manager.

Anda dapat menggunakan kebijakan pencadangan tunggal AWS Backup untuk mengotomatiskan pembuatan cadangan data aplikasi Anda secara terpusat. AWS Backup Secara otomatis mengatur cadangan di berbagai AWS layanan dan aplikasi pihak ketiga di satu lokasi terpusat dan terenkripsi (dikenal sebagai brankas cadangan) sehingga Anda dapat mengelola cadangan seluruh aplikasi Anda melalui pengalaman terpusat. Untuk S3, Anda dapat membuat cadangan berkelanjutan dan mengembalikan data aplikasi Anda yang disimpan di S3 dan mengembalikan cadangan ke a dengan satu klik. point-in-time

Dengan AWS Backup, Anda dapat membuat jenis cadangan bucket S3 berikut, termasuk data objek, tag, Daftar Kontrol Akses (ACL), dan metadata yang ditentukan pengguna:

- Pencadangan berkelanjutan memungkinkan Anda mengembalikan ke titik waktu mana pun dalam 35 hari terakhir. Pencadangan berkelanjutan untuk bucket S3 hanya boleh dikonfigurasi dalam satu paket cadangan.

  Lihat Point-in-Time Recovery untuk daftar layanan yang didukung dan petunjuk tentang cara menggunakan AWS Backup untuk melakukan backup berkelanjutan.
- Pencadangan berkala menggunakan snapshot data Anda untuk memungkinkan Anda menyimpan data selama durasi yang ditentukan hingga 99 tahun. Anda dapat menjadwalkan backup periodik dalam frekuensi seperti 1 jam, 12 jam, 1 hari, 1 minggu, atau 1 bulan. AWS Backup mengambil cadangan berkala selama jendela cadangan yang Anda tentukan dalam rencana cadangan Anda.

  Lihat Membuat paket cadangan untuk memahami cara AWS Backup menerapkan rencana cadangan ke sumber daya Anda.

Salinan lintas akun dan lintas wilayah tersedia untuk cadangan S3, tetapi salinan cadangan berkelanjutan tidak memiliki kemampuan pemulihan. point-in-time

Pencadangan bucket S3 yang berkelanjutan dan berkala harus berada di brankas cadangan yang sama.

Untuk kedua jenis cadangan, cadangan pertama adalah cadangan penuh, sedangkan cadangan berikutnya bersifat inkremental pada tingkat objek.

> **Note**
>
> Anda harus mengaktifkan S3 Versioning pada bucket S3 Anda untuk digunakan untuk Amazon AWS Backup S3. Kami telah menyimpan prasyarat ini karena AWS kami merekomendasikan versi S3 sebagai praktik terbaik untuk perlindungan data.
> Kami menyarankan Anda menetapkan periode kedaluwarsa siklus hidup untuk versi S3 Anda. Tidak menyiapkan periode kedaluwarsa siklus hidup dapat meningkatkan biaya S3 Anda karena AWS Backup mencadangkan dan menyimpan semua versi data S3 Anda yang belum kedaluwarsa. Untuk mempelajari selengkapnya tentang menyiapkan kebijakan siklus hidup S3, ikuti petunjuk di halaman ini.

Bandingkan jenis cadangan S3

Strategi pencadangan Anda untuk sumber daya S3 hanya dapat melibatkan pencadangan berkelanjutan, hanya cadangan berkala (snapshot), atau kombinasi keduanya. Informasi di bawah ini dapat membantu Anda memilih yang terbaik untuk organisasi Anda:

Hanya backup berkelanjutan:

- Setelah pencadangan penuh pertama dari data Anda yang ada selesai, perubahan dalam data bucket S3 Anda dilacak saat terjadi.
- Perubahan yang dilacak memungkinkan Anda menggunakan PITR (point-in-time restore) untuk periode retensi pencadangan berkelanjutan. Untuk melakukan pekerjaan pemulihan, Anda memilih titik waktu yang ingin Anda pulihkan.
- Periode retensi setiap cadangan berkelanjutan memiliki maksimum 35 hari.

Pencadangan berkala (snapshot) saja, terjadwal atau sesuai permintaan:

- AWS Backup memindai seluruh bucket S3, mengambil ACL dan tag setiap objek, dan memulai permintaan Head untuk setiap objek yang ada di snapshot sebelumnya tetapi tidak ditemukan dalam snapshot yang sedang dibuat.
- Backup point-in-time konsisten.
- Tanggal dan waktu pencadangan yang direkam adalah waktu di mana AWS Backup menyelesaikan traversal bucket, bukan pada saat pekerjaan cadangan dibuat.
- Cadangan pertama ember adalah cadangan penuh. Setiap cadangan berikutnya bersifat inkremental, mewakili perubahan data sejak snapshot terakhir.
- Cuplikan yang dibuat oleh cadangan berkala dapat memiliki periode retensi hingga 99 tahun.

Pencadangan berkelanjutan dikombinasikan dengan cadangan periodik/snapshot:

- Setelah pencadangan penuh pertama dari data Anda yang ada (setiap bucket) selesai, perubahan dalam bucket Anda akan dilacak saat terjadi.
- Anda dapat melakukan point-in-time pemulihan dari titik pemulihan berkelanjutan.
- Snapshot point-in-time konsisten.
- Snapshot diambil langsung dari titik pemulihan berkelanjutan, menghilangkan kebutuhan untuk memindai ulang bucket untuk memungkinkan proses yang lebih cepat.
- Snapshot dan titik pemulihan berkelanjutan berbagi garis keturunan data; penyimpanan data antara snapshot dan titik pemulihan berkelanjutan tidak diduplikasi.

Kelas Penyimpanan S3 yang Didukung

AWS Backup memungkinkan Anda untuk mencadangkan data S3 yang disimpan di Kelas Penyimpanan S3 berikut:

- S3 Standard
- Standar S3 - Akses Jarang (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- Tingkat Cerdas S3 (S3 INT)

Cadangan objek di kelas penyimpanan S3 Intelligent-Tiering (INT) mengakses objek tersebut. Akses ini memicu S3 Intelligent-Tiering untuk secara otomatis memindahkan objek tersebut ke Frequent Access.

Cadangan yang mengakses tingkatan Akses Jarang, termasuk kelas Standar S3 - Akses Jarang (IA) dan S3 One Zone-IA, bergerak di bawah biaya penyimpanan S3 dari Akses Sering (berlaku untuk tingkat Akses Jarang atau Arsip Akses Instan).

Dengan pengecualian Glacier Instant Retrieval, kelas penyimpanan yang diarsipkan tidak didukung.

Untuk informasi selengkapnya tentang harga penyimpanan untuk Amazon S3, lihat Harga Amazon S3.

Pertimbangan AWS Backup untuk Amazon S3

Poin-poin berikut harus dipertimbangkan ketika Anda mencadangkan sumber daya S3:

- Dukungan metadata objek terfokus: AWS Backup mendukung metadata berikut: tag, daftar kontrol akses (ACL), metadata yang ditentukan pengguna, tanggal pembuatan asli, dan ID versi. Anda juga dapat memulihkan semua data dan metadata yang dicadangkan kecuali tanggal pembuatan asli, ID versi, kelas penyimpanan, dan e-tag.
- Nama kunci objek S3 dapat terdiri dari sebagian besar string UTF-8 yang dapat dikodekan. Karakter Unicode berikut diperbolehkan: `#x9` | `#xA` | `#xD` | `#x20 to #xD7FF` `#xE000 to #xFFFD` |`#x10000 to #x10FFFF`.

  Nama kunci objek yang menyertakan karakter yang tidak ada dalam daftar ini dapat dikecualikan dari cadangan. Untuk informasi lebih lanjut, lihat spesifikasi W3C untuk karakter.
- Kebijakan manajemen siklus hidup transisi penyimpanan dingin memungkinkan Anda menentukan timeline untuk kedaluwarsa cadangan, tetapi transisi penyimpanan dingin cadangan S3 saat ini tidak didukung saat ini. AWS Backup
- Cadangan bucket S3 dengan banyak versi objek yang sama yang dibuat pada detik yang sama saat ini tidak didukung saat ini.
- Untuk pencadangan berkala, AWS Backup lakukan upaya terbaik untuk melacak semua perubahan pada metadata objek Anda. Namun, jika Anda memperbarui tag atau ACL beberapa kali dalam 1 menit, AWS Backup mungkin tidak menangkap semua status perantara.
- AWS Backup saat ini tidak menawarkan dukungan untuk cadangan objek terenkripsi SSE-C. AWS Backup juga saat ini tidak mendukung cadangan konfigurasi bucket, termasuk kebijakan bucket, pengaturan, nama, atau titik akses.

- AWS Backup saat ini tidak mendukung cadangan S3 aktif. AWS Outposts

> **Important**
>
> Di akun yang mencatat peristiwa pembacaan data, bucket S3 dengan CloudTrail log yang diaktifkan memerlukan log aksesnya disimpan ke bucket target yang berbeda; jika CloudTrail log disimpan dalam bucket yang sama dengan log, loop tak terbatas akan terbentuk. Loop ini dapat memicu muatan yang tidak terduga dan tidak diinginkan.
> Untuk informasi selengkapnya, lihat Peristiwa data di Panduan CloudTrail Pengguna.

Jendela penyelesaian cadangan S3

Tabel di bawah ini menunjukkan contoh bucket dengan berbagai ukuran untuk membantu Anda memandu perkiraan waktu penyelesaian pencadangan penuh awal bucket S3. Waktu pencadangan akan bervariasi sesuai dengan ukuran, konten, konfigurasi, dan pengaturan setiap bucket.

Ukuran bucket	Jumlah objek	Perkiraan waktu untuk menyelesaikan pencadangan awal
425 GB (gigabyte)	135 juta	31 jam
800 TB (terabyte)	670 juta	38 jam
6 PB (petabyte)	5 miliar	100 jam
370 TB (terabyte)	7,5 miliar	180 jam

Izin dan kebijakan untuk pencadangan dan pemulihan Amazon S3

Untuk membuat cadangan, menyalin, dan memulihkan sumber daya S3, Anda harus memiliki kebijakan yang benar dalam peran Anda. Untuk menambahkan kebijakan ini, buka kebijakan AWS terkelola. Tambahkan AWSBackupServiceRolePolicyForS3Backupdan AWSBackupServiceRolePolicyForS3Restoreke peran yang ingin Anda gunakan untuk mencadangkan dan memulihkan bucket S3.

Jika Anda tidak memiliki izin yang memadai, mohon minta manajer akun administratif (admin) organisasi Anda untuk menambahkan kebijakan ke peran yang dimaksud.

Untuk informasi selengkapnya, lihat Kebijakan terkelola dan kebijakan sebaris di Panduan Pengguna IAM.

AWS Backup untuk S3 bergantung pada penerimaan acara S3 melalui Amazon. EventBridge Jika pengaturan ini dinonaktifkan di pengaturan notifikasi bucket S3, pencadangan berkelanjutan akan berhenti untuk bucket tersebut dengan pengaturan dimatikan. Untuk informasi selengkapnya, lihat Menggunakan EventBridge.

Praktik terbaik dan pertimbangan biaya untuk cadangan S3

Praktik terbaik

Untuk ember dengan lebih dari 300 juta objek:

- Untuk ember dengan lebih dari 300 juta objek, tingkat cadangan dapat mencapai hingga 17.000 objek per detik selama pencadangan penuh awal bucket (pencadangan tambahan akan memiliki kecepatan yang berbeda); ember yang berisi kurang dari 300 juta objek cadangan dengan kecepatan mendekati 1.000 objek per detik.
- Cadangan berkelanjutan direkomendasikan.
- Jika siklus hidup pencadangan direncanakan selama lebih dari 35 hari, Anda juga dapat mengaktifkan cadangan snapshot untuk bucket di brankas yang sama tempat pencadangan berkelanjutan Anda disimpan.

Pertimbangan biaya

- Kebijakan siklus hidup S3 memiliki fitur opsional yang disebut Hapus penanda penghapusan objek kedaluwarsa. Ketika fitur ini ditinggalkan, hapus spidol, terkadang dalam jutaan, kedaluwarsa tanpa rencana pembersihan. Saat bucket tanpa fitur ini dicadangkan, dua masalah memengaruhi waktu dan biaya:
  - Hapus penanda dicadangkan, seperti objek. Waktu pencadangan dan waktu pemulihan dapat dipengaruhi tergantung pada rasio objek untuk menghapus penanda.
  - Setiap objek dan penanda yang dicadangkan memiliki biaya minimum. Setiap penanda hapus dibebankan sama dengan objek 128KiB.

- Untuk akun yang membuat backup setidaknya setiap hari atau lebih sering, manfaat biaya dapat direalisasikan dengan menggunakan backup berkelanjutan jika data dalam backup memiliki perubahan minimal antara backup.
- Bucket yang lebih besar yang tidak sering berubah dapat memperoleh manfaat dari pencadangan berkelanjutan, karena ini dapat menghasilkan biaya yang lebih rendah ketika pemindaian seluruh bucket bersama dengan beberapa permintaan per objek tidak perlu dilakukan pada objek yang sudah ada sebelumnya (objek yang tidak berubah dari cadangan sebelumnya).
- Bucket yang berisi lebih dari 100 juta objek dan yang memiliki tingkat penghapusan kecil dibandingkan dengan ukuran cadangan keseluruhan mungkin mewujudkan manfaat biaya dengan paket cadangan yang berisi cadangan berkelanjutan dengan periode retensi 2 hari bersama dengan snapshot dari retensi yang lebih lama.
- Waktu pencadangan periodik (snapshot) sejalan dengan dimulainya proses pencadangan saat pemindaian bucket tidak diperlukan. Pemindaian tidak diperlukan dalam ember yang berisi cadangan dan snapshot berkelanjutan karena dalam kasus ini snapshot diambil dari titik pemulihan berkelanjutan.
- Untuk setiap objek dalam satu S3-GIR (Amazon S3 Glacier Instant Retrieval), AWS Backup melakukan beberapa panggilan, yang akan menghasilkan biaya pengambilan saat pencadangan dilakukan.

  Biaya pengambilan serupa berlaku untuk ember dengan objek di kelas penyimpanan IA S3-IA dan S3 One Zone-IA.
- AWS KMS, CloudTrail, dan CloudWatch fitur Amazon yang merupakan bagian dari strategi pencadangan Anda dapat menghasilkan biaya tambahan di luar penyimpanan data bucket S3. Lihat berikut ini untuk informasi tentang menyesuaikan fitur-fitur ini:
  - Mengurangi biaya SSE-KMS dengan kunci Bucket Amazon S3 di Panduan Pengguna Amazon S3.
  - Anda dapat mengurangi CloudTrail biaya dengan mengecualikan AWS KMS peristiwa dan dengan menonaktifkan peristiwa data S3:
    - Kecualikan AWS KMS peristiwa: Di Panduan CloudTrail Pengguna, Membuat jejak di konsol (pemilih acara dasar) memungkinkan opsi untuk mengecualikan AWS KMS peristiwa untuk memfilter peristiwa ini dari jejak Anda (pengaturan default mencakup semua peristiwa KMS):
    - Opsi untuk mencatat atau mengecualikan peristiwa KMS hanya tersedia jika Anda mencatat peristiwa manajemen di jejak Anda. Jika Anda memilih untuk tidak mencatat peristiwa manajemen, peristiwa KMS tidak dicatat, dan Anda tidak dapat mengubah pengaturan pencatatan peristiwa KMS.

- AWS KMS tindakan sepertiEncrypt,Decrypt, dan GenerateDataKey biasanya menghasilkan volume besar (lebih dari 99%) peristiwa. Tindakan ini sekarang dicatat sebagai peristiwa Baca. Volume rendah, tindakan KMS yang relevan seperti**Disable**,**Delete**, dan **ScheduleKey** (yang biasanya menyumbang kurang dari 0,5% dari volume peristiwa KMS) dicatat sebagai peristiwa Tulis.
- Untuk mengecualikan peristiwa bervolume tinggi sepertiEncrypt,Decrypt, danGenerateDataKey, tetapi masih mencatat peristiwa yang relevan sepertiDisable,, dan DeleteScheduleKey, pilih untuk mencatat peristiwa manajemen Tulis, dan kosongkan kotak centang untuk Kecualikan AWS KMS peristiwa.
- Nonaktifkan peristiwa data S3: Secara default, jejak dan penyimpanan data peristiwa tidak mencatat peristiwa data. Nonaktifkan peristiwa data S3 sebelum pencadangan awal Anda untuk mengurangi biaya.

- Untuk mengurangi CloudWatch biaya, Anda dapat menghentikan pengiriman CloudTrail peristiwa ke CloudWatch Log saat memperbarui jejak untuk menonaktifkan pengaturan CloudWatch Log.

Memulihkan cadangan S3

Anda dapat memulihkan data S3 yang Anda backup menggunakan AWS Backup kelas S3 Standard Storage. Anda dapat memulihkan data S3 ke bucket yang sudah ada, termasuk bucket asli. Selama pemulihan, Anda juga dapat membuat bucket S3 baru sebagai target pemulihan. Anda dapat mengembalikan cadangan S3 hanya ke tempat yang sama di Wilayah AWS mana cadangan Anda berada.

Anda dapat memulihkan seluruh bucket S3, atau folder atau objek di dalam bucket. AWS Backup mengembalikan versi saat ini dari objek itu.

Untuk memulihkan data S3 Anda menggunakan AWS Backup, lihatMemulihkan data S3.

Pencadangan mesin virtual

AWS Backup mendukung perlindungan data terpusat dan otomatis untuk mesin virtual VMware (VM) lokal bersama dengan VM di VMware Cloud™ (VMC) dan VMware Cloud™ (VMC) aktif. AWS AWS Outposts Anda dapat membuat cadangan dari mesin virtual lokal dan VMC ke. AWS Backup Kemudian, Anda dapat memulihkan dari AWS Backup ke VM lokal, VM di VMC, atau VMC aktif. AWS Outposts

AWS Backup juga memberi Anda kemampuan manajemen cadangan VM AWS asli yang dikelola sepenuhnya, seperti penemuan VM, penjadwalan cadangan, manajemen retensi, tingkat penyimpanan berbiaya rendah, salinan lintas wilayah dan lintas akun, dukungan untuk Vault Lock dan AWS Backup Audit Manager, enkripsi yang independen dari data sumber, AWS Backup dan kebijakan akses cadangan. Untuk daftar lengkap kemampuan dan detail, lihat Ketersediaan fitur berdasarkan sumber daya tabel.

Anda dapat menggunakan AWS Backup untuk melindungi mesin virtual Anda di VMware Cloud™ aktif. AWS Outposts AWS Backup menyimpan cadangan VM Anda di tempat VMware Cloud™ Anda terhubung. Wilayah AWS AWS Outposts Anda dapat menggunakan AWS Backup untuk melindungi VMware Cloud™ di AWS Backup VM saat Anda menggunakan VMware Cloud™ on AWS Outposts untuk memenuhi latensi rendah dan kebutuhan pemrosesan data lokal untuk data aplikasi Anda. Berdasarkan persyaratan residensi data Anda, Anda dapat memilih AWS Backup untuk menyimpan cadangan data aplikasi Anda di induk yang Wilayah AWS terhubung dengan Anda AWS Outposts .

VM yang didukung

AWS Backup dapat mencadangkan dan mengembalikan mesin virtual yang dikelola oleh vCenter VMware.

Saat ini didukung:

- vSphere 8, 7.0, dan 6.7
- Ukuran disk virtual yang kelipatan 1 KiB
- Datastores NFS, VMFS, dan VSAN di tempat dan di VMC di AWS
- SCSI Hot-Add dan Network Block Device Secure Sockets Layer (NBDSSL) mode transportasi untuk menyalin data dari VM sumber ke VMware lokal AWS
- Mode Hot-Add untuk melindungi VM di VMware Cloud di AWS

Saat ini tidak didukung:

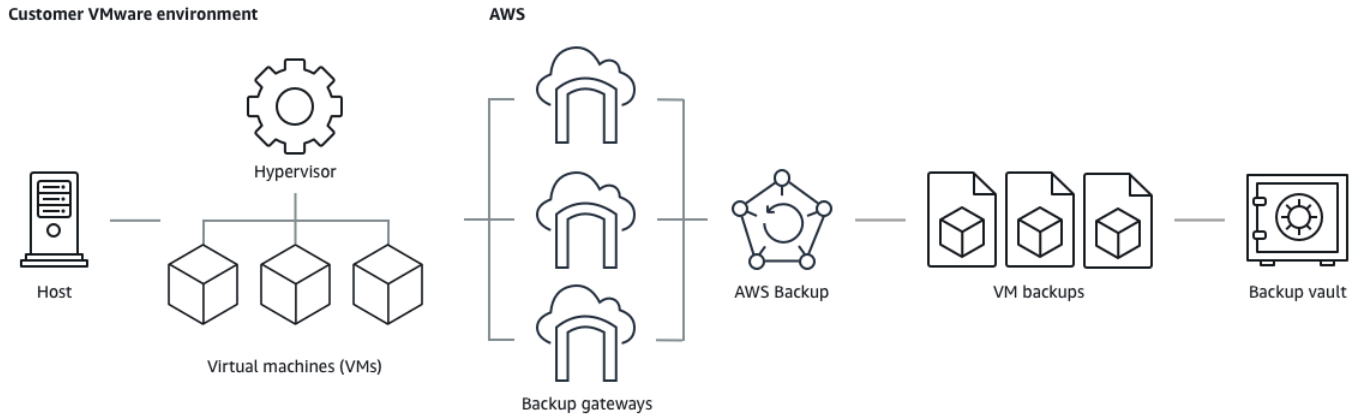
- Disk RDM (pemetaan disk mentah) atau pengontrol NVMe dan disknya
- Mode disk independen-persisten dan independen-non-persisten

Konsistensi Backup

AWS Backup, secara default, menangkap cadangan VM yang konsisten dengan aplikasi menggunakan pengaturan diam VMware Tools pada VM. Cadangan Anda konsisten aplikasi jika aplikasi Anda kompatibel dengan VMware Tools. Jika kemampuan diam tidak tersedia, AWS Backup menangkap backup yang konsisten dengan crash. Validasi bahwa backup Anda memenuhi kebutuhan organisasi Anda dengan menguji pemulihan Anda.

Gateway Backup

Backup gateway adalah AWS Backup perangkat lunak yang dapat diunduh yang Anda gunakan ke infrastruktur VMware Anda untuk menghubungkan VM VMware Anda. AWS Backup Gateway terhubung ke server manajemen VM Anda untuk menemukan VM, menemukan VM Anda, mengenkripsi data, dan mentransfer data secara efisien. AWS Backup Diagram berikut menggambarkan bagaimana Backup gateway terhubung ke VM Anda:



Untuk mengunduh perangkat lunak gateway Backup, ikuti prosedur untukBekerja dengan gateway.

Untuk informasi tentang titik akhir VPC (Virtual Private Cloud), lihat AWS Backup dan konektivitas. AWS PrivateLink

Backup gateway dilengkapi dengan API sendiri yang dikelola secara terpisah dari AWS Backup API. Untuk melihat daftar tindakan API gateway Backup, lihat Tindakan gateway Backup. Untuk melihat daftar tipe data API gateway Backup, lihat Jenis data gateway Backup.

Titik akhir

Pengguna lama yang saat ini menggunakan titik akhir publik dan yang ingin beralih ke titik akhir VPC (Virtual Private Cloud) dapat membuat gateway baru dengan titik akhir VPC AWS

PrivateLinkmenggunakan, mengaitkan hypervisor yang ada ke gateway, dan kemudian menghapus gateway yang berisi titik akhir publik.

Konfigurasikan infrastruktur Anda untuk menggunakan gateway Backup

Backup gateway memerlukan konfigurasi jaringan, firewall, dan perangkat keras berikut untuk mencadangkan dan memulihkan mesin virtual Anda.

Konfigurasi jaringan

Backup gateway membutuhkan port tertentu untuk diizinkan untuk operasinya. Izinkan port berikut:

1. TCP 443 Keluar
   - Sumber: Backup gateway
   - Tujuan: AWS
   - Gunakan: Memungkinkan gateway Backup untuk berkomunikasi dengan AWS.
2. TCP 80 Masuk
   - Sumber: Host yang Anda gunakan untuk terhubung ke AWS Management Console
   - Tujuan: Backup gateway
   - Gunakan: Dengan sistem lokal untuk mendapatkan kunci aktivasi gateway Backup. Port 80 hanya digunakan selama aktivasi gateway Backup. AWS Backup tidak memerlukan port 80 untuk dapat diakses publik. Tingkat akses yang diperlukan ke port 80 tergantung pada konfigurasi jaringan Anda. Jika Anda mengaktifkan gateway Anda dari AWS Management Console, host dari mana Anda terhubung ke konsol harus memiliki akses ke port gateway Anda 80.
3. UDP 53 Keluar
   - Sumber: Backup gateway
   - Tujuan: Server Layanan Nama Domain (DNS)
   - Gunakan: Memungkinkan gateway Backup untuk berkomunikasi dengan DNS.
4. Keluar TCP 22
   - Sumber: Backup gateway
   - Tujuan: AWS Support
   - Gunakan: Memungkinkan AWS Support untuk mengakses gateway Anda untuk membantu Anda dengan masalah. Anda tidak perlu membuka port ini untuk pengoperasian normal gateway Anda, tetapi Anda harus membukanya untuk pemecahan masalah.

5. UDP 123 Keluar
   - Sumber: Klien NTP
   - Tujuan: Server NTP
   - Gunakan: Digunakan oleh sistem lokal untuk menyinkronkan waktu mesin virtual ke waktu host.
6. TCP 443 Keluar
   - Sumber: Backup gateway
   - Tujuan: VMware vCenter
   - Gunakan: Memungkinkan gateway Backup untuk berkomunikasi dengan VMware vCenter.
7. TCP 443 Keluar
   - Sumber: Backup gateway
   - Tujuan: tuan rumah ESXi
   - Gunakan: Memungkinkan gateway Backup untuk berkomunikasi dengan host ESXi.
8. TCP 902 Keluar
   - Sumber: Backup gateway
   - Tujuan: Host VMware ESXi
   - Penggunaan: Digunakan untuk transfer data melalui gateway Backup.

Port di atas diperlukan untuk gateway Backup. Lihat Membuat titik akhir AWS Backup VPC untuk informasi selengkapnya tentang cara mengonfigurasi titik akhir VPC Amazon untuk. AWS Backup

Konfigurasi firewall

Backup gateway memerlukan akses ke endpoint layanan berikut untuk berkomunikasi Amazon Web Services. Jika Anda menggunakan firewall atau router untuk memfilter atau membatasi lalu lintas jaringan, Anda harus mengonfigurasi firewall dan router Anda untuk mengizinkan titik akhir layanan ini untuk komunikasi keluar. AWS Penggunaan proxy HTTP di antara gateway Backup dan titik layanan tidak didukung.

```
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
```

Konfigurasikan gateway Anda untuk beberapa NIC di VMware

Anda dapat memelihara jaringan terpisah untuk lalu lintas internal dan eksternal Anda dengan melampirkan beberapa koneksi antarmuka jaringan virtual (NIC) ke gateway Anda dan kemudian mengarahkan lalu lintas internal (gateway ke hypervisor) dan lalu lintas eksternal (gateway ke) secara terpisah. AWS

Secara default, mesin virtual yang terhubung ke AWS Backup gateway memiliki satu adaptor jaringan (`eth0`). Jaringan ini mencakup hypervisor, mesin virtual, dan gateway jaringan (Backup gateway) yang berkomunikasi dengan Internet yang lebih luas.

Berikut adalah contoh pengaturan dengan beberapa antarmuka jaringan virtual:

```
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
```

- Dalam contoh ini, koneksi ke hypervisor dengan IP`10.0.3.123`, gateway akan digunakan `eth0` sebagai IP hypervisor adalah bagian dari blok `10.0.3.0/24`
- Untuk terhubung ke hypervisor dengan IP`10.0.0.234`, gateway akan menggunakan `eth1`
- Untuk terhubung ke IP di luar jaringan lokal (mis. `34.193.121.211`), gateway akan kembali ke gateway default,`10.0.0.1`, yang ada di `10.0.0.0/24` blok dan dengan demikian melewati `eth1`

Urutan pertama untuk menambahkan adaptor jaringan tambahan terjadi di klien vSphere:

1. Di klien VMware vSphere, buka menu konteks (dengan klik kanan) untuk mesin virtual gateway Anda, dan pilih Edit Pengaturan.
2. Pada tab Virtual Hardware pada kotak dialog Virtual Machine Properties, buka menu Add New Device, dan pilih Network Adapter untuk menambahkan adaptor jaringan baru.
3. a. Perluas detail K Networ Baru untuk mengonfigurasi adaptor baru.
   b. Pastikan Connect At Power On dipilih.

   c. Untuk Jenis Adaptor, lihat Jenis Adaptor Jaringan di Dokumentasi Server ESXi dan vCenter.
4. Klik Oke untuk menyimpan pengaturan adaptor jaringan baru.

Urutan langkah berikutnya untuk mengonfigurasi adaptor tambahan terjadi di konsol AWS Backup gateway (perhatikan ini bukan antarmuka yang sama dengan konsol AWS manajemen tempat cadangan dan layanan lainnya dikelola).

Setelah NIC baru ditambahkan ke gateway VM, Anda perlu

- Pergi ke `Command Prompt` dan nyalakan adaptor baru
- Konfigurasikan IP statis untuk setiap NIC baru
- Tetapkan NIC pilihan sebagai default

Untuk melakukan ini:

1. Di klien VMware vSphere, pilih mesin virtual gateway Anda dan Luncurkan Konsol Web untuk mengakses konsol lokal gateway Backup.
   - Untuk informasi selengkapnya tentang mengakses konsol lokal, lihat Mengakses Konsol Lokal Gateway dengan VMware ESXi
2. Keluar dari Command Prompt dan pergi ke Network Configuration > Configure Static IP dan ikuti instruksi setup untuk memperbarui tabel routing.
   a. Tetapkan IP statis dalam subnet adaptor jaringan.
   b. Siapkan masker jaringan.
   c. Masukkan alamat IP gateway default. Ini adalah gateway jaringan yang terhubung ke semua lalu lintas di luar jaringan lokal.
3. Pilih Set Default Adapter untuk menunjuk adaptor yang akan terhubung ke cloud sebagai perangkat default.
4. Semua alamat IP untuk gateway dapat ditampilkan di konsol lokal dan di halaman ringkasan VM di VMware vSphere.

Persyaratan perangkat keras

Anda harus dapat mendedikasikan sumber daya minimum berikut pada host mesin virtual untuk gateway Backup:

- 4 prosesor virtual
- 8 GiB RAM yang dipesan

Izin VMware

Bagian ini mencantumkan izin VMware minimum yang diperlukan untuk digunakan. AWS Backup gateway Izin ini diperlukan untuk gateway Backup untuk menemukan, mencadangkan, dan memulihkan mesin virtual.

Untuk menggunakan gateway Backup dengan VMware Cloud™ on AWS atau VMware Cloud™ aktif AWS Outposts, Anda harus menggunakan pengguna admin default `cloudadmin@vmc.local` atau menetapkan CloudAdmin peran tersebut ke pengguna khusus Anda.

Untuk menggunakan gateway Backup dengan mesin virtual lokal VMware, buat pengguna khusus dengan izin yang tercantum di bawah ini.

Global

- Nonaktifkan metode
- Aktifkan metode
- Lisensi
- Log acara
- Mengelola atribut kustom
- Mengatur atribut kustom

Penandaan vSphere

- Tetapkan atau Batalkan Tetapkan Tag vSphere

DataStore

- Alokasikan ruang
- Jelajahi datastore
- Konfigurasikan datastore (untuk vSAN datastore)
- Operasi file tingkat rendah
- Perbarui file mesin virtual

Host

- Konfigurasi
  - Pengaturan lanjutan
  - Konfigurasi partisi penyimpanan

Folder

- Buat folder

Jaringan

- Tetapkan jaringan

Grup DVport

- Buat
- Hapus

Sumber Daya

- Tetapkan mesin virtual ke kumpulan sumber daya

Mesin Virtual

- Ubah Konfigurasi
  - Dapatkan sewa disk
  - Tambahkan disk yang ada
  - Tambahkan disk baru
  - Konfigurasi lanjutan
  - Ubah pengaturan
  - Konfigurasikan perangkat mentah
  - Ubah pengaturan perangkat
  - Hapus disk

    - Tetapkan anotasi
    - Alihkan pelacakan perubahan disk
- Edit Inventaris
    - Buat dari yang ada
    - Buat yang baru
    - Pendaftaran
    - Menghapus
    - Batalkan pendaftaran
- Interaksi
    - Matikan
    - Hidupkan
- Penyediaan
    - Izinkan akses disk
    - Izinkan akses disk hanya-baca
    - Izinkan unduhan mesin virtual
- Manajemen Snapshot
    - Membuat snapshot
    - Hapus Snapshot
    - Kembali ke snapshot

Bekerja dengan gateway

Untuk mencadangkan dan memulihkan mesin virtual (VM) Anda menggunakan AWS Backup, Anda harus terlebih dahulu menginstal gateway Backup. Gateway adalah perangkat lunak dalam bentuk template OVF (Open Virtualization Format) yang menghubungkan Amazon Web Services Backup ke hypervisor Anda, memungkinkannya mendeteksi mesin virtual Anda secara otomatis, dan memungkinkan Anda untuk mencadangkan dan memulihkannya.

Sebuah gateway tunggal dapat menjalankan hingga 4 backup atau memulihkan pekerjaan sekaligus. Untuk menjalankan lebih dari 4 pekerjaan sekaligus, buat lebih banyak gateway dan kaitkan dengan hypervisor Anda.

Membuat gateway

Untuk membuat gateway:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, di bawah bagian Sumber daya eksternal, pilih Gateway.
3. Pilih Buat gateway.
4. Di bagian Siapkan gateway, ikuti petunjuk ini untuk mengunduh dan menyebarkan template OVF.

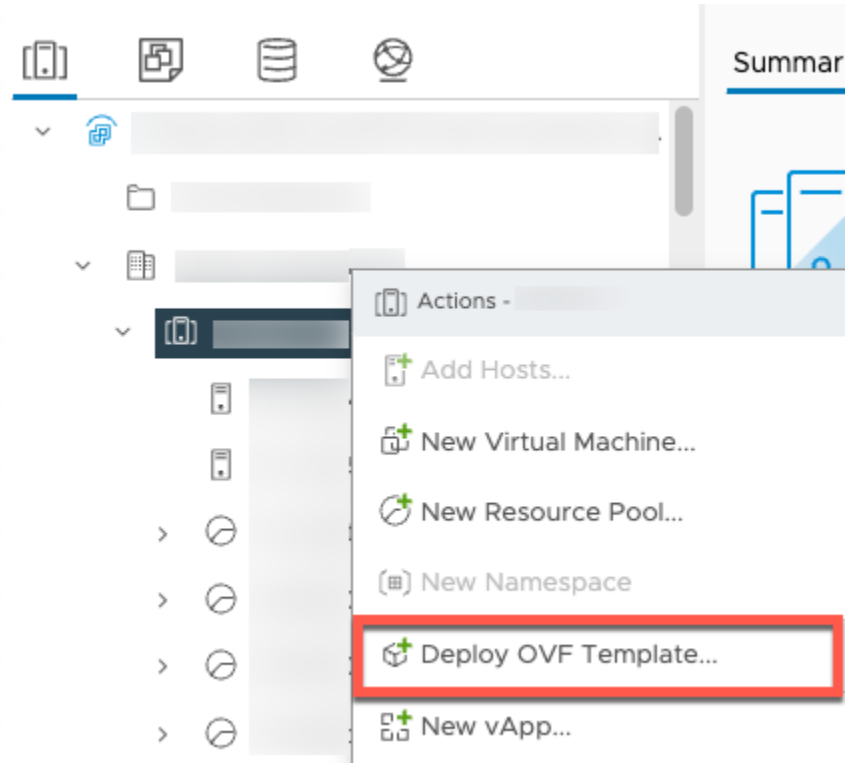
Mengunduh perangkat lunak VMware

Menghubungkan hypervisor

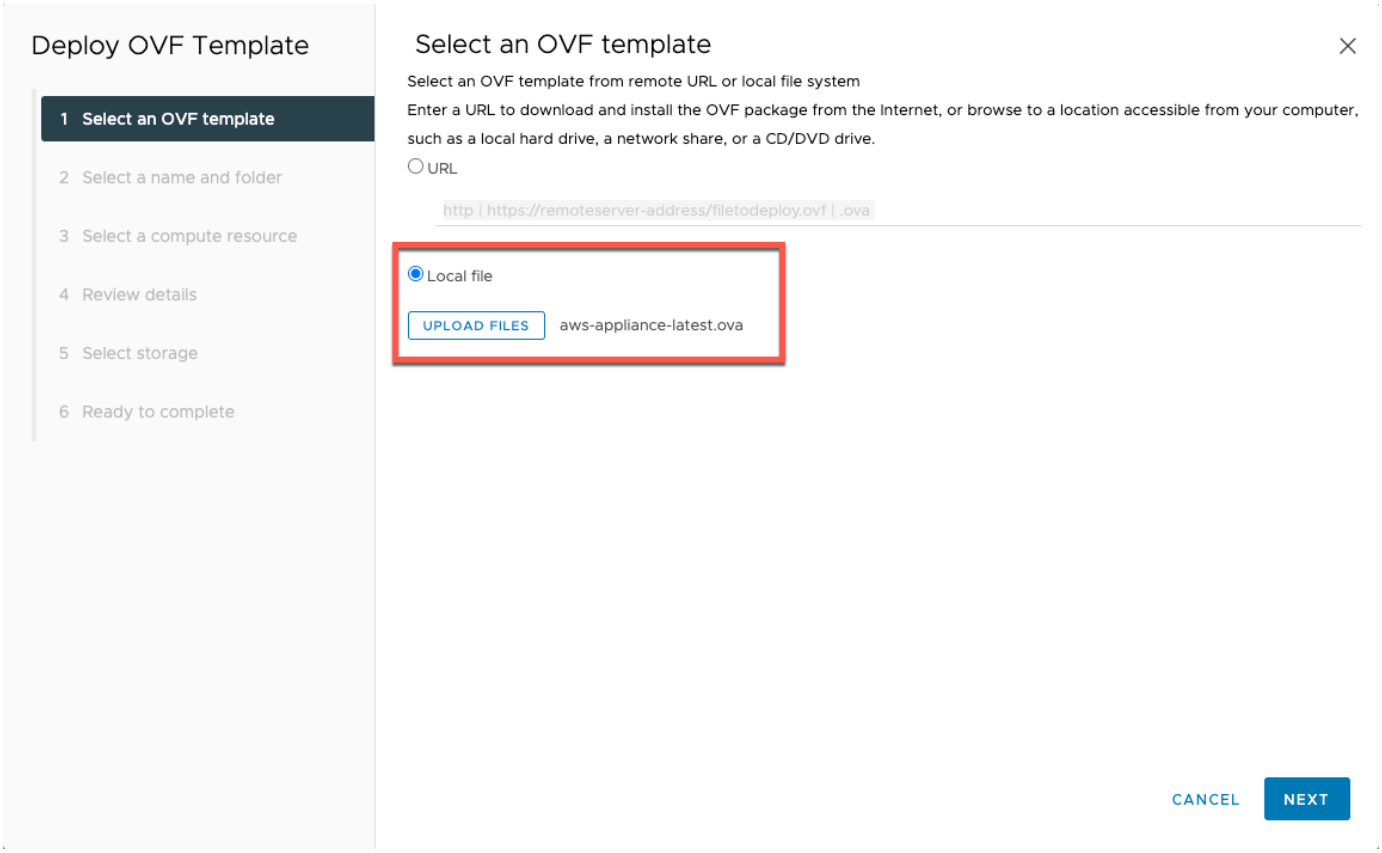
Gateway terhubung AWS Backup ke hypervisor Anda sehingga Anda dapat membuat dan menyimpan cadangan mesin virtual Anda. Untuk mengatur gateway Anda di VMware ESXi, unduh template OVF. Pengunduhan mungkin memakan waktu sekitar 10 menit.

Setelah selesai, lanjutkan dengan langkah-langkah berikut:

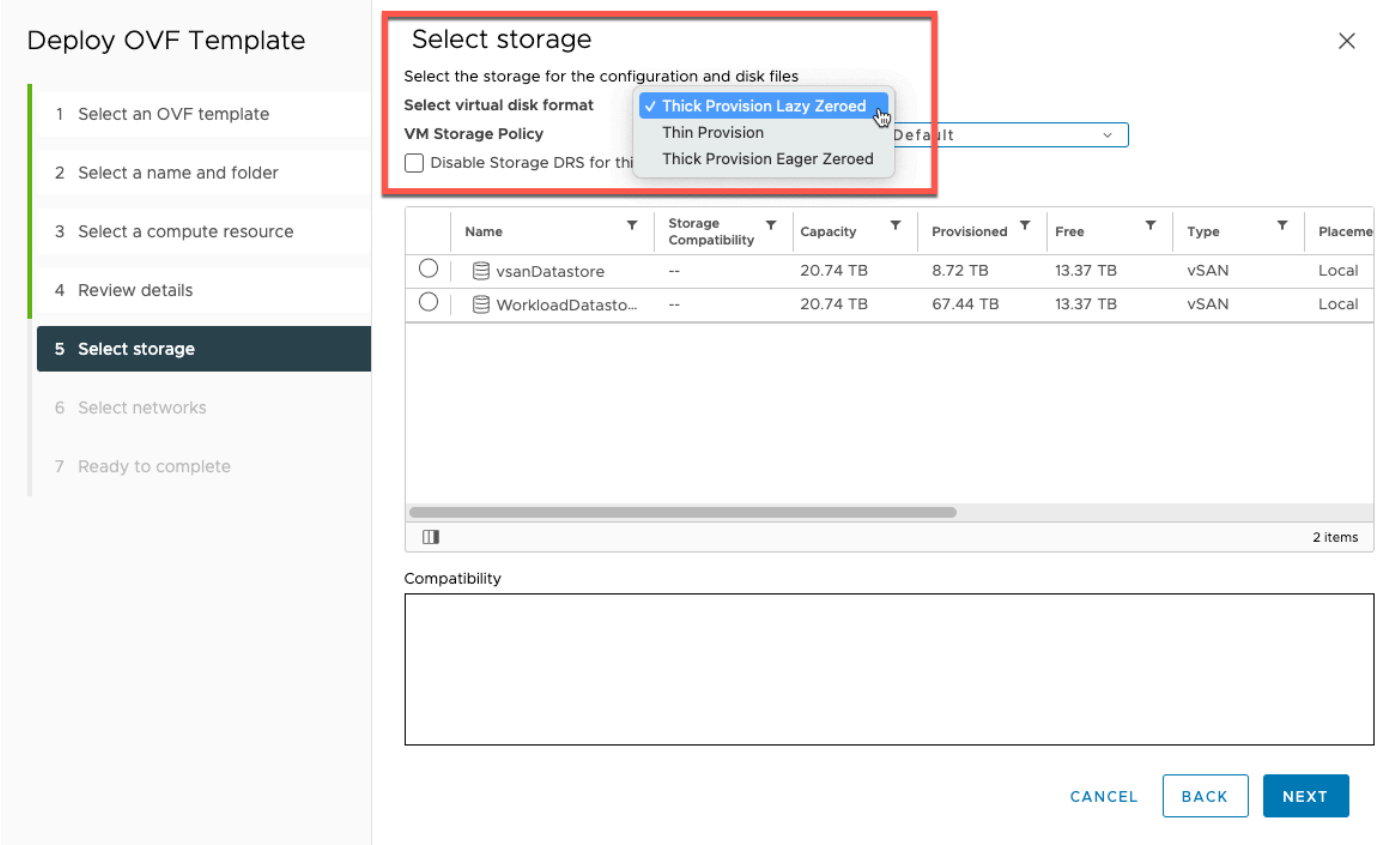
1. Connect ke hypervisor mesin virtual Anda menggunakan VMware vSphere.
2. Klik kanan objek induk dari mesin virtual dan pilih Deploy OVF Template.



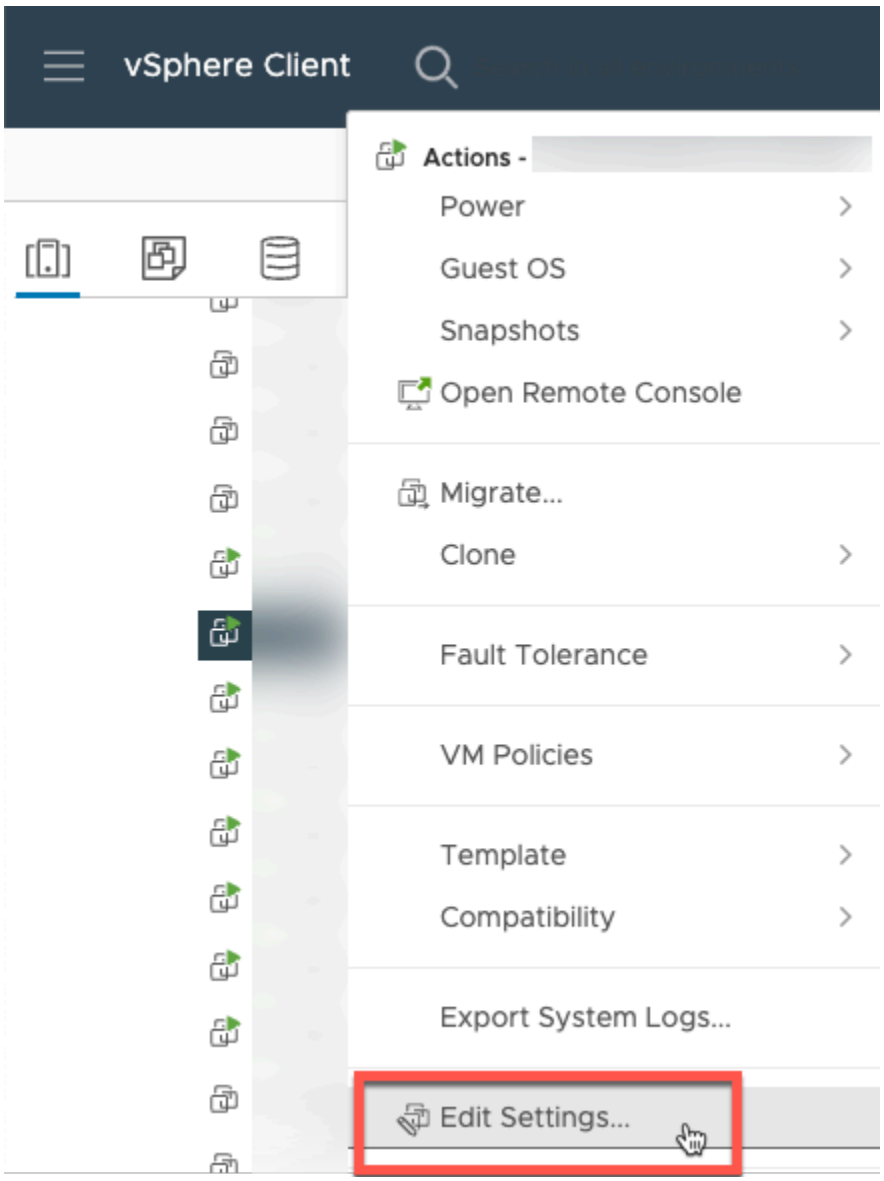
3. Pilih File lokal, dan unggah aws-appliance-latestfile.ova yang Anda unduh.



4. Ikuti langkah-langkah panduan penerapan untuk menerapkannya. Pada halaman Pilih penyimpanan, pilih format disk virtual Thick Provision Lazy Zeroed.

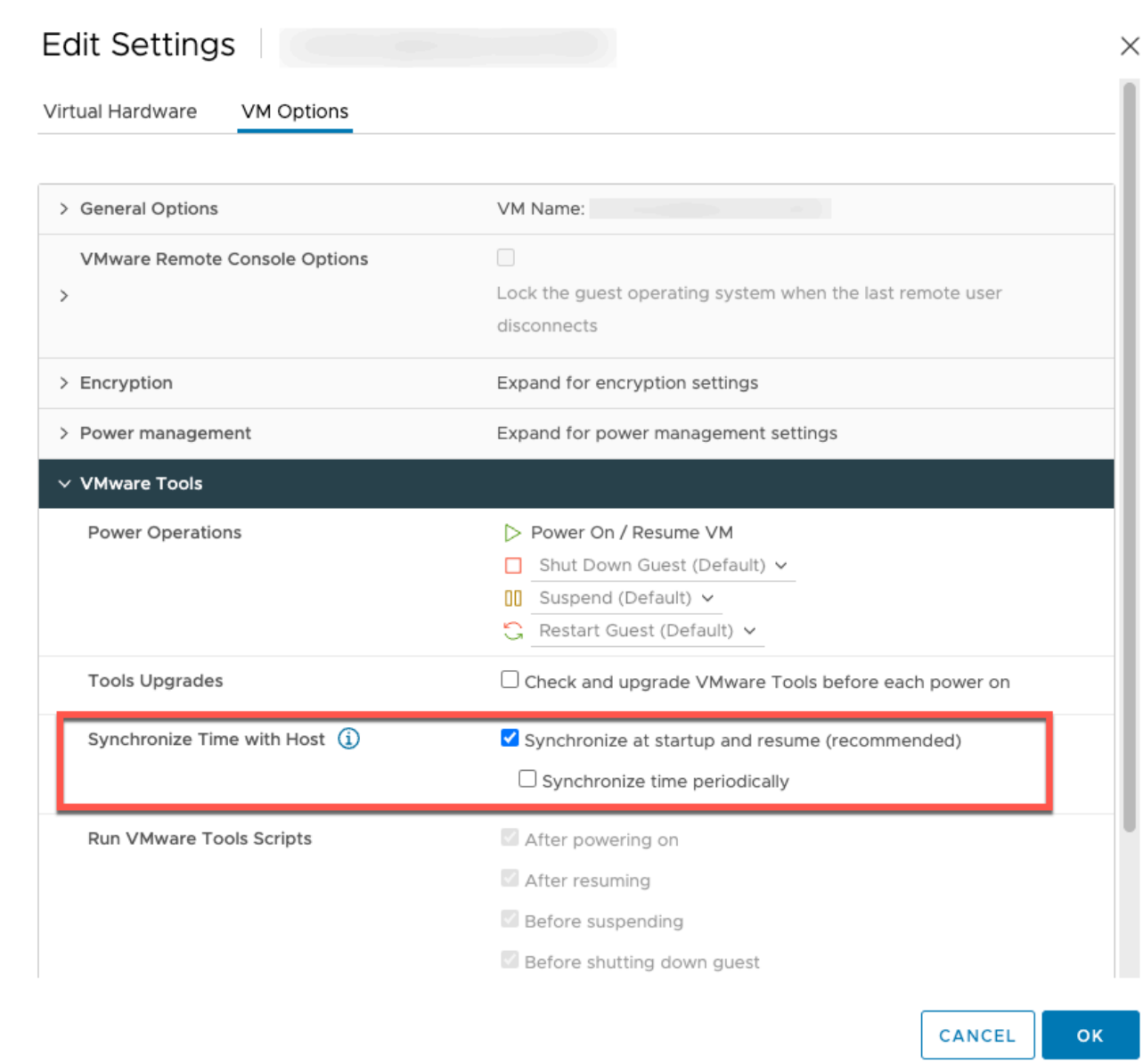


5. Setelah menerapkan OVF, klik kanan gateway dan pilih Edit Pengaturan.

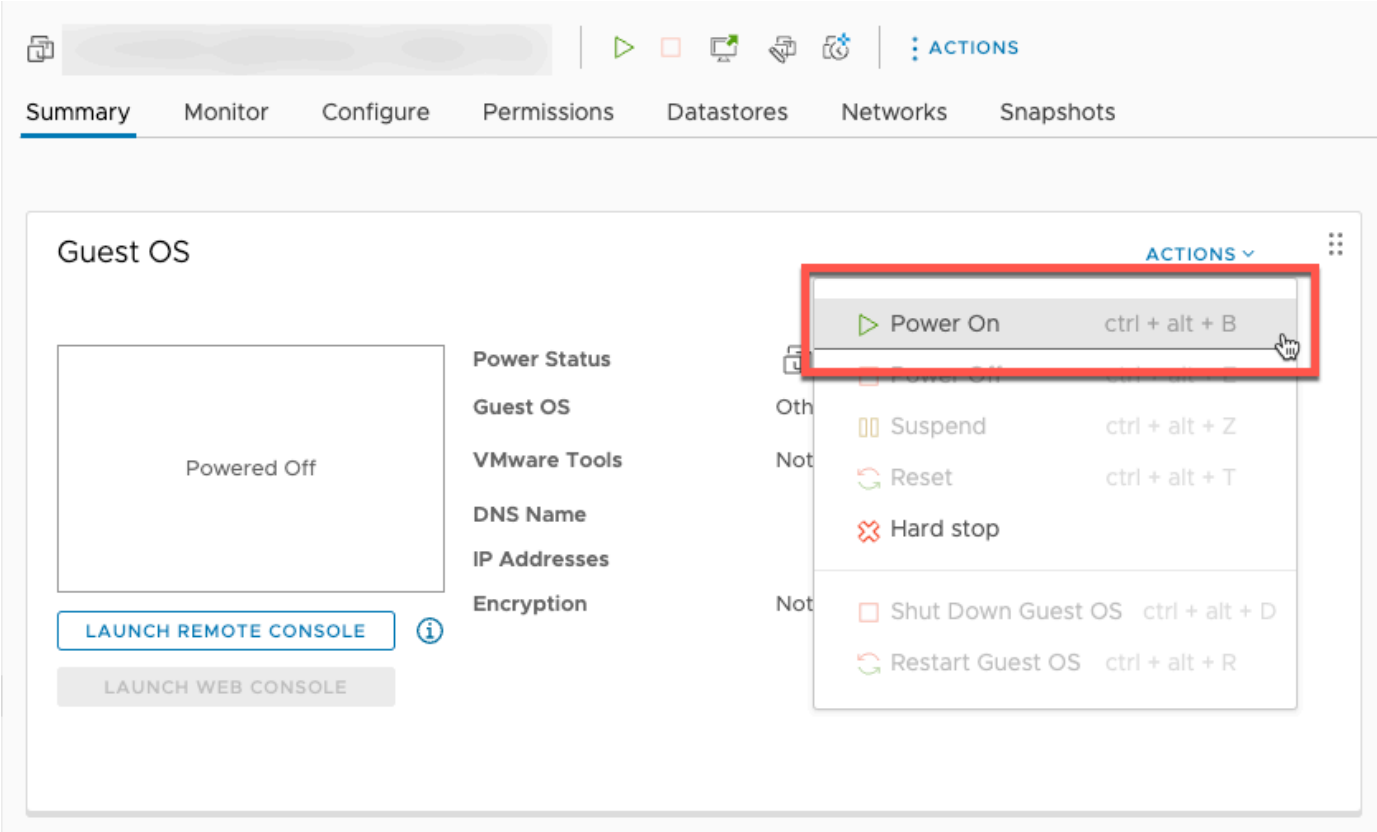


a. Di bawah VM Options, buka VM Tools.

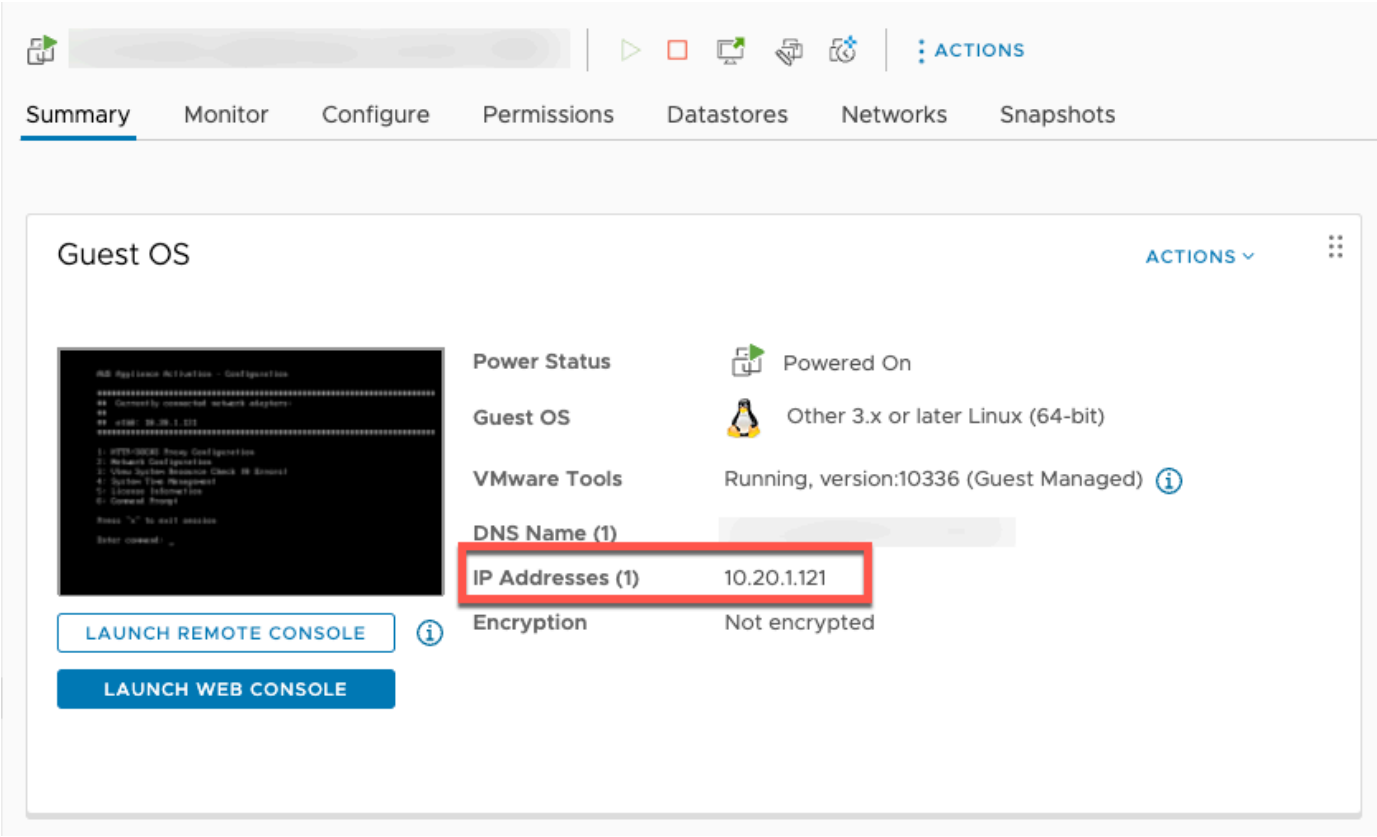
b. Pastikan bahwa untuk Sinkronisasi Waktu dengan Host, Sinkronisasi saat memulai dan melanjutkan dipilih.



6. Nyalakan mesin virtual dengan memilih “Power On” dari menu Tindakan.



7. Salin alamat IP dari ringkasan VM dan masukkan di bawah ini.



Setelah perangkat lunak VMware diunduh, selesaikan langkah-langkah berikut:

1. Di bagian koneksi Gateway, ketik alamat IP gateway.
   a. Untuk menemukan alamat IP ini, buka Klien vSphere.
   b. Pilih gateway Anda di bawah tab Ringkasan.
   c. Salin alamat IP dan tempel di bilah teks AWS Backup konsol.
2. Di bagian Pengaturan Gateway,
   a. Ketik nama Gateway.
   b. Verifikasi AWS Wilayah.
   c. Pilih apakah titik akhir dapat diakses publik atau di-host dengan virtual private cloud (VPC) Anda.
   d. Bergantung pada titik akhir yang dipilih, masukkan Nama DNS titik akhir VPC.

      Untuk informasi selengkapnya, lihat Membuat titik akhir VPC.
3. [Opsional] Di bagian tag Gateway, Anda dapat menetapkan tag dengan memasukkan kunci dan nilai opsional. Untuk menambahkan lebih dari satu tag, klik Tambahkan tag lain.
4. Untuk menyelesaikan proses, klik Buat gateway, yang akan membawa Anda ke halaman detail gateway.

Mengedit atau menghapus gateway

Untuk mengedit atau menghapus gateway:

1. Di panel navigasi kiri, di bawah bagian Sumber daya eksternal, pilih Gateway.
2. Di bagian Gateway, pilih gateway dengan nama Gateway nya.
3. Untuk mengedit nama gateway, pilih Edit.
4. Untuk menghapus gateway, pilih Hapus, lalu pilih Hapus gateway.

   Anda tidak dapat mengaktifkan kembali gateway yang dihapus. Jika Anda ingin terhubung ke hypervisor lagi, ikuti prosedur di. Membuat gateway
5. Untuk terhubung ke hypervisor, di bagian Connected hypervisor, pilih Connect.

Setiap gateway terhubung ke hypervisor tunggal. Namun, Anda dapat menghubungkan beberapa gateway ke hypervisor yang sama untuk meningkatkan bandwidth di antara mereka di luar gateway pertama.

6. Untuk menetapkan, mengedit, atau mengelola tag, di bagian Tag, pilih Kelola tag.

Backup gateway Bandwidth Throttling

> **Note**
>
> Fitur ini akan tersedia di gateway baru yang digunakan setelah 15 Desember 2022. Untuk gateway yang ada, kemampuan baru ini akan tersedia melalui pembaruan perangkat lunak otomatis pada atau sebelum 30 Januari 2023. Untuk memperbarui gateway ke versi terbaru secara manual, gunakan AWS CLI perintah `UpdateGatewaySoftwareNow`.

Anda dapat membatasi throughput unggahan dari gateway Anda AWS Backup untuk mengontrol jumlah bandwidth jaringan yang digunakan gateway. Secara default, gateway yang diaktifkan tidak memiliki batas tarif.

Anda dapat mengonfigurasi jadwal batas kecepatan bandwidth menggunakan AWS Backup Konsol atau menggunakan API melalui AWS CLI () `PutBandwidthRateLimitSchedule`. Saat Anda menggunakan jadwal batas tingkat bandwidth, Anda dapat mengonfigurasi batas untuk berubah secara otomatis sepanjang hari atau minggu.

Pembatasan laju bandwidth bekerja dengan menyeimbangkan throughput semua data yang diunggah, dirata-ratakan setiap detik. Meskipun dimungkinkan untuk unggahan untuk melewati batas laju bandwidth secara singkat untuk setiap mikro atau milidetik tertentu, ini biasanya tidak menghasilkan lonjakan besar dalam jangka waktu yang lebih lama.

Anda dapat menambahkan hingga maksimal 20 interval. Nilai maksimum untuk kecepatan unggah adalah 8.000.000 (juta) megabita per detik (Mbps).

Lihat dan edit jadwal batas kecepatan bandwidth untuk gateway Anda menggunakan konsol. AWS Backup

Bagian ini menjelaskan cara melihat dan mengedit jadwal batas laju bandwidth untuk gateway Anda.

Untuk melihat dan mengedit jadwal batas bandwidth rate

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Gateway. Di panel Gateways, gateway ditampilkan berdasarkan nama. Klik tombol radio yang berdekatan dengan nama gateway yang ingin Anda kelola.
3. Setelah Anda memilih tombol radio, menu drop-down Tindakan tersedia untuk diklik. Klik Tindakan, lalu klik Edit jadwal batas laju bandwidth. Jadwal saat ini ditampilkan. Secara default, gateway baru atau yang belum diedit tidak memiliki batas kecepatan bandwidth yang ditentukan.

   > **Note**
   >
   > Anda juga dapat mengklik Kelola jadwal di halaman detail gateway untuk menavigasi ke halaman Edit bandwidth.

4. (Opsional) Pilih Tambahkan interval untuk menambahkan interval baru yang dapat dikonfigurasi ke jadwal. Untuk setiap interval, masukkan informasi berikut:

   a. Hari dalam seminggu — Pilih hari berulang atau hari di mana Anda ingin interval diterapkan. Saat dipilih, hari akan ditampilkan di bawah menu tarik-turun. Anda dapat menghapusnya dengan mengklik X di sebelah hari.

   b. Waktu mulai - Masukkan waktu mulai untuk interval bandwidth, menggunakan format 24 jam HH: MM. Waktu diberikan dalam Universal Coordinated Time (UTC).

      Catatan: bandwidth-rate-limit Interval Anda dimulai pada awal menit yang ditentukan.

   c. Waktu akhir - Masukkan waktu akhir untuk interval bandwidth, menggunakan format 24 jam HH: MM. Waktu diberikan dalam Universal Coordinated Time (UTC).

      > **Important**
      >
      > bandwidth-rate-limit Interval berakhir pada akhir menit yang ditentukan. Untuk menjadwalkan interval yang berakhir pada akhir jam, masukkan`59`. Untuk menjadwalkan interval kontinu berturut-turut, transisi pada awal jam, tanpa gangguan di antara interval, masukkan `59` untuk menit akhir interval pertama. Masukkan `00` untuk menit awal interval berikutnya.

   d. Kecepatan unggah - Masukkan batas kecepatan unggah, dalam megabit per detik (Mbps). Nilai minimum adalah 102 megabyte per detik (Mbps).

5. (Opsional) Ulangi langkah sebelumnya sesuai keinginan hingga jadwal batas laju bandwidth Anda selesai. Jika Anda perlu menghapus interval dari jadwal Anda, pilih Hapus.

> **Important**
>
> Interval batas laju bandwidth tidak dapat tumpang tindih. Waktu mulai suatu interval harus terjadi setelah waktu akhir dari interval sebelumnya dan sebelum waktu mulai dari interval berikut; waktu akhirnya harus terjadi sebelum waktu mulai interval berikut.

6. Setelah selesai, klik tombol Simpan perubahan.

Lihat dan edit jadwal batas kecepatan bandwidth untuk gateway Anda menggunakan. AWS CLI

`GetBandwidthRateLimitSchedule`Tindakan ini dapat digunakan untuk melihat jadwal throttle bandwidth untuk gateway tertentu. Jika tidak ada jadwal yang ditetapkan, jadwal akan menjadi daftar interval kosong. Berikut adalah contoh menggunakan AWS CLI untuk mengambil jadwal bandwidth gateway:

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

Untuk mengedit jadwal throttle bandwidth gateway, Anda dapat menggunakan tindakan. `PutBandwidthRateLimitSchedule` Perhatikan bahwa Anda hanya dapat memperbarui jadwal gateway secara keseluruhan, daripada memodifikasi, menambahkan, atau menghapus interval individual. Memanggil tindakan ini akan menimpa jadwal throttle bandwidth gateway sebelumnya.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

Bekerja dengan hypervisor

Setelah selesaiMembuat gateway, Anda dapat menghubungkannya ke hypervisor AWS Backup untuk memungkinkan bekerja dengan mesin virtual yang dikelola oleh hypervisor itu. Misalnya, hypervisor untuk VMware VM adalah VMware vCenter Server. Pastikan hypervisor Anda dikonfigurasi dengan izin yang diperlukan untuk. AWS Backup

Menambahkan hypervisor

Untuk menambahkan hypervisor:

1. Di panel navigasi kiri, di bawah bagian Sumber daya eksternal, pilih Hypervisor.
2. Pilih Tambahkan hypervisor.
3. Di bagian pengaturan Hypervisor, ketik nama Hypervisor.
4. Untuk host server vCenter, gunakan menu dropdown untuk memilih alamat IP atau FQDN (nama domain yang sepenuhnya memenuhi syarat). Ketik nilai yang sesuai.
5. AWS Backup Untuk memungkinkan menemukan mesin virtual pada hypervisor, masukkan Nama Pengguna dan Kata Sandi hypervisor.
6. Enkripsi kata sandi Anda. Anda dapat menentukan enkripsi ini dengan memilih kunci KMS yang dikelola layanan tertentu atau kunci KMS yang dikelola pelanggan menggunakan menu tarik-turun atau pilih Buat kunci KMS. Jika Anda tidak memilih kunci tertentu, AWS Backup akan mengenkripsi kata sandi Anda menggunakan kunci milik layanan.
7. Di bagian Connecting gateway, gunakan daftar dropdown untuk menentukan Gateway mana yang akan dihubungkan ke hypervisor Anda.
8. Pilih Uji koneksi gateway untuk memverifikasi input Anda sebelumnya.
9. Secara opsional, di bagian tag Hypervisor, Anda dapat menetapkan tag ke hypervisor dengan memilih Tambahkan tag baru.
10. Pemetaan tag VMware opsional: Anda dapat menambahkan hingga 10 tag VMware yang saat ini Anda gunakan di mesin virtual Anda untuk menghasilkan tag. AWS
11. Di panel pengaturan grup Log, Anda dapat memilih untuk berintegrasi dengan Amazon CloudWatch Logs untuk memelihara log hypervisor Anda (harga CloudWatch Log standar akan berlaku berdasarkan penggunaan). Setiap hypervisor dapat menjadi milik satu grup log.
    a. Jika Anda belum membuat grup log, pilih tombol Buat grup log baru radio. Hypervisor yang Anda edit akan dikaitkan dengan grup log ini.
    b. Jika sebelumnya Anda telah membuat grup log untuk hypervisor yang berbeda, Anda dapat menggunakan grup log tersebut untuk hypervisor ini. Pilih Gunakan grup log yang ada.
    c. Jika Anda tidak ingin CloudWatch logging, pilih Nonaktifkan logging.
12. Pilih Tambahkan hypervisor, yang membawa Anda ke halaman detailnya.

> **Tip**
>
> Anda dapat menggunakan Amazon CloudWatch Logs (lihat langkah 11 di atas) untuk mendapatkan informasi tentang hypervisor Anda, termasuk pemantauan kesalahan, koneksi jaringan antara gateway dan hypervisor, dan informasi konfigurasi jaringan. Untuk informasi tentang grup CloudWatch log, lihat Bekerja dengan Grup Log dan Aliran Log di Panduan CloudWatch Pengguna Amazon.

Melihat mesin virtual yang dikelola oleh hypervisor

Untuk melihat mesin virtual pada hypervisor:

1. Di panel navigasi kiri, di bawah bagian Sumber daya eksternal, pilih Hypervisor.
2. Di bagian Hypervisors, pilih hypervisor dengan nama Hypervisor untuk membuka halaman detailnya.
3. Di bagian di bawah ringkasan Hypervisor, pilih tab Mesin virtual.
4. Di bagian Connected Virtual Machines, daftar mesin virtual terisi secara otomatis.

Melihat gateway yang terhubung ke hypervisor

Untuk melihat gateway yang terhubung ke hypervisor:

1. Pilih tab Gateways.
2. Di bagian gateway Terhubung, daftar gateway terisi secara otomatis.

Menghubungkan hypervisor ke gateway tambahan

Kecepatan pencadangan dan pemulihan Anda mungkin dibatasi oleh bandwidth koneksi antara gateway dan hypervisor Anda. Anda dapat meningkatkan kecepatan ini dengan menghubungkan satu atau lebih gateway tambahan ke hypervisor Anda. Anda dapat melakukan ini di bagian gateway Terhubung sebagai berikut:

1. Pilih Hubungkan.
2. Pilih gateway lain menggunakan menu tarik-turun. Atau, pilih Buat gateway untuk membuat gateway baru.
3. Pilih Hubungkan.

Mengedit konfigurasi hypervisor

Jika Anda tidak menggunakan fitur koneksi gateway Uji, Anda dapat menambahkan hypervisor dengan nama pengguna atau kata sandi yang salah. Dalam hal ini, status koneksi hypervisor selalu. `Pending` Atau, Anda dapat memutar nama pengguna atau kata sandi untuk mengakses hypervisor Anda. Perbarui informasi ini menggunakan prosedur berikut:

Untuk mengedit hypervisor yang sudah ditambahkan:

1. Di panel navigasi kiri, di bawah bagian Sumber daya eksternal, pilih Hypervisor.
2. Di bagian Hypervisors, pilih hypervisor dengan nama Hypervisor untuk membuka halaman detailnya.
3. Pilih Edit.
4. Panel atas diberi nama pengaturan Hypervisor.
    a. Di bawah host server vCenter, Anda juga dapat mengedit FQDN (Fully-Qualified Domain Name) atau alamat IP.
    b. Secara opsional, masukkan Nama Pengguna dan Kata Sandi hypervisor.
5. Di panel pengaturan grup Log, Anda dapat memilih untuk berintegrasi dengan Amazon CloudWatch untuk memelihara log hypervisor Anda (CloudWatch harga standar akan berlaku berdasarkan penggunaan). Setiap hypervisor dapat menjadi milik satu grup log.
    a. Jika Anda belum membuat grup log, pilih tombol Buat grup log baru radio. Hypervisor yang Anda edit akan dikaitkan dengan grup log ini.
    b. Jika sebelumnya Anda telah membuat grup log untuk hypervisor yang berbeda, Anda dapat menggunakan grup log tersebut untuk hypervisor ini. Pilih Gunakan grup log yang ada.
    c. Jika Anda tidak ingin CloudWatch logging, pilih Nonaktifkan logging.

> **Tip**
>
> Anda dapat menggunakan Amazon CloudWatch Logs (lihat langkah 5 di atas) untuk mendapatkan informasi tentang hypervisor Anda, termasuk pemantauan kesalahan, koneksi jaringan antara gateway dan hypervisor, dan informasi konfigurasi jaringan. Untuk informasi tentang grup CloudWatch log, lihat Bekerja dengan Grup Log dan Aliran Log di Panduan CloudWatch Pengguna Amazon.

Untuk memperbarui hypervisor secara terprogram, gunakan perintah CLI update-hypervisor dan panggilan API. _UpdateHypervisor

Menghapus konfigurasi hypervisor

Jika Anda perlu menghapus hypervisor yang sudah ditambahkan, hapus konfigurasi hypervisor dan tambahkan yang lain. Operasi hapus ini berlaku untuk konfigurasi untuk terhubung ke hypervisor. Itu tidak menghapus hypervisor.

Untuk menghapus konfigurasi untuk terhubung ke hypervisor yang sudah ditambahkan:

1. Di panel navigasi kiri, di bawah bagian Sumber daya eksternal, pilih Hypervisor.
2. Di bagian Hypervisors, pilih hypervisor dengan nama Hypervisor untuk membuka halaman detailnya.
3. Pilih Hapus, lalu pilih Hapus hypervisor.
4. Opsional: ganti konfigurasi hypervisor yang dihapus menggunakan prosedur untuk. Menambahkan hypervisor

Memahami status hypervisor

Berikut ini menjelaskan masing-masing status hypevisor yang mungkin dan, jika berlaku, langkah-langkah remediasi. `ONLINE`Statusnya adalah status normal hypervisor. Hypervisor harus memiliki status ini sepanjang atau sebagian besar waktu itu digunakan untuk pencadangan dan pemulihan VM yang dikelola oleh hypervisor.

Status hypervisor

Status	Arti dan remediasi
`ONLINE`	Anda menambahkan hypervisor ke AWS Backup, yang terkait dengannya gateway, dan dapat terhubung dengan gateway itu melalui jaringan Anda untuk melakukan pencadangan dan pemulihan mesin virtual yang dikelola oleh hypervisor. Anda dapat melakukan pencadangan sesuai permintaan dan terjadwal dari mesin virtual tersebut kapan saja.

Status	Arti dan remediasi
`PENDING`	Anda menambahkan hypervisor ke AWS Backup tetapi: • Ini tidak terkait dengan gateway apa pun, atau • Ini terkait dengan satu atau lebih gateway, tetapi semua gateway itu dihapus atau tidak aktif. Untuk mengubah status hypervisor dari `PENDING` ke`ONLINE`, buat gateway dan hubungkan hypervisor Anda ke gateway itu.
`OFFLINE`	Anda menambahkan hypervisor ke AWS Backup dan menghubungkannya dengan gateway, tetapi gateway tidak dapat terhubung ke hypervisor melalui jaringan Anda. Untuk mengubah status hypervisor dari `OFFLINE` ke`ONLINE`, verifikasi kebenaran konfigurasi jaringan Anda. Jika masalah berlanjut, verifikasi bahwa alamat IP hypervisor Anda atau nama domain yang sepenuhnya memenuhi syarat sudah benar. Jika salah, tambahkan hypervisor Anda lagi menggunakan informasi yang benar dan uji koneksi gateway Anda.

Status	Arti dan remediasi
ERROR	Anda menambahkan hypervisor ke AWS Backup dan menghubungkannya dengan gateway, tetapi gateway tidak dapat berkomuni kasi dengan hypervisor. Untuk mengubah status hypervisor dari ERROR keONLINE, verifikasi bahwa nama pengguna dan kata sandi hypervisor sudah benar. Jika salah, edit konfigurasi hypervisor Anda.

Langkah selanjutnya

Untuk mencadangkan mesin virtual pada hypervisor Anda, lihat. Mencadangkan mesin virtual

Mencadangkan mesin virtual

Setelah ituMenambahkan hypervisor, Backup gateway secara otomatis mencantumkan mesin virtual Anda. Anda dapat melihat mesin virtual Anda dengan memilih Hypervisor atau mesin Virtual di panel navigasi kiri.

- Pilih Hypervisor untuk melihat hanya mesin virtual yang dikelola oleh hypervisor tertentu. Dengan tampilan ini, Anda dapat bekerja dengan satu mesin virtual sekaligus.
- Pilih mesin Virtual untuk melihat semua mesin virtual di semua hypervisor yang Anda tambahkan ke Anda. Akun AWS Dengan tampilan ini, Anda dapat bekerja dengan beberapa atau semua mesin virtual Anda di beberapa hypervisor.

Terlepas dari tampilan mana yang Anda pilih, untuk melakukan operasi pencadangan pada mesin virtual tertentu, pilih nama VM untuk membuka halaman detailnya. Halaman detail VM adalah titik awal untuk prosedur berikut.

Membuat cadangan on-demand dari mesin virtual

Pencadangan sesuai permintaan adalah cadangan penuh satu kali yang Anda lakukan secara manual. Anda dapat menggunakan cadangan sesuai permintaan untuk menguji AWS Backup kemampuan pencadangan dan pemulihan.

Untuk membuat cadangan on-demand dari mesin virtual:

1. Pilih Buat cadangan sesuai permintaan.
2. Konfigurasikan cadangan sesuai permintaan Anda.
3. Pilih Buat cadangan sesuai permintaan.
4. Periksa kapan pekerjaan cadangan Anda memiliki status`Completed`. Di menu navigasi kiri, pilih Jobs.
5. Pilih Backup Job ID untuk melihat informasi pekerjaan cadangan seperti ukuran Backup dan waktu yang telah berlalu antara tanggal pembuatan dan tanggal Penyelesaian.

Cadangan VM tambahan

Versi VMware yang lebih baru berisi fitur yang disebut Changed Block Tracking, yang melacak blok penyimpanan mesin virtual saat mereka berubah seiring waktu. Saat Anda menggunakan AWS Backup untuk membuat cadangan mesin virtual, AWS Backup coba gunakan data CBT jika tersedia. AWS Backup menggunakan data CBT untuk mempercepat proses pencadangan; tanpa data CBT, pekerjaan cadangan seringkali lebih lambat dan menggunakan lebih banyak sumber daya hypervisor. Pencadangan masih dapat berhasil diselesaikan bahkan ketika data CBT tidak valid atau tersedia. Misalnya, data CBT mungkin tidak valid atau mungkin tidak tersedia jika mesin virtual atau host ESXi mengalami hard shutdown.

Pada kesempatan data CBT tidak valid atau tidak tersedia, status cadangan akan dibaca `Successful` dengan pesan. Dalam kasus ini, pesan akan menunjukkan bahwa, dengan tidak adanya data CBT, AWS Backup menggunakan mekanisme deteksi perubahan miliknya sendiri untuk menyelesaikan cadangan alih-alih data CBT VMware. Pencadangan selanjutnya akan mencoba kembali menggunakan data CBT, dan dalam banyak kasus data CBT akan berhasil valid dan tersedia. Jika masalah berlanjut, lihat Pemecahan Masalah VMware untuk langkah-langkah untuk memperbaiki.

Agar CBT berfungsi dengan benar, berikut ini harus benar:

- Host harus ESXi 4.0 atau yang lebih baru
- VM yang memiliki disk harus memiliki perangkat keras versi 7 atau yang lebih baru
- CBT harus diaktifkan untuk mesin virtual (diaktifkan secara default)

Untuk memverifikasi apakah disk virtual telah mengaktifkan CBT:

1. Buka Klien vSphere dan pilih mesin virtual yang dimatikan.
2. Klik kanan mesin virtual dan arahkan ke Edit Settings > Options > Advanced/General > Configuration Parameters.
3. Opsi `ctkEnabled` harus sama`True`.

Mengotomatiskan pencadangan mesin virtual dengan menetapkan sumber daya ke rencana cadangan

Rencana cadangan adalah kebijakan perlindungan data yang ditentukan pengguna yang mengotomatiskan perlindungan data di banyak AWS layanan dan aplikasi pihak ketiga. Pertama-tama Anda membuat paket cadangan dengan menentukan frekuensi cadangan, periode retensi, kebijakan siklus hidup, dan banyak opsi lainnya. Untuk membuat rencana cadangan, lihat Memulai tutorial.

Setelah membuat paket cadangan, Anda menetapkan sumber daya yang AWS Backup didukung, termasuk mesin virtual, ke paket cadangan tersebut. AWS Backup menawarkan banyak cara untuk menetapkan sumber daya, termasuk menetapkan semua sumber daya di akun Anda, termasuk atau mengecualikan sumber daya tunggal tertentu, atau menambahkan sumber daya dengan tag tertentu.

Selain fitur penugasan sumber daya yang ada, AWS Backup dukungan untuk mesin virtual memperkenalkan beberapa fitur baru untuk membantu Anda dengan cepat menetapkan mesin virtual ke rencana cadangan. Dari halaman mesin Virtual, Anda dapat menetapkan tag ke beberapa mesin virtual atau menggunakan fitur Tetapkan sumber daya baru untuk merencanakan. Gunakan fitur-fitur ini untuk menetapkan mesin virtual Anda yang sudah ditemukan oleh AWS Backup gateway.

Jika Anda mengantisipasi menemukan dan menetapkan mesin virtual tambahan di masa depan, dan ingin mengotomatiskan langkah penetapan sumber daya untuk menyertakan mesin virtual masa depan tersebut, gunakan fitur Create group assignment yang baru.

Tag VMware

Tag adalah pasangan nilai kunci yang dapat Anda gunakan untuk mengelola, memfilter, dan mencari sumber daya Anda.

Tag VMware terdiri dari kategori dan nama tag. Tag VMware digunakan untuk mengelompokkan mesin virtual. Nama tag adalah label yang ditetapkan ke mesin virtual. Kategori adalah kumpulan nama tag.

Dalam AWS tag, Anda dapat menggunakan karakter di antara huruf UTF-8, angka, spasi, dan karakter khusus. `+ - = . _ : /`

Jika Anda menggunakan tag pada mesin virtual Anda, Anda dapat menambahkan hingga 10 tag yang cocok AWS Backup untuk membantu organisasi. Anda dapat memetakan hingga 10 tag VMware ke AWS tag. Di AWS Backup konsol, ini dapat ditemukan di Organisasi saya> Mesin Virtual > AWS tag atau tag VMware.

Pemetaan tag VMware

Jika Anda menggunakan tag pada mesin virtual Anda, Anda dapat menambahkan hingga 10 tag yang cocok AWS Backup untuk kejelasan dan organisasi tambahan. Pemetaan berlaku untuk mesin virtual apa pun di hypervisor.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di konsol, buka edit Hypervisor (Klik Sumber daya eksternal, lalu Hypervisors, lalu klik nama Hypervisor, lalu klik Kelola pemetaan).
3. Panel terakhir, pemetaan tag VMware, berisi empat bidang kotak teks tempat Anda dapat memasukkan informasi tag VMware yang masih ada ke dalam tag yang sesuai. AWS Keempat bidang tersebut adalah kategori tag Vmware, nama tag VMware, kunci AWS tag, dan nilai AWS tag (contoh: Kategori = OS; Nama tag = Windows; kunci AWS tag = OS-Windows, dan AWS nilai tag = Windows).
4. Setelah Anda memasukkan nilai pilihan Anda, klik Tambahkan pemetaan. Jika Anda membuat kesalahan, Anda dapat mengklik Hapus untuk menghapus informasi yang dimasukkan.
5. Setelah menambahkan pemetaan, tentukan peran IAM yang ingin Anda gunakan untuk menerapkan AWS tag ini ke mesin virtual VMware.

   Kebijakan ini `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`berisi izin yang diperlukan. Anda dapat melampirkan kebijakan ini ke peran yang Anda gunakan (atau memiliki administrator yang melampirkannya) atau Anda dapat membuat kebijakan khusus untuk peran yang digunakan.
6. Terakhir, klik Tambahkan hypervisor or Simpan.

Hubungan kepercayaan peran IAM harus dimodifikasi untuk menambahkan layanan backup-gateway.amazonaws.com dan backup.amazonaws.com. Tanpa layanan ini, Anda mungkin akan

mengalami kesalahan saat memetakan tag. Untuk mengedit hubungan kepercayaan untuk peran yang ada,

1. Masuk ke konsol IAM.
2. Di panel navigasi konsol, pilih Peran.
3. Pilih nama peran yang ingin Anda ubah, lalu pilih tab Trust relationship di halaman detail.
4. Di bawah Dokumen Kebijakan, tempel berikut ini:

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

5. Pilih Perbarui Kebijakan Kepercayaan.

Lihat Mengedit hubungan kepercayaan untuk peran yang ada di AWS Directory Service Administration Guide untuk detail selengkapnya.

Lihat pemetaan tag VMware

Di AWS Backup konsol, klik Sumber Daya Eksternal, lalu klik Hypervisor, lalu klik tautan nama Hypervisor untuk melihat properti untuk hypervisor yang dipilih. Di bawah panel ringkasan, ada empat tab, yang terakhir adalah pemetaan tag VMware. Perhatikan jika Anda belum memiliki pemetaan, “Tidak ada pemetaan tag VMware.” akan ditampilkan.

Dari sini, Anda dapat menyinkronkan metadata mesin virtual yang ditemukan oleh hypervisor, Anda dapat menyalin pemetaan ke hypervisor Anda, Anda dapat menambahkan AWS tag yang dipetakan ke tag VMware ke pilihan cadangan rencana cadangan, atau Anda dapat mengelola pemetaan.

Di konsol, untuk melihat tag mana yang diterapkan ke mesin virtual yang dipilih, klik Mesin virtual, lalu nama mesin virtual, lalu AWS tag atau tag VMware. Anda dapat melihat tag yang terkait dengan mesin virtual ini, dan juga Anda dapat mengelola tag.

Tetapkan mesin virtual untuk merencanakan menggunakan pemetaan tag VMware

Untuk menetapkan mesin virtual ke paket cadangan menggunakan tag yang dipetakan, lakukan hal berikut:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di konsol, buka pemetaan tag VMware di halaman detail hypervisor (klik Sumber daya eksternal, lalu klik Hypervisors lalu klik nama hypervisor).
3. Pilih kotak centang di samping beberapa tag yang dipetakan untuk menetapkan tag tersebut ke paket cadangan yang sama.
4. Klik Tambahkan ke penetapan sumber daya.
5. Pilih paket Backup yang ada dari daftar dropdown. Atau, Anda dapat memilih Buat rencana cadangan untuk membuat rencana cadangan baru.
6. Klik Konfirmasi. Ini membuka halaman Tetapkan sumber daya dengan pemilihan Perbaiki menggunakan bidang tag dengan nilai yang telah diisi sebelumnya.

Tag VMware menggunakan AWS CLI

AWS Backup menggunakan panggilan API `PutHypervisorPropertyMappings`untuk memetakan properti entitas hypervisor di on-premise ke properti di. AWS

Dalam AWS CLI, gunakan operasi`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
```

Inilah contohnya:

```
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
```

Anda juga dapat menggunakan GetHypervisorPropertyMappingsuntuk membantu dengan informasi pemetaan properti. Dalam AWS CLI, gunakan operasi`get-hypervisor-property-mappings`. Berikut adalah contoh template:

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

Inilah contohnya:

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Sinkronkan metadata mesin virtual yang ditemukan oleh hypervisor dalam menggunakan AWS API, CLI, atau SDK

Anda dapat menyinkronkan metadata mesin virtual. Ketika Anda melakukannya, tag VMware hadir pada mesin virtual yang merupakan bagian dari pemetaan akan disinkronkan. Selain itu, AWS tag yang dipetakan ke tag VMware yang ada di mesin virtual akan diterapkan ke sumber daya Mesin AWS Virtual.

AWS Backup menggunakan panggilan API StartVirtualMachinesMetadataSyncuntuk menyinkronkan metadata mesin virtual yang ditemukan oleh hypervisor. Untuk menyinkronkan metadata mesin virtual yang ditemukan oleh hypervisor menggunakan AWS CLI, gunakan operasi. `start-virtual-machines-metadata-sync`

Contoh template:

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Contoh:

```
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
```

Anda juga dapat menggunakan `GetHypervisor`untuk membantu informasi hypervisor, seperti host, status, status sinkronisasi metadata terbaru, dan juga untuk mengambil waktu sinkronisasi metadata terakhir yang berhasil. Dalam AWS CLI, gunakan operasi`get-hypervisor`.

Contoh template:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Contoh:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Untuk informasi selengkapnya, lihat dokumentasi API VmwareTagdan VmwareToAwsTagMapping.

Fitur ini akan tersedia di gateway baru yang digunakan setelah 15 Desember 2022. Untuk gateway yang ada, kemampuan baru ini akan tersedia melalui pembaruan perangkat lunak otomatis pada atau sebelum 30 Januari 2023. Untuk memperbarui gateway ke versi terbaru secara manual, gunakan AWS CLI perintah UpdateGatewaySoftwareNow.

Contoh:

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

Menetapkan mesin virtual menggunakan tag

Anda dapat menetapkan mesin virtual Anda yang saat ini ditemukan oleh AWS Backup, bersama dengan AWS Backup sumber daya lain, dengan memberi mereka tag yang telah Anda tetapkan ke salah satu paket cadangan yang ada. Anda juga dapat membuat rencana cadangan baru dan

penetapan sumber daya berbasis tag baru. Rencana cadangan memeriksa sumber daya yang baru ditetapkan setiap kali mereka menjalankan pekerjaan cadangan.

Untuk menandai beberapa mesin virtual dengan tag yang sama:

1. Di panel navigasi kiri, pilih mesin Virtual.
2. Pilih kotak centang di sebelah nama VM untuk memilih semua mesin virtual Anda. Atau, pilih kotak centang di sebelah nama VM yang ingin Anda tag.
3. Pilih Tambahkan tag.
4. Ketik kunci tag.
5. Direkomendasikan: ketik tag Nilai.
6. Pilih Konfirmasi.

Menetapkan mesin virtual menggunakan fitur Tetapkan sumber daya untuk merencanakan

Anda dapat menetapkan mesin virtual yang saat ini ditemukan oleh AWS Backup ke paket cadangan yang ada atau yang baru menggunakan fitur Tetapkan sumber daya ke rencana.

Untuk menetapkan mesin virtual menggunakan fitur Tetapkan sumber daya untuk merencanakan:

1. Di panel navigasi kiri, pilih mesin Virtual.
2. Pilih kotak centang di sebelah nama VM untuk memilih semua mesin virtual Anda. Atau, pilih kotak centang di sebelah beberapa nama VM untuk menetapkannya ke paket cadangan yang sama.
3. Pilih Penugasan, lalu pilih Tetapkan sumber daya untuk direncanakan.
4. Ketik nama tugas Sumber Daya.
5. Pilih peran IAM penugasan sumber daya untuk membuat cadangan dan mengelola titik pemulihan. Jika Anda tidak memiliki peran IAM tertentu untuk digunakan, kami merekomendasikan peran Default yang memiliki izin yang benar.
6. Di bagian Backup plan, pilih paket Backup yang ada dari daftar dropdown. Atau, pilih Buat rencana cadangan untuk membuat rencana cadangan baru.
7. Pilih Tetapkan sumber daya.
8. Opsional: Verifikasi mesin virtual Anda ditetapkan ke paket cadangan dengan memilih Lihat paket Backup. Kemudian, di bagian Penugasan sumber daya, pilih Nama penetapan sumber daya.

Menetapkan mesin virtual menggunakan fitur Create group assignment

Berbeda dengan dua fitur penugasan sumber daya sebelumnya untuk mesin virtual, fitur Create group assignment tidak hanya menetapkan mesin virtual yang saat ini ditemukan oleh AWS Backup, tetapi juga mesin virtual yang ditemukan di masa depan dalam folder atau hypervisor yang Anda tentukan.

Selain itu, Anda tidak perlu memilih kotak centang apa pun untuk menggunakan fitur Buat tugas grup.

Untuk menetapkan mesin virtual menggunakan fitur Tetapkan sumber daya untuk merencanakan:

1. Di panel navigasi kiri, pilih mesin Virtual.
2. Pilih Penugasan, lalu pilih Buat tugas grup.
3. Ketik nama tugas Sumber Daya.
4. Pilih peran IAM penugasan sumber daya untuk membuat cadangan dan mengelola titik pemulihan. Jika Anda tidak memiliki peran IAM tertentu untuk digunakan, kami merekomendasikan peran Default yang memiliki izin yang benar.
5. Di bagian Grup sumber daya, pilih menu tarik-turun Jenis grup. Pilihan Anda adalah Folder atau Hypervisor.

    a. Pilih Folder untuk menetapkan semua mesin virtual dalam folder pada hypervisor. Pilih folder Nama grup, seperti`datacenter/vm`, menggunakan menu tarik-turun. Anda juga dapat memilih untuk menyertakan Subfolder.

    > **Note**
    >
    > Untuk membuat tugas berbasis Folder, selama proses penemuan, beri AWS Backup tag mesin virtual dengan folder tempat mereka menemukannya selama proses penemuan. Jika nanti Anda memindahkan mesin virtual ke folder lain, AWS Backup tidak dapat memperbarui tag untuk Anda karena praktik terbaik AWS penandaan. Metode penugasan ini dapat mengakibatkan terus mengambil cadangan mesin virtual yang Anda pindahkan dari folder yang Anda tetapkan.

    b. Pilih Hypervisor untuk menetapkan semua mesin virtual yang dikelola oleh hypervisor. Pilih nama Grup ID hypervisor menggunakan menu tarik-turun.
6. Di bagian Backup plan, pilih paket Backup yang ada dari daftar dropdown. Atau, pilih Buat rencana cadangan untuk membuat rencana cadangan baru.
7. Pilih Buat tugas grup.

8. Opsional: verifikasi mesin virtual Anda ditetapkan ke paket cadangan dengan memilih Lihat paket Backup. Di bagian Penugasan sumber daya, pilih Nama penetapan sumber daya.

Langkah selanjutnya

Untuk mengembalikan mesin virtual, lihatMemulihkan mesin virtual menggunakan AWS Backup.

Informasi tentang komponen sumber pihak ketiga untuk gateway Backup

Di bagian ini, Anda dapat menemukan informasi tentang alat dan lisensi pihak ketiga yang kami andalkan untuk memberikan fungsionalitas gateway Backup.

Kode sumber untuk komponen perangkat lunak sumber pihak ketiga tertentu yang disertakan dengan perangkat lunak gateway Backup tersedia untuk diunduh di lokasi berikut:

- Untuk gateway yang digunakan di VMware ESXi, unduh sources.tgz.

Produk ini mencakup perangkat lunak yang dikembangkan oleh proyek OpenSSL untuk digunakan dalam OpenSSL Toolkit (https://www.openssl.org/).

Produk ini mencakup perangkat lunak yang dikembangkan oleh VMware® vSphere Software Development Kit (https://www.vmware.com).

Untuk lisensi yang relevan untuk semua alat pihak ketiga yang bergantung, lihat Lisensi Pihak Ketiga.

Komponen sumber terbuka untuk AWS Appliance

Beberapa alat dan lisensi pihak ketiga digunakan untuk memberikan fungsionalitas untuk gateway Backup.

Gunakan tautan berikut untuk mengunduh kode sumber untuk komponen perangkat lunak sumber terbuka tertentu yang disertakan dengan perangkat lunak AWS Appliance:

- Untuk gateway yang digunakan di VMware ESXi, unduh sources.tar

Produk ini mencakup perangkat lunak yang dikembangkan oleh proyek OpenSSL untuk digunakan dalam OpenSSL Toolkit (https://www.openssl.org/). Untuk lisensi yang relevan untuk semua alat pihak ketiga yang bergantung, lihat Lisensi Pihak Ketiga.

Memecahkan masalah VM

Cadangan Inkremental/masalah CBT dan pesan

Pesan kegagalan: **`"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."`**

Jika pesan ini berlanjut, setel ulang CBT seperti yang diarahkan oleh VMware.

Catatan pesan CBT tidak diaktifkan atau tidak tersedia: “VMware Change Block Tracking (CBT) tidak tersedia untuk mesin virtual ini, tetapi pencadangan tambahan berhasil diselesaikan dengan mekanisme perubahan eksklusif kami.”

Periksa untuk memastikan CBT dihidupkan. Untuk memverifikasi apakah disk virtual telah mengaktifkan CBT:

1. Buka Klien vSphere dan pilih mesin virtual yang dimatikan.
2. Klik kanan mesin virtual dan arahkan ke Edit Settings > Options > Advanced/General > Configuration Parameters.
3. Opsi `ctkEnabled` harus sama`True`.

Jika dihidupkan, pastikan Anda menggunakan fitur up-to-date VMware. Host harus ESXi 4.0 atau yang lebih baru dan mesin virtual yang memiliki disk yang akan dilacak harus perangkat keras versi 7 atau yang lebih baru.

Jika CBT dihidupkan (diaktifkan) dan perangkat lunak dan perangkat keras diperbarui, matikan mesin virtual dan kemudian hidupkan kembali. Pastikan CBT dihidupkan. Kemudian, lakukan pencadangan lagi.

Cadangan DynamoDB tingkat lanjut

AWS Backup mendukung fitur tambahan dan canggih untuk kebutuhan perlindungan data Amazon DynamoDB Anda. Setelah Anda mengaktifkan AWS Backup fitur-fitur canggih di Anda Wilayah AWS, Anda membuka fitur berikut untuk semua cadangan tabel DynamoDB baru yang Anda buat:

- Penghematan biaya dan optimalisasi:
  - Tiering backup ke cold storage untuk mengurangi biaya penyimpanan
  - Penandaan alokasi biaya untuk digunakan dengan Cost Explorer

- Kelangsungan bisnis:
  - Salinan Lintas Wilayah
  - Salinan lintas akun
- Keamanan:
  - Simpan cadangan di brankas terenkripsi, yang dapat Anda amankan dengan AWS BackupAWS Backup VaultLock, kebijakan, dan kunci enkripsi.AWS Backup
  - Cadangan mewarisi tag dari tabel DynamoDB sumbernya, memungkinkan Anda menggunakan tag tersebut untuk mengatur izin dan kebijakan kontrol layanan (SCP).

Pelanggan baru yang melakukan onboarding AWS Backup setelah November 2021 mengaktifkan fitur cadangan DynamoDB lanjutan secara default. Secara khusus, fitur cadangan DynamoDB lanjutan diaktifkan secara default untuk pelanggan yang belum membuat brankas cadangan sebelum 21 November 2021.

Kami merekomendasikan semua AWS Backup pelanggan yang ada mengaktifkan fitur-fitur canggih untuk DynamoDB. Tidak ada perbedaan dalam harga penyimpanan cadangan hangat setelah Anda mengaktifkan fitur-fitur canggih. Anda dapat menghemat uang dengan meningkatkan cadangan ke penyimpanan dingin dan mengoptimalkan biaya Anda dengan menggunakan tag alokasi biaya. Anda juga dapat mulai memanfaatkan AWS Backup kelangsungan bisnis dan fitur keamanan.

> **Note**
>
> Jika Anda menggunakan peran atau kebijakan kustom alih-alih AWS Backup peran layanan default, Anda harus menambahkan atau menggunakan kebijakan izin berikut (atau menambahkan izin yang setara) ke peran kustom Anda:
>
> - `AWSBackupServiceRolePolicyForBackup`untuk melakukan backup DynamoDB lanjutan.
> - `AWSBackupServiceRolePolicyForRestores`untuk mengembalikan cadangan DynamoDB tingkat lanjut.
>
> Untuk mempelajari selengkapnya tentang kebijakan yang AWS dikelola dan melihat contoh kebijakan yang dikelola pelanggan, lihat. Kebijakan terkelola untuk AWS Backup

Topik

- Mengaktifkan cadangan DynamoDB lanjutan menggunakan konsol
- Mengaktifkan cadangan DynamoDB lanjutan secara terprogram
- Mengedit cadangan DynamoDB tingkat lanjut
- Memulihkan cadangan DynamoDB tingkat lanjut
- Menghapus cadangan DynamoDB lanjutan
- Manfaat lain dari AWS Backup manajemen penuh saat Anda mengaktifkan cadangan DynamoDB tingkat lanjut

Mengaktifkan cadangan DynamoDB lanjutan menggunakan konsol

Anda dapat mengaktifkan fitur-fitur AWS Backup lanjutan untuk backup DynamoDB menggunakan konsol atau DynamoDB. AWS Backup

Untuk mengaktifkan fitur cadangan DynamoDB lanjutan dari konsol: AWS Backup

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di menu navigasi kiri, pilih Pengaturan.
3. Di bawah bagian Layanan yang didukung, verifikasi bahwa DynamoDB Diaktifkan.

   Jika tidak, pilih Opt-in dan aktifkan DynamoDB sebagai layanan yang didukung. AWS Backup
4. Di bawah bagian Advanced features for DynamoDB backup, pilih Enable.
5. Pilih Aktifkan fitur.

Untuk cara mengaktifkan fitur AWS Backup lanjutan menggunakan konsol DynamoDB, lihat AWS Backup Mengaktifkan fitur di Panduan Pengguna Amazon DynamoDB.

Mengaktifkan cadangan DynamoDB lanjutan secara terprogram

Anda juga dapat mengaktifkan fitur-fitur AWS Backup canggih untuk backup DynamoDB menggunakan AWS Command Line Interface (CLI). Anda mengaktifkan cadangan DynamoDB lanjutan saat Anda menetapkan kedua nilai berikut ke: `true`

Untuk mengaktifkan fitur-fitur AWS Backup lanjutan secara terprogram untuk backup DynamoDB:

1. Periksa apakah Anda sudah mengaktifkan fitur AWS Backup lanjutan untuk DynamoDB menggunakan perintah berikut:

```
$ aws backup describe-region-settings
```

Jika `"DynamoDB":true` di bawah keduanya `"ResourceTypeManagementPreference"` dan`"ResourceTypeOptInPreference"`, Anda telah mengaktifkan cadangan DynamoDB lanjutan.

Jika, seperti output berikut, Anda memiliki setidaknya satu contoh`"DynamoDB":false`, Anda belum mengaktifkan cadangan DynamoDB lanjutan, lanjutkan ke langkah berikutnya.

```
{
  "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. Gunakan UpdateRegionSettingsoperasi berikut untuk mengatur keduanya `"ResourceTypeManagementPreference"` dan `"ResourceTypeOptInPreference"` ke`"DynamoDB":true`:

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

Mengedit cadangan DynamoDB tingkat lanjut

Saat Anda membuat cadangan DynamoDB setelah AWS Backup mengaktifkan fitur-fitur lanjutan, Anda dapat menggunakan untuk: AWS Backup

- Salin cadangan di seluruh Wilayah
- Salin cadangan di seluruh akun
- Ubah saat AWS Backup tingkatan cadangan ke cold storage
- Tandai cadangan

Untuk menggunakan fitur-fitur canggih tersebut pada cadangan yang ada, lihat Mengedit cadangan.

Jika nanti Anda menonaktifkan fitur AWS Backup lanjutan untuk DynamoDB, Anda dapat terus melakukan operasi tersebut ke backup DynamoDB yang Anda buat selama periode waktu ketika Anda mengaktifkan fitur lanjutan.

Memulihkan cadangan DynamoDB tingkat lanjut

Anda dapat memulihkan cadangan DynamoDB yang diambil AWS Backup dengan fitur-fitur canggih yang diaktifkan dengan cara yang sama seperti Anda memulihkan cadangan DynamoDB yang diambil sebelum mengaktifkan fitur-fitur canggih. AWS Backup Anda dapat melakukan pemulihan menggunakan salah satu AWS Backup atau DynamoDB.

Anda dapat menentukan cara mengenkripsi tabel yang baru dipulihkan dengan opsi berikut:

- Saat memulihkan di Wilayah yang sama dengan tabel asli, Anda dapat menentukan kunci enkripsi untuk tabel yang dipulihkan secara opsional. Jika Anda tidak menentukan kunci enkripsi, secara otomatis AWS Backup akan mengenkripsi tabel dipulihkan Anda menggunakan kunci yang sama yang mengenkripsi tabel asli Anda.
- Ketika Anda memulihkan di Wilayah yang berbeda dari tabel asli Anda, Anda harus menentukan kunci enkripsi.

Untuk memulihkan penggunaan AWS Backup, lihatMemulihkan tabel Amazon DynamoDB.

Untuk memulihkan menggunakan DynamoDB, lihat Memulihkan tabel DynamoDB dari cadangan di Panduan Pengguna Amazon DynamoDB.

Menghapus cadangan DynamoDB lanjutan

Anda tidak dapat menghapus cadangan yang dibuat menggunakan fitur-fitur canggih ini di DynamoDB. Anda harus menggunakan AWS Backup untuk menghapus cadangan untuk menjaga konsistensi global di seluruh lingkungan Anda AWS .

Untuk menghapus cadangan DynamoDB, lihat. Menghapus cadangan

Manfaat lain dari AWS Backup manajemen penuh saat Anda mengaktifkan cadangan DynamoDB tingkat lanjut

Saat Anda mengaktifkan fitur AWS Backup lanjutan untuk DynamoDB, Anda memberikan manajemen penuh cadangan DynamoDB Anda. AWS Backup Melakukannya memberi Anda manfaat tambahan berikut:

Enkripsi

AWS Backup secara otomatis mengenkripsi cadangan dengan kunci KMS dari brankas tujuan Anda. AWS Backup Sebelumnya, mereka dienkripsi menggunakan metode enkripsi yang sama dari tabel DynamoDB sumber Anda. Ini meningkatkan jumlah pertahanan yang dapat Anda gunakan untuk melindungi data Anda. Untuk informasi selengkapnya, lihat Enkripsi untuk backup di AWS Backup.

Nama Sumber Daya Amazon (ARN)

Setiap namespace layanan ARN cadangan adalah. `awsbackup` Sebelumnya, namespace layanan adalah. `dynamodb` Dengan kata lain, awal setiap ARN akan berubah dari `arn:aws:dynamodb` ke. `arn:aws:backup` Lihat ARN untuk AWS Backup di Referensi Otorisasi Layanan.

Dengan perubahan ini, Anda atau administrator cadangan Anda dapat membuat kebijakan akses untuk backup menggunakan namespace `awsbackup` layanan yang sekarang berlaku untuk backup DynamoDB yang dibuat setelah Anda mengaktifkan fitur lanjutan. Dengan menggunakan namespace `awsbackup` layanan, Anda juga dapat menerapkan kebijakan ke cadangan lain yang diambil. AWS Backup Untuk informasi selengkapnya, lihat Pengendalian akses.

Lokasi biaya pada laporan penagihan

Biaya untuk backup (termasuk penyimpanan, transfer data, pemulihan, dan penghapusan awal) muncul di bawah “Backup” di tagihan Anda. AWS Sebelumnya, tagihan muncul di bawah “DynamoDB” di tagihan Anda.

Perubahan ini memastikan bahwa Anda dapat menggunakan AWS Backup penagihan untuk memantau biaya cadangan Anda secara terpusat. Untuk informasi selengkapnya, lihat Pengukuran, biaya, dan penagihan.

Pencadangan Amazon Timestream

Amazon Timestream adalah database deret waktu yang dapat diskalakan yang memungkinkan penyimpanan dan analisis hingga triliunan titik data deret waktu setiap hari. Timestream dioptimalkan untuk menghemat biaya dan waktu dengan menyimpan data terbaru dalam memori dan dengan menyimpan data historis dalam tingkat penyimpanan yang dioptimalkan biaya sesuai dengan kebijakan Anda.

Database Timestream memiliki tabel. Tabel ini berisi catatan, dan setiap catatan adalah titik data tunggal dalam deret waktu. Deret waktu adalah urutan catatan yang direkam selama interval waktu, seperti harga saham, tingkat penggunaan memori instans Amazon EC2, atau pembacaan suhu. AWS Backup dapat membuat cadangan dan memulihkan tabel Timestream secara terpusat. Anda dapat menyalin cadangan tabel ini ke akun lain dan beberapa lainnya Wilayah AWS dalam organisasi yang sama.

Timestream saat ini tidak menawarkan layanan pencadangan dan pemulihan asli, jadi menggunakan AWS Backup untuk membuat salinan aman tabel Timestream Anda dapat menambahkan lapisan keamanan dan ketahanan ekstra ke sumber daya Anda.

Cadangkan tabel Timestream

Anda dapat mencadangkan tabel Timestream baik melalui AWS Backup konsol atau menggunakan. AWS CLI

Ada dua cara untuk menggunakan AWS Backup konsol untuk mencadangkan tabel Timestream: sesuai permintaan atau sebagai bagian dari rencana cadangan.

Buat cadangan Timestream sesuai permintaan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Menggunakan panel navigasi, pilih Sumber daya yang dilindungi, lalu Buat cadangan sesuai permintaan.
3. Pada halaman Buat cadangan sesuai permintaan, pilih Amazon Timestream.
4. Pilih Jenis sumber daya Timestream, lalu pilih nama tabel yang ingin Anda cadangkan.

5. Di jendela Backup, pastikan bahwa Buat cadangan sekarang dipilih. Ini segera memulai pencadangan dan memungkinkan Anda melihat klaster Anda lebih cepat di halaman Sumber daya yang dilindungi.
6. Di menu tarik-turun Transisi ke penyimpanan dingin, Anda dapat mengatur pengaturan transisi Anda.
7. Di Periode Retensi, Anda dapat memilih berapa lama untuk menyimpan cadangan Anda.
8. Pilih brankas cadangan yang ada atau buat brankas cadangan baru. Memilih Buat brankas cadangan baru membuka halaman baru untuk membuat brankas dan kemudian mengembalikan Anda ke halaman Buat cadangan sesuai permintaan setelah Anda selesai.
9. Di bawah peran IAM, pilih Peran AWS Backup default (jika peran default tidak ada di akun Anda, itu akan dibuat untuk Anda dengan izin yang benar).
10. Secara opsional, tag dapat ditambahkan ke titik pemulihan Anda. Jika Anda ingin menetapkan satu atau beberapa tag ke cadangan sesuai permintaan, masukkan kunci dan nilai opsional, lalu pilih Tambah tag.
11. Pilih Buat cadangan sesuai permintaan. Ini membawa Anda ke halaman Pekerjaan, di mana Anda akan melihat daftar pekerjaan.
12. Pilih ID pekerjaan Backup untuk klaster untuk melihat detail pekerjaan itu. Ini akan menampilkan status`Completed`,`In Progress`, atau`Failed`. Anda dapat mengklik tombol refresh untuk memperbarui status yang ditampilkan.

Buat cadangan Timestream terjadwal dalam rencana cadangan

Pencadangan terjadwal Anda dapat menyertakan tabel Timestream jika merupakan sumber daya yang dilindungi. Untuk memilih untuk melindungi tabel Amazon Timestream:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Menggunakan panel navigasi, pilih Sumber daya yang dilindungi.
3. Alihkan Amazon Timestream ke Aktif.
4. Lihat Menetapkan sumber daya ke konsol untuk menyertakan tabel Timestream dalam paket yang sudah ada atau yang baru.

Di bawah Kelola paket Backup, Anda dapat memilih untuk membuat rencana cadangan dan menyertakan tabel Timestream, atau Anda dapat memperbarui yang sudah ada untuk menyertakan tabel Timestream. Saat menambahkan tipe sumber daya Timestream, Anda dapat memilih untuk

menambahkan semua tabel Timestream, atau centang kotak di sebelah tabel yang ingin Anda tambahkan di bawah Pilih jenis sumber daya tertentu.

Cadangan pertama yang terbuat dari tabel Timestream akan menjadi cadangan penuh. Backup selanjutnya akan menjadi backup tambahan.

Setelah Anda membuat atau memodifikasi paket cadangan, navigasikan ke Paket Backup di navigasi kiri. Rencana cadangan yang Anda tentukan harus menampilkan kluster Anda di bawah Penugasan Sumber Daya.

Mencadangkan secara terprogram

Anda dapat menggunakan nama operasi`start-backup-job`. Sertakan parameter berikut:

```
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 Wilayah AWS \
--endpoint-url URL
```

Lihat cadangan tabel Timestream

Untuk melihat dan memodifikasi cadangan tabel Timestream Anda di dalam konsol:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pilih Brankas Cadangan. Kemudian, klik pada nama brankas cadangan yang berisi tabel Timestream Anda.
3. Brankas cadangan akan menampilkan ringkasan dan daftar cadangan.
    a. Anda dapat mengklik tautan di kolom ID titik pemulihan, atau
    b. Anda dapat mencentang kotak di sebelah kiri ID titik pemulihan dan klik Tindakan untuk menghapus titik pemulihan yang tidak lagi diperlukan.

Mengembalikan tabel Timestream

Lihat cara mengembalikan tabel Timestream

Database SAP HANA di Amazon EC2 membuat cadangan instans

> **Note**
>
> Layanan yang didukung oleh Wilayah AWSberisi Wilayah yang saat ini didukung di mana cadangan basis data SAP HANA di instans Amazon EC2 tersedia.

AWS Backup mendukung backup dan mengembalikan database SAP HANA pada instans Amazon EC2.

Topik

Ikhtisar database SAP HANA dengan AWS Backup

Selain kemampuan untuk membuat backup dan memulihkan database, AWS Backup integrasi dengan Amazon EC2 Systems Manager untuk SAP memungkinkan pelanggan untuk mengidentifikasi dan menandai database SAP HANA.

AWS Backup terintegrasi dengan AWS Backint Agent untuk melakukan backup dan pemulihan SAP HANA. Untuk informasi lebih lanjut, lihat AWS Backint.

Prasyarat untuk mencadangkan database SAP HANA melalui AWS Backup

Beberapa prasyarat harus diselesaikan sebelum aktivitas pencadangan dan pemulihan dapat dilakukan. Catatan Anda akan memerlukan akses administratif ke database SAP HANA Anda dan izin untuk membuat peran dan kebijakan IAM baru di AWS akun Anda untuk melakukan langkah-langkah ini.

Lengkapi prasyarat ini di Amazon EC2 Systems Manager.

1. Menyiapkan izin yang diperlukan untuk instans Amazon EC2 yang menjalankan database SAP HANA
2. Daftarkan kredensi di AWS Secrets Manager
3. Instal AWS Backint dan AWS Systems Manager untuk Agen SAP
4. Verifikasi Agen SSM
5. Verifikasi parameter
6. Daftarkan database SAP HANA

Ini adalah praktik terbaik untuk mendaftarkan setiap instance HANA hanya sekali. Beberapa pendaftaran dapat menghasilkan beberapa ARN untuk database yang sama. Mempertahankan ARN tunggal dan pendaftaran menyederhanakan pembuatan dan pemeliharaan rencana cadangan dan juga dapat membantu mengurangi duplikasi cadangan yang tidak direncanakan.

Operasi cadangan SAP HANA di konsol AWS Backup

Setelah prasyarat dan SSM untuk setup SAP selesai, Anda dapat mencadangkan dan memulihkan SAP HANA Anda pada database EC2.

Pilih untuk melindungi sumber daya SAP HANA

Untuk digunakan AWS Backup untuk melindungi database SAP HANA Anda, SAP HANA harus diaktifkan sebagai salah satu sumber daya yang dilindungi. Untuk ikut serta:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Di bawah Keikutsertaan layanan, pilih Konfigurasi sumber daya.
4. Pilih SAP HANA di Amazon EC2. .
5. Klik Konfirmasi.

Layanan opt-in untuk SAP HANA di Amazon EC2 sekarang akan diaktifkan.

Buat cadangan terjadwal dari database SAP HANA

Anda dapat mengedit rencana cadangan yang ada dan menambahkan sumber daya SAP HANA ke dalamnya, atau Anda dapat membuat rencana cadangan baru hanya untuk sumber daya SAP HANA.

Jika Anda memilih untuk membuat rencana cadangan baru, Anda akan memiliki tiga opsi:

1. Opsi 1: Mulailah dengan templat
    1. Pilih templat rencana cadangan.
    2. Tentukan nama rencana cadangan.
    3. Klik Buat rencana.
2. Opsi 2: Bangun rencana baru
    1. Tentukan nama rencana cadangan.
    2. Secara opsional menentukan tag untuk ditambahkan ke rencana cadangan.
    3. Tentukan konfigurasi aturan cadangan.
        a. Tentukan nama aturan cadangan.
        b. Pilih brankas yang ada atau buat brankas cadangan baru. Di sinilah cadangan Anda disimpan.
        c. Tentukan frekuensi cadangan.
        d. Tentukan jendela cadangan.

            Catatan transisi ke penyimpanan dingin saat ini tidak didukung.
        e. Tentukan periode retensi.

            Salin ke tujuan saat ini tidak didukung
        f. (Opsional) Tentukan tag untuk ditambahkan ke titik pemulihan.
    4. Klik Buat rencana.
3. Opsi 3: Tentukan rencana menggunakan JSON
    1. Tentukan JSON untuk rencana cadangan Anda dengan memodifikasi ekspresi JSON dari rencana cadangan yang ada atau membuat ekspresi baru.
    2. Tentukan nama rencana cadangan.
    3. Klik Validasi JSON.

Setelah rencana cadangan berhasil dibuat, Anda dapat menetapkan sumber daya ke rencana cadangan di langkah berikutnya.

Paket apa pun yang Anda gunakan, pastikan Anda menetapkan sumber daya. Anda dapat memilih database SAP HANA mana yang akan ditetapkan, termasuk database sistem dan penyewa. Anda juga memiliki opsi untuk mengecualikan ID sumber daya tertentu.

Buat cadangan basis data SAP HANA sesuai permintaan

Anda dapat membuat cadangan sesuai permintaan penuh yang berjalan segera setelah pembuatan. Perhatikan bahwa cadangan berdasarkan permintaan database SAP HANA di instans Amazon EC2 adalah cadangan penuh; cadangan tambahan tidak didukung.

Cadangan sesuai permintaan Anda sekarang dibuat. Ini akan mulai mencadangkan sumber daya yang Anda tentukan. Konsol akan mentransisikan Anda ke halaman Backup jobs di mana Anda dapat melihat kemajuan pekerjaan. Catat ID pekerjaan cadangan dari spanduk biru di bagian atas layar Anda, karena Anda akan membutuhkannya untuk dengan mudah menemukan status pekerjaan cadangan Anda. Ketika cadangan selesai, status akan berlanjut ke`Completed`. Pencadangan dapat memakan waktu hingga beberapa jam.

Segarkan daftar pekerjaan Backup untuk melihat perubahan status. Anda juga dapat mencari dan mengklik ID pekerjaan cadangan Anda untuk melihat status pekerjaan terperinci.

Pencadangan berkelanjutan dari database SAP HANA

Anda dapat membuat backup berkelanjutan, yang dapat digunakan dengan point-in-time restore (PITR) (perhatikan bahwa on-demand backup menyimpan sumber daya dalam keadaan di mana mereka diambil; sedangkan PITR menggunakan backup berkelanjutan yang mencatat perubahan selama periode waktu tertentu).

Dengan pencadangan berkelanjutan, Anda dapat memulihkan database SAP HANA Anda pada instans EC2 dengan memutarnya kembali ke waktu tertentu yang Anda pilih, dalam waktu 1 detik presisi (kembali maksimal 35 hari). Pencadangan berkelanjutan bekerja dengan terlebih dahulu membuat cadangan penuh sumber daya Anda, dan kemudian terus-menerus mencadangkan log transaksi sumber daya Anda. PITR restore bekerja dengan mengakses cadangan penuh Anda dan memutar ulang log transaksi ke waktu yang Anda minta AWS Backup untuk memulihkan.

Anda dapat ikut serta dalam pencadangan berkelanjutan saat membuat paket cadangan AWS Backup menggunakan AWS Backup konsol atau API.

Untuk mengaktifkan pencadangan berkelanjutan menggunakan konsol

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.

2. Di panel navigasi, pilih Backup plan, lalu pilih Buat paket Backup.
3. Di bawah Aturan Backup, pilih Aturan Tambahkan Cadangan.
4. Di bagian Konfigurasi aturan Backup, pilih Aktifkan pencadangan berkelanjutan untuk sumber daya yang didukung.

Setelah Anda menonaktifkan PITR (point-in-timerestore) untuk backup database SAP HANA, log akan terus dikirim AWS Backup sampai titik pemulihan berakhir (status sama. `EXPIRED`) Anda dapat mengubah ke lokasi cadangan log alternatif di SAP HANA untuk menghentikan transmisi log ke AWS Backup.

Titik pemulihan berkelanjutan dengan status `STOPPED` menunjukkan bahwa titik pemulihan berkelanjutan telah terputus; yaitu, log yang ditransmisikan dari SAP HANA ke AWS Backup yang menunjukkan perubahan tambahan ke database memiliki celah. Titik pemulihan yang terjadi dalam jeda jangka waktu ini memiliki status. `STOPPED`.

Untuk masalah yang mungkin Anda temui selama memulihkan pekerjaan pencadangan berkelanjutan (titik pemulihan), lihat bagian pemecahan masalah SAP HANA Restore dari panduan ini.

Lihat cadangan basis data SAP HANA

Lihat status pekerjaan pencadangan dan pemulihan:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Tugas.
3. Pilih pekerjaan cadangan, pulihkan pekerjaan, atau salin pekerjaan untuk melihat daftar pekerjaan Anda.
4. Cari dan klik ID pekerjaan Anda untuk melihat status pekerjaan terperinci.

Lihat semua titik pemulihan di brankas:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Cari dan klik brankas cadangan untuk melihat semua titik pemulihan di dalam brankas.

Lihat detail sumber daya yang dilindungi:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.

2. Di panel navigasi, pilih Sumber daya yang dilindungi.
3. Anda juga dapat memfilter berdasarkan jenis sumber daya untuk melihat semua cadangan dari jenis sumber daya tersebut.

Gunakan AWS CLI untuk database SAP HANA dengan AWS Backup

Setiap tindakan dalam konsol Backup memiliki panggilan API yang sesuai.

Untuk mengonfigurasi dan mengelola AWS Backup dan sumber dayanya secara terprogram, gunakan panggilan API `StartBackupJob`untuk membuat cadangan database SAP HANA pada instans EC2.

Gunakan `start-backup-job` sebagai perintah CLI.

Memecahkan masalah backup database SAP HANA

Jika Anda menemukan kesalahan selama alur kerja Anda, lihat contoh kesalahan berikut dan resolusi yang disarankan:

Prasyarat Python

- Kesalahan: Kesalahan Zypper terkait dengan versi Python sejak SSM untuk SAP dan memerlukan Python 3.6 tetapi SUSE 12 SP5 secara default mendukung AWS Backup Python 3.4.

  Resolusi: Instal beberapa versi Python pada SUSE12 SP5 dengan melakukan langkah-langkah berikut:

  1. Jalankan perintah update-alternative untuk membuat symlink untuk Python 3 di '/usr/local/bin/' alih-alih langsung menggunakan '/usr/bin/python3'. Perintah ini akan menetapkan Python 3.4 sebagai versi default. Perintahnya adalah: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.4 5`
  2. Tambahkan Python 3.6 ke konfigurasi alternatif dengan menjalankan perintah berikut: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
  3. Ubah konfigurasi alternatif ke Python 3.6 dengan menjalankan perintah berikut: `# sudo update-alternatives –config python3`

     Output berikut harus ditampilkan:

     ```
     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. Masukkan nomor yang sesuai dengan Python 3.6.
5. Periksa versi Python dan konfirmasikan Python 3.6 sedang digunakan.
6. (Opsional, tetapi disarankan) Verifikasi perintah Zypper berfungsi seperti yang diharapkan.

Amazon EC2 Systems Manager untuk penemuan dan pendaftaran SAP

- Kesalahan: SSM untuk SAP gagal menemukan beban kerja karena akses yang diblokir ke titik akhir publik untuk dan SSM. AWS Secrets Manager

  Resolusi: Uji apakah titik akhir dapat dijangkau dari database SAP HANA Anda. Jika tidak dapat dijangkau, Anda dapat membuat titik akhir Amazon VPC untuk AWS Secrets Manager dan SSM untuk SAP.

  1. Uji akses ke Secrets Manager dari host Amazon EC2 untuk HANA DB dengan menjalankan perintah berikut:. `aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp` Jika perintah gagal mengembalikan nilai, firewall memblokir akses ke titik akhir layanan Secrets Manager. Log akan berhenti pada langkah “Mengambil rahasia dari Secrets Manager”.
  2. Uji konektivitas ke SSM untuk titik akhir SAP dengan menjalankan perintah. `aws ssm-sap list-registration` Jika perintah gagal mengembalikan nilai, firewall memblokir akses ke SSM untuk titik akhir SAP.

     Contoh kesalahan:`Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application"`.

  Ada dua opsi untuk melanjutkan jika titik akhir tidak dapat dijangkau.

  - Buka port firewall untuk memungkinkan akses ke titik akhir layanan publik untuk Secrets Manager dan SSM untuk SAP; atau,
  - Buat endpoint VPC untuk Secrets Manager dan SSM untuk SAP, lalu:
    - Pastikan Amazon VPC diaktifkan untuk DNSSupport dan DNShostName.
    - Pastikan titik akhir VPC Anda telah mengaktifkan Izinkan Nama DNS Pribadi.

    - Jika SSM untuk penemuan SAP berhasil diselesaikan, log akan menunjukkan host ditemukan.
- Kesalahan: AWS Backup dan koneksi Backint gagal karena akses yang diblokir ke titik akhir publik AWS Backup layanan. `aws-backint-agent.log`dapat menunjukkan kesalahan yang mirip dengan ini: `time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id"` atau`level=fatal msg="Error performing backup missing backup data plane Id`. Selain itu, AWS Backup konsol dapat menampilkan `Fatal Error: An internal error occured.`

  Resolusi: Ada dua opsi untuk melanjutkan jika titik akhir tidak dapat dijangkau:

  - Buka port firewall untuk memungkinkan akses ke titik akhir layanan publik (HTTPS). Setelah opsi ini digunakan, DNS akan menyelesaikan permintaan ke AWS layanan melalui alamat IP publik.
  - Buat titik akhir VPC secara pribadi merutekan lalu lintas ke dan dari AWS layanan yang diperlukan untuk. AWS Backup Setelah opsi ini digunakan, DNS akan menyelesaikan permintaan untuk layanan tersebut melalui alamat IP pribadi. Opsi ini mungkin memerlukan pembaruan ke server DNS untuk menambahkan aturan untuk meneruskan permintaan ke titik akhir pribadi.
- Kesalahan: SSM untuk pendaftaran SAP gagal karena kata sandi HANA yang mengandung karakter khusus. Contoh kesalahan dapat mencakup `Error connecting to database HBX/HBX when validating its credentials.` atau `Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.` setelah menguji koneksi menggunakan `hdbsql` for `systemdb` dan `tenantdb` yang telah diuji dari database HANA Amazon EC2 instans.

  Di AWS Backup konsol di halaman Pekerjaan, detail pekerjaan cadangan dapat menampilkan status `FAILED` dengan kesalahan`Miscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’`.

  Resolusi: Pastikan kata sandi Anda tidak memiliki karakter khusus, seperti $.
- Kesalahan: **`b’* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  Resolusi: AWS BackInt Agen untuk instalasi SAP HANA mungkin tidak berhasil diselesaikan. Coba lagi proses untuk menyebarkan Backint AWS Agent dan Amazon EC2 Systems Manager Agent di server aplikasi SAP Anda.
- Kesalahan: Konsol tidak cocok dengan file log setelah pendaftaran.

Log penemuan menunjukkan pendaftaran yang gagal ketika mencoba terhubung ke HANA DB karena kata sandi yang mengandung karakter khusus, meskipun SSM untuk SAP Application Manager untuk konsol SAP menampilkan pendaftaran yang berhasil. itu tidak mengkonfirmasi bahwa pendaftaran berhasil. Jika konsol menunjukkan pendaftaran yang berhasil tetapi log tidak, cadangan akan gagal.

Konfirmasikan status pendaftaran:

1. Masuk ke konsol SSM
2. Pilih Run Command dari navigasi sisi kiri.
3. Di bawah bidang teks Riwayat perintah`Instance ID:Equal:`, masukan, dengan nilai yang sama dengan instance yang Anda gunakan untuk pendaftaran. Ini akan memfilter riwayat perintah.
4. Gunakan kolom id perintah untuk menemukan perintah dengan status`Failed`. Kemudian, cari nama dokumen AWSSystemsManagerSAP-Discovery.
5. Di AWS CLI, jalankan perintah`aws ssm-sap register-application status`. Jika nilai yang dikembalikan menunjukkan`Error`, pendaftaran tidak berhasil.

Resolusi: Pastikan password HANA Anda tidak memiliki karakter khusus (seperti '$').

Membuat cadangan database SAP HANA

- Kesalahan: AWS Backup konsol menampilkan pesan “Kesalahan Fatal” ketika cadangan sesuai permintaan untuk SystemDB atau TenantDB dibuat. Hal ini terjadi karena titik akhir publik cell-1.prod.us-west-2.storage.cryo.aws.a2z.com tidak dapat diakses. Ini disebabkan oleh firewall sisi klien yang memblokir akses ke titik akhir ini.

  `aws-backint-agent.log`dapat menunjukkan kesalahan seperti `level=error msg="Storage configuration validation failed: missing backup data plane Id"` atau `level=fatal msg="Error performing backup missing backup data plane Id."`

  Resolusi: Buka akses firewall ke titik akhir publik cell-1.prod.us-west-2.storage.cryo.aws.a2z.com.
- Kesalahan:`Database cannot be backed up while it is stopped`.

  Resolusi: Pastikan database yang akan dicadangkan aktif. Database data dan log dapat dicadangkan hanya saat database sedang online.

- Kesalahan: `Getting backup metadata failed. Check the SSM document execution for more details.`

  Resolusi: Pastikan database yang akan dicadangkan aktif. Database data dan log dapat dicadangkan hanya saat database sedang online.

Memantau log cadangan

- Kesalahan: `Encountered an issue with log backups, please check SAP HANA for details.`

  Resolusi: Periksa SAP HANA untuk memastikan cadangan log dikirim AWS Backup dari SAP HANA.
- Kesalahan: `One or more log backup attempts failed for recovery point.`

  Resolusi: Periksa SAP HANA untuk detailnya. Pastikan backup log dikirim AWS Backup dari SAP HANA.
- Kesalahan: `Unable to determine the status of log backups for recovery point.`

  Resolusi: Periksa SAP HANA untuk detailnya. Pastikan backup log dikirim AWS Backup dari SAP HANA.
- Kesalahan: `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

  Resolusi: Tunggu sampai pekerjaan pemulihan selesai. Pencadangan log harus dilanjutkan.

Glosarium istilah SAP HANA saat menggunakan AWS Backup

Jenis Backup Data: SAP HANA mendukung dua jenis backup data: Full dan INC (incremental). AWS Backup mengoptimalkan jenis yang digunakan selama setiap operasi pencadangan.

Cadangan Katalog: SAP HANA mempertahankan manifesnya sendiri yang disebut katalog. AWS Backup berinteraksi dengan katalog ini. Setiap cadangan baru akan membuat entri dalam katalog.

Continuous Log Backup (Transaction Logs): Untuk fungsi Point in Time Recovery (PITR), SAP HANA melacak semua transaksi sejak backup terbaru.

System Copy: Pekerjaan pemulihan di mana database target pemulihan berbeda dari database sumber tempat titik pemulihan dibuat.

Destructive Restore: Restore destruktif adalah jenis pekerjaan pemulihan di mana database dipulihkan menghapus atau menimpa sumber atau database yang ada.

FULL: Full backup adalah backup dari database yang lengkap.

INC: Cadangan tambahan adalah cadangan dari semua perubahan pada database SAP HANA sejak cadangan sebelumnya.

Untuk detail tambahan, lihat AWS glosarium.

AWS Backup dukungan database SAP HANA pada catatan rilis instans EC2

Fungsionalitas tertentu tidak didukung saat ini:

- Penyalinan lintas wilayah dan lintas akun saat ini tidak didukung.
- Backup Audit Manager dan pelaporan saat ini tidak didukung.
- Layanan yang didukung oleh Wilayah AWSberisi Wilayah yang saat ini didukung untuk backup database SAP HANA di instans Amazon EC2.

Cadangan Amazon Redshift

Amazon Redshift adalah gudang data cloud yang terkelola sepenuhnya dan dapat diskalakan yang mempercepat waktu Anda menuju wawasan dengan analitik yang cepat, mudah, dan aman. Anda dapat menggunakan AWS Backup untuk melindungi gudang data Anda dengan cadangan yang tidak dapat diubah, kebijakan akses terpisah, dan tata kelola organisasi terpusat untuk pencadangan dan pemulihan pekerjaan.

Gudang data Amazon Redshift adalah kumpulan sumber daya komputasi yang disebut node, yang diatur ke dalam grup yang disebut cluster. AWS Backup dapat membuat cadangan cluster ini.

Untuk informasi tentang Amazon Redshift, lihat Panduan Memulai Amazon Redshift, Panduan Pengembang Database Amazon Redshift, dan Panduan Manajemen Cluster Amazon Redshift.

Cadangkan cluster yang disediakan Amazon Redshift

Anda dapat melindungi kluster Amazon Redshift menggunakan AWS Backup konsol atau secara terprogram menggunakan API atau CLI. Cluster ini dapat dicadangkan pada jadwal reguler sebagai

bagian dari rencana cadangan, atau mereka dapat dicadangkan sesuai kebutuhan melalui cadangan sesuai permintaan.

Anda dapat mengembalikan satu tabel (juga dikenal sebagai pemulihan tingkat item) atau seluruh cluster. Perhatikan bahwa tabel tidak dapat dicadangkan sendiri; tabel dicadangkan sebagai bagian dari cluster saat cluster dicadangkan.

Menggunakan AWS Backup memungkinkan Anda untuk melihat sumber daya Anda secara terpusat; Namun, jika Amazon Redshift adalah satu-satunya sumber daya yang Anda gunakan, Anda dapat terus menggunakan penjadwal snapshot otomatis di Amazon Redshift. Perhatikan bahwa Anda tidak dapat terus mengelola pengaturan snapshot manual menggunakan Amazon Redshift jika Anda memilih untuk mengelola ini melalui. AWS Backup

Anda dapat mencadangkan cluster Amazon Redshift baik melalui AWS Backup konsol atau menggunakan. AWS CLI

Ada dua cara untuk menggunakan AWS Backup konsol untuk mencadangkan cluster Amazon Redshift: sesuai permintaan atau sebagai bagian dari paket cadangan.

Buat cadangan Amazon Redshift sesuai permintaan

Lihat Membuat halaman jenis cadangan sesuai permintaan untuk informasi selengkapnya.

Untuk membuat snapshot manual, biarkan kotak centang pencadangan berkelanjutan tidak dicentang saat Anda membuat paket cadangan yang menyertakan sumber daya Amazon Redshift.

Buat cadangan Amazon Redshift terjadwal dalam paket cadangan

Pencadangan terjadwal Anda dapat menyertakan kluster Amazon Redshift jika merupakan sumber daya yang dilindungi. Untuk memilih melindungi tabel Amazon Redshift:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Menggunakan panel navigasi, pilih Sumber daya yang dilindungi.
3. Alihkan Amazon Redshift ke Aktif.
4. Lihat Menetapkan sumber daya ke konsol untuk menyertakan klaster Amazon Redshift dalam paket yang sudah ada atau yang baru.

Di bawah Kelola paket Cadangan, Anda dapat memilih untuk membuat paket cadangan dan menyertakan kluster Amazon Redshift, atau Anda dapat memperbarui yang sudah ada untuk

menyertakan kluster Amazon Redshift. Saat menambahkan jenis sumber daya Amazon Redshift, Anda dapat memilih untuk menambahkan Semua klaster Amazon Redshift, atau mencentang kotak di sebelah cluster Anda

Cadangkan secara terprogram

Anda juga dapat menentukan rencana cadangan Anda dalam dokumen JSON dan menyediakannya menggunakan AWS Backup konsol atau AWS CLI. Lihat Membuat rencana cadangan menggunakan dokumen JSON dan AWS Backup CLI untuk informasi tentang cara membuat rencana cadangan secara terprogram.

Anda dapat melakukan operasi berikut menggunakan API:

- Mulai pekerjaan cadangan
- Jelaskan pekerjaan cadangan
- Dapatkan metadata titik pemulihan
- Daftar poin pemulihan berdasarkan sumber daya
- Tag daftar untuk titik pemulihan

Lihat cadangan klaster Amazon Redshift

Untuk melihat dan memodifikasi cadangan tabel Amazon Redshift Anda di dalam konsol:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pilih Brankas Cadangan. Kemudian, klik nama brankas cadangan yang berisi kluster Amazon Redshift Anda.
3. Brankas cadangan akan menampilkan ringkasan dan daftar cadangan. Anda dapat mengklik tautan di kolom ID titik pemulihan.
4. Untuk menghapus satu atau beberapa titik pemulihan, centang kotak yang ingin Anda hapus. Di bawah tombol Tindakan, Anda dapat memilih Hapus.

Memulihkan klaster Amazon Redshift

Lihat cara Memulihkan klaster Amazon Redshift untuk informasi selengkapnya.

Pencadangan Layanan Basis Data Relasional Amazon

Amazon RDS dan AWS Backup

Saat Anda mempertimbangkan opsi untuk mencadangkan instans dan cluster Amazon RDS Anda, penting untuk mengklarifikasi jenis cadangan yang ingin Anda buat dan gunakan. Beberapa AWS sumber daya, termasuk Amazon RDS, menawarkan solusi cadangan asli mereka sendiri.

Amazon RDS memberikan opsi untuk membuat cadangan otomatis dan pencadangan manual. Dalam terminologi Amazon RDS, semua titik pemulihan yang dibuat oleh AWS Backup, termasuk yang ada dalam rencana cadangan, sedang mempertimbangkan pencadangan manual.

Saat Anda menggunakan AWS Backup untuk membuat cadangan (titik pemulihan) instans Amazon RDS, AWS Backup periksa apakah Anda sebelumnya telah menggunakan Amazon RDS untuk membuat cadangan otomatis. Jika ada cadangan otomatis, AWS Backup buat salinan snapshot ini (`copy-db-snapshot`operasi). Jika tidak ada cadangan yang masih ada, AWS Backup buat snapshot dari instance yang Anda tunjukkan, bukan salinan (`create-db-snapshot`operasi).

Snapshot pertama yang dibuat oleh AWS Backup, dibuat oleh salah satu operasi, akan menghasilkan 1 snapshot penuh. Semua salinan berikutnya dari ini akan menjadi cadangan tambahan, selama cadangan lengkap ada.

> **Important**
>
> Ketika rencana AWS Backup cadangan dijadwalkan untuk membuat beberapa snapshot harian dari instans Amazon RDS, dan ketika salah satu jendela Start AWS Backup Backup yang dijadwalkan bertepatan dengan jendela Cadangan Amazon RDS, garis keturunan data cadangan dapat bercabang menjadi cadangan yang tidak identik, membuat cadangan yang tidak direncanakan dan bertentangan. Untuk mencegah hal ini, pastikan rencana AWS Backup cadangan Anda atau jendela Amazon RDS tidak bertepatan dengan waktu mereka.

Pencadangan berkelanjutan Amazon RDS dan pemulihan titik waktu

Pencadangan berkelanjutan melibatkan penggunaan AWS Backup untuk membuat cadangan lengkap sumber daya Amazon RDS Anda, lalu menangkap semua perubahan melalui log transaksi. Anda dapat mencapai perincian yang lebih besar dengan memutar ulang ke titik waktu yang ingin Anda kembalikan daripada memilih snapshot sebelumnya yang diambil pada interval waktu tetap.

Lihat pencadangan berkelanjutan dan layanan yang didukung PITR dan mengelola pengaturan pencadangan berkelanjutan untuk informasi selengkapnya.

Pencadangan Zona Multi-Ketersediaan Amazon RDS

AWS Backup mencadangkan dan mendukung Amazon RDS untuk MySQL dan untuk opsi penyebaran PostgreSQL Multi-AZ (Availability Zone) dengan satu instance database siaga utama dan dua instance basis data siaga yang dapat dibaca.

Pencadangan Zona Ketersediaan Multi tersedia di wilayah berikut: Wilayah Asia Pasifik (Sydney), Wilayah Asia Pasifik (Tokyo), Wilayah Eropa (Irlandia), Wilayah AS Timur (Ohio), Wilayah AS Barat (Oregon), Wilayah Eropa (Stockholm), Wilayah Asia Pasifik (Singapura), Wilayah AS Timur (Virginia N.), dan Wilayah Eropa (Frankfurt).

Opsi penyebaran multi-AZ mengoptimalkan transaksi tulis dan sangat ideal ketika beban kerja Anda memerlukan kapasitas baca tambahan, latensi transaksi tulis yang lebih rendah, lebih banyak ketahanan dari jitter jaringan (yang berdampak pada konsistensi latensi transaksi tulis), serta ketersediaan dan daya tahan yang tinggi.

Untuk membuat cluster multi-AZ, Anda dapat memilih MySQL atau PostgreSQL sebagai tipe mesin.

Di AWS Backup konsol, ada tiga opsi penerapan:

- Cluster DB multi-AZ: Membuat cluster DB dengan instans DB primer dan dua instans DB siaga yang dapat dibaca, yang masing-masing instans DB di Availability Zone yang berbeda. Menyediakan ketersediaan tinggi, redundansi data, dan meningkatkan kapasitas untuk beban kerja server-ready.
- Instans DB multi-AZ: Membuat instans DB primer dan instans DB siaga di Availability Zone yang berbeda. Ini memberikan ketersediaan tinggi dan redundansi data, tetapi instans DB siaga tidak mendukung koneksi untuk beban kerja baca.
- Instance DB tunggal: Membuat instans DB tunggal tanpa instans DB siaga.

Untuk membuat cadangan untuk Amazon RDS, lihat Membuat cadangan untuk menjadwalkan cadangan sebagai bagian dari rencana pencadangan atau membuat cadangan sesuai permintaan.

> **Note**
>
> Point-in-Time Recovery (PITR) dapat mendukung instance, tetapi bukan cluster. Menyalin snapshot cluster DB multi-AZ tidak didukung.

Perbedaan antara cluster Multi-AZ dan instans RDS

Cadangan dalam satu Availability Zone atau dalam dua Availability Zone adalah instans RDS; penerapan dan pencadangan dengan tiga instans atau lebih adalah cluster, mirip dengan Amazon Aurora, Amazon Neptune, dan Amazon DocumentDB cluster.

ARN (Nama Sumber Daya Amazon) dirender secara berbeda tergantung pada apakah instance atau cluster digunakan:

Sebuah contoh RDS ARN: `arn:aws:rds:region: account:db:name`

Cluster Multi-Ketersediaan RDS: `arn:aws:rds:region:account :cluster:name`

Untuk informasi selengkapnya, lihat penerapan klaster DB multi-AZ di Panduan Pengguna Amazon RDS.

Untuk informasi selengkapnya tentang Membuat snapshot cluster DB multi-AZ, lihat Panduan Pengguna Amazon RDS.

AWS CloudFormation cadangan tumpukan

CloudFormation Tumpukan terdiri dari beberapa sumber daya stateful dan stateless yang dapat Anda cadangkan sebagai satu unit. Dengan kata lain, Anda dapat membuat cadangan dan memulihkan aplikasi yang berisi banyak sumber daya dengan membuat cadangan tumpukan dan memulihkan sumber daya di dalamnya. Semua sumber daya dalam tumpukan ditentukan oleh templat AWS CloudFormation tumpukan.

Ketika CloudFormation tumpukan dicadangkan, titik pemulihan dibuat untuk CloudFormation template dan untuk setiap sumber daya tambahan yang didukung oleh AWS Backup dalam tumpukan. Titik pemulihan ini dikelompokkan bersama dalam titik pemulihan menyeluruh yang disebut komposit.

Titik pemulihan komposit ini tidak dapat dipulihkan, tetapi titik pemulihan bersarang dapat dipulihkan. Anda dapat memulihkan di mana saja dari satu ke semua cadangan bersarang dalam cadangan komposit menggunakan konsol atau. AWS CLI

CloudFormation terminologi tumpukan aplikasi

- Titik pemulihan komposit: Titik pemulihan yang digunakan untuk mengelompokkan titik pemulihan bersarang bersama-sama, serta metadata lainnya.

- Titik pemulihan bersarang: Titik pemulihan sumber daya yang merupakan bagian dari CloudFormation tumpukan dan dicadangkan sebagai bagian dari titik pemulihan komposit. Setiap titik pemulihan bersarang termasuk dalam tumpukan satu titik pemulihan komposit.
- Pekerjaan komposit: Pekerjaan pencadangan, salin, atau pemulihan untuk CloudFormation tumpukan yang dapat memicu pekerjaan cadangan lainnya untuk sumber daya individu dalam tumpukan.
- Pekerjaan bersarang: Pekerjaan pencadangan, salin, atau pemulihan untuk sumber daya dalam AWS CloudFormation tumpukan.

CloudFormation pekerjaan stack backup

Proses pembuatan cadangan disebut pekerjaan cadangan. Pekerjaan cadangan CloudFormation tumpukan memiliki status. Ketika pekerjaan cadangan telah selesai, ia memiliki status`Completed`. Ini menandakan AWS CloudFormation titik pemulihan (cadangan) telah dibuat.

CloudFormation tumpukan dapat dicadangkan menggunakan konsol atau dicadangkan secara terprogram. Untuk membuat cadangan sumber daya apa pun, termasuk CloudFormation tumpukan, lihat Membuat cadangan di tempat lain di Panduan AWS Backup Pengembang ini.

CloudFormation tumpukan dapat dicadangkan menggunakan perintah `StartBackupJob` API. Perhatikan bahwa dokumentasi dan konsol merujuk ke titik pemulihan komposit dan bersarang; bahasa API menggunakan terminologi “titik pemulihan induk dan anak” dalam hubungan kontekstual yang sama.

CloudFormation tumpukan berisi semua AWS sumber daya yang ditunjukkan oleh CloudFormation template Anda. Perhatikan bahwa template Anda mungkin berisi sumber daya yang belum didukung oleh AWS Backup. Jika template Anda berisi kombinasi sumber daya yang AWS didukung dan sumber daya yang tidak didukung, masih AWS Backup akan mencadangkan template ke tumpukan komposit, tetapi Backup hanya akan membuat titik pemulihan dari layanan yang didukung Backup. Semua jenis sumber daya yang terkandung dalam CloudFormation template akan disertakan dalam cadangan, bahkan jika Anda belum memilih ke layanan tertentu (beralih layanan ke “Diaktifkan” di Pengaturan konsol). Cadangan bersarang (titik pemulihan) yang didukung oleh AWS Backup dapat dipulihkan, tetapi tumpukan bersarang tidak dapat dicadangkan atau dipulihkan.

AWS CloudFormation titik pemulihan

Status titik pemulihan

Ketika pekerjaan cadangan tumpukan selesai (status pekerjaan`Completed`), cadangan tumpukan telah dibuat. Cadangan ini juga dikenal sebagai titik pemulihan komposit. Titik pemulihan komposit dapat memiliki salah satu status berikut:`Completed`,`Failed`, atau`Partial`. Perhatikan bahwa pekerjaan cadangan memiliki status, dan titik pemulihan (juga disebut cadangan) juga memiliki status terpisah.

Pekerjaan pencadangan yang lengkap berarti seluruh tumpukan Anda dan sumber daya di dalamnya dilindungi oleh AWS Backup. Status gagal menunjukkan bahwa pekerjaan pencadangan tidak berhasil; Anda harus membuat cadangan lagi setelah masalah yang menyebabkan kegagalan diperbaiki.

`Partial`Status berarti bahwa tidak semua sumber daya dalam tumpukan dicadangkan. Ini dapat terjadi jika CloudFormation template berisi sumber daya yang saat ini tidak didukung oleh AWS Backup, atau mungkin terjadi jika satu atau lebih pekerjaan cadangan milik sumber daya dalam tumpukan (sumber daya bersarang) memiliki status selain. `Completed` Anda dapat secara manual membuat cadangan sesuai permintaan untuk menjalankan kembali sumber daya apa pun yang menghasilkan status selain. `Completed` Jika Anda mengharapkan tumpukan memiliki status `Completed` tetapi ditandai sebagai `Partial` gantinya, periksa untuk melihat kondisi mana di atas yang mungkin benar tentang tumpukan Anda.

Setiap sumber daya bersarang dalam titik pemulihan komposit memiliki titik pemulihan masing-masing, masing-masing dengan statusnya sendiri (salah satu `Completed` atau`Failed`). Poin pemulihan bersarang dengan status `Completed` dapat dipulihkan.

Kelola poin pemulihan

Poin pemulihan komposit (cadangan) dapat disalin; titik pemulihan bersarang dapat disalin, dihapus, dipisahkan, atau dipulihkan. Titik pemulihan komposit yang berisi cadangan bersarang tidak dapat dihapus. Setelah titik pemulihan bersarang dalam titik pemulihan komposit telah dihapus atau dipisahkan, Anda dapat secara manual menghapus titik pemulihan komposit secara manual atau membiarkannya tetap sampai siklus hidup rencana cadangan menghapusnya.

Hapus titik pemulihan

Anda dapat menghapus titik pemulihan menggunakan AWS Backup konsol atau menggunakan AWS CLI.

Untuk menghapus titik pemulihan menggunakan AWS Backup konsol,

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Klik pada Sumber Daya yang Dilindungi di navigasi sebelah kiri. Di kotak teks, ketik `CloudFormation` untuk hanya menampilkan CloudFormation tumpukan Anda.
3. Poin pemulihan komposit akan ditampilkan di panel Recovery points. Tanda plus (+) di sebelah kiri setiap ID titik pemulihan dapat diklik untuk memperluas setiap titik pemulihan komposit, menunjukkan semua titik pemulihan bersarang yang terkandung dalam komposit. Anda dapat mencentang kotak di sebelah kiri setiap titik pemulihan untuk memasukkannya dalam pilihan titik pemulihan yang ingin Anda hapus.
4. Klik tombol Hapus.

Saat Anda menggunakan konsol untuk menghapus satu atau lebih titik pemulihan komposit, kotak peringatan akan muncul. Kotak peringatan ini mengharuskan Anda mengonfirmasi niat Anda untuk menghapus titik pemulihan komposit, termasuk titik pemulihan bersarang di dalam tumpukan komposit.

Untuk menghapus titik pemulihan menggunakan API, gunakan `DeleteRecoveryPoint` perintah.

Saat Anda menggunakan API dengan API, AWS Command Line Interface Anda harus menghapus semua titik pemulihan bersarang sebelum menghapus titik komposit. Jika Anda mengirim permintaan API untuk menghapus cadangan tumpukan komposit (titik pemulihan) yang masih berisi titik pemulihan bersarang di dalamnya, permintaan akan mengembalikan kesalahan.

Putuskan titik pemulihan bersarang dari titik pemulihan komposit

Anda dapat memisahkan titik pemulihan bersarang dari titik pemulihan komposit (misalnya, Anda ingin mempertahankan titik pemulihan bersarang tetapi menghapus titik pemulihan komposit). Kedua titik pemulihan akan tetap ada, tetapi mereka tidak akan lagi terhubung; yaitu, tindakan yang terjadi pada titik pemulihan komposit tidak akan lagi berlaku untuk titik pemulihan bersarang setelah dipisahkan.

Anda dapat memisahkan titik pemulihan menggunakan konsol, atau Anda dapat memanggil API`DisassociateRecoveryPointFromParent`. [Perhatikan bahwa panggilan API menggunakan istilah “induk” untuk merujuk ke titik pemulihan komposit.]

Salin titik pemulihan

Anda dapat menyalin titik pemulihan komposit, atau Anda dapat menyalin titik pemulihan bersarang jika sumber daya mendukung salinan lintas akun dan lintas wilayah.

Untuk menyalin titik pemulihan menggunakan AWS Backup konsol:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Klik pada Sumber Daya yang Dilindungi di navigasi sebelah kiri. Di kotak teks, ketik `CloudFormation` untuk hanya menampilkan CloudFormation tumpukan Anda.
3. Poin pemulihan komposit akan ditampilkan di panel Recovery points. Tanda plus (+) di sebelah kiri setiap ID titik pemulihan dapat diklik untuk memperluas setiap titik pemulihan komposit, menunjukkan semua titik pemulihan bersarang yang terkandung dalam komposit. Anda dapat mengklik tombol lingkaran radial di sebelah kiri titik pemulihan untuk menyalinnya.
4. Setelah dipilih, klik tombol Salin di sudut kanan atas panel.

Saat Anda menyalin titik pemulihan komposit, titik pemulihan bersarang yang tidak mendukung fungsionalitas salinan tidak akan berakhir di tumpukan yang disalin. Titik pemulihan komposit akan memiliki status`Partial`.

Pertanyaan yang Sering Diajukan

1. “Apa yang termasuk sebagai bagian dari cadangan aplikasi?”

   Sebagai bagian dari setiap cadangan aplikasi yang didefinisikan menggunakan CloudFormation, template, nilai yang diproses dari setiap parameter dalam template, dan sumber daya bersarang yang AWS Backup didukung oleh dicadangkan. Sumber daya bersarang dicadangkan dengan cara yang sama seperti sumber daya individu yang bukan bagian dari CloudFormation tumpukan dicadangkan. Perhatikan bahwa nilai parameter yang ditandai sebagai tidak `no-echo` akan dicadangkan.

2. “Bisakah saya mencadangkan AWS CloudFormation tumpukan saya yang memiliki tumpukan bersarang?”

   Ya. CloudFormation Tumpukan Anda yang berisi tumpukan bersarang dapat ada di cadangan Anda.

3. “Apakah *`Partial`* status berarti pembuatan cadangan saya gagal?”

Tidak. Status sebagian menunjukkan bahwa beberapa titik pemulihan didukung, sementara beberapa tidak. Ada tiga kondisi untuk memeriksa apakah Anda mengharapkan hasil `Completed` cadangan:

a. Apakah CloudFormation tumpukan Anda berisi sumber daya yang saat ini tidak didukung oleh? AWS Backup Untuk daftar sumber daya yang didukung, lihat Sumber AWS daya yang didukung dan aplikasi pihak ketiga di Panduan Pengembang kami.

b. Satu atau lebih pekerjaan cadangan milik sumber daya dalam tumpukan tidak berhasil dan pekerjaan harus dijalankan kembali.

c. Titik pemulihan bersarang telah dihapus atau dipisahkan dari titik pemulihan komposit.

4. “Bagaimana cara mengecualikan sumber daya dalam cadangan CloudFormation tumpukan saya?”

   Ketika Anda mencadangkan CloudFormation tumpukan Anda, Anda dapat mengecualikan sumber daya dari menjadi bagian dari cadangan. Di konsol, selama membuat rencana cadangan dan memperbarui proses rencana cadangan, ada langkah menetapkan sumber daya. Pada langkah ini, ada bagian Pemilihan sumber daya. Jika Anda memilih menyertakan jenis sumber daya tertentu dan telah disertakan CloudFormation sebagai sumber daya untuk dicadangkan, Anda dapat mengecualikan ID sumber daya tertentu dari jenis sumber daya yang dipilih. Anda juga dapat menggunakan tag untuk mengecualikan sumber daya dalam tumpukan.

   Menggunakan CLI, Anda dapat menggunakan

   - `NotResources`dalam rencana cadangan Anda untuk mengecualikan sumber daya tertentu dari CloudFormation tumpukan Anda.
   - `StringNotLike`untuk mengecualikan item melalui tag.

5. “Jenis cadangan apa yang didukung untuk sumber daya bersarang?”

   Pencadangan sumber daya bersarang dapat berupa cadangan penuh atau tambahan, tergantung pada jenis cadangan yang didukung oleh sumber daya ini. AWS Backup Untuk informasi selengkapnya, lihat Cara kerja pencadangan tambahan. Namun, perhatikan bahwa PITR (point-in-time restore) tidak didukung untuk sumber daya bersarang Amazon S3 dan Amazon RDS.

6. “Apakah set perubahan yang merupakan bagian dari CloudFormation tumpukan dicadangkan?”

   Tidak. Set perubahan tidak dicadangkan sebagai bagian dari cadangan CloudFormation tumpukan.

7. “Bagaimana status AWS CloudFormation tumpukan memengaruhi cadangan?”

   Status CloudFormation tumpukan dapat memengaruhi cadangan. Tumpukan dengan status yang mencakup `COMPLETE` dapat dicadangkan, seperti status`CREATE_COMPLETE`,,`ROLLBACK_COMPLETE`, `UPDATE_COMPLETE` `UPDATE_ROLLBACK_COMPLETE`IMPORT_COMPLETE, atau`IMPORT_ROLLBACK_COMPLETE`.

   Dalam kasus di mana unggahan template baru gagal dan tumpukan pindah ke status`ROLLBACK_COMPLETE`, template baru akan dicadangkan tetapi cadangan sumber daya bersarang akan didasarkan pada sumber daya yang digulung kembali.

8. “Bagaimana siklus hidup tumpukan aplikasi berbeda dari siklus hidup titik pemulihan lainnya?”

   Siklus hidup titik pemulihan bersarang ditentukan oleh rencana cadangan yang menjadi miliknya. Titik pemulihan komposit ditentukan oleh siklus hidup terpanjang dari semua titik pemulihan bersarang. Ketika titik pemulihan bersarang terakhir yang tersisa dalam titik pemulihan komposit dihapus atau dipisahkan, titik pemulihan komposit juga akan dihapus.

9. “Bagaimana tag yang CloudFormation disalin ke titik pemulihan?”

   Ya. Tag tersebut akan disalin ke setiap titik pemulihan bersarang masing-masing.

10. “Apakah ada perintah untuk menghapus titik pemulihan komposit dan bersarang (cadangan)?”

    Ya. Beberapa backup harus dihapus sebelum yang lain dapat dihapus. Cadangan komposit yang berisi titik pemulihan bersarang tidak dapat dihapus sampai semua titik pemulihan dalam komposit telah dihapus. Setelah titik pemulihan komposit tidak lagi berisi titik pemulihan bersarang, Anda dapat menghapusnya secara manual. Jika tidak, itu akan dihapus sesuai dengan siklus hidup rencana cadangannya.

Kembalikan aplikasi dalam tumpukan

Lihat Cara memulihkan cadangan tumpukan aplikasi untuk informasi tentang memulihkan titik pemulihan bersarang.

Membuat cadangan Windows VSS

Dengan AWS Backup, Anda dapat mencadangkan dan memulihkan aplikasi Windows berkemampuan VSS (Volume Shadow Copy Service) yang berjalan di instans Amazon EC2. Jika

aplikasi memiliki penulis VSS terdaftar dengan Windows VSS, maka AWS Backup buat snapshot yang akan konsisten untuk aplikasi itu.

Anda dapat melakukan pemulihan yang konsisten, saat menggunakan layanan pencadangan terkelola yang sama yang digunakan untuk melindungi AWS sumber daya lainnya. Dengan pencadangan Windows yang konsisten aplikasi pada EC2, Anda mendapatkan pengaturan konsistensi dan kesadaran aplikasi yang sama dengan alat cadangan tradisional.

> **Note**
>
> AWS Backup saat ini hanya mendukung pencadangan sumber daya yang konsisten aplikasi yang berjalan di Amazon EC2, khususnya skenario pencadangan di mana data aplikasi dapat dipulihkan dengan mengganti instance yang ada dengan instance baru yang dibuat dari cadangan. Tidak semua jenis instans atau aplikasi didukung untuk cadangan Windows VSS.

Untuk informasi selengkapnya, lihat Membuat Snapshot Konsisten Aplikasi VSS di Panduan Pengguna Amazon EC2.

Untuk mencadangkan dan memulihkan sumber daya Windows berkemampuan VSS yang menjalankan Amazon EC2, ikuti langkah-langkah berikut untuk menyelesaikan tugas prasyarat yang diperlukan. Untuk petunjuk, lihat Sebelum Anda Memulai di Panduan Pengguna Amazon EC2 untuk Instans Windows.

1. Unduh, instal, dan konfigurasikan agen SSM di AWS Systems Manager. Langkah ini diperlukan. Untuk petunjuk, lihat Bekerja dengan agen SSM di instans Amazon EC2 untuk Windows Server di Panduan Pengguna Systems AWS Manager.
2. Tambahkan kebijakan IAM ke peran IAM dan lampirkan peran tersebut ke instans Amazon EC2 sebelum Anda mengambil cadangan Windows VSS (Volume Shadow Copy Service). Untuk petunjuknya, lihat Membuat Peran IAM untuk Snapshot berkemampuan VSS di Panduan Pengguna Amazon EC2. Untuk contoh kebijakan IAM, lihatKebijakan terkelola untuk AWS Backup.
3. Unduh dan instal komponen VSS ke Windows pada instans Amazon EC2
4. Aktifkan VSS di AWS Backup:
    1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
    2. Di dasbor, pilih jenis cadangan yang ingin Anda buat, baik Buat cadangan sesuai permintaan atau Kelola paket Cadangan. Berikan informasi yang diperlukan untuk jenis cadangan Anda.

3. Saat Anda menetapkan sumber daya, pilih EC2. Cadangan Windows VSS saat ini hanya didukung untuk instans EC2.
4. Di bagian Pengaturan lanjutan, pilih Windows VSS. Ini memungkinkan Anda untuk mengambil cadangan Windows VSS yang konsisten dengan aplikasi.
5. Buat cadangan Anda.

Pekerjaan cadangan dengan status `Completed` tidak menjamin bahwa bagian VSS berhasil; Inklusi VSS dilakukan atas dasar upaya terbaik. Lanjutkan dengan langkah-langkah berikut untuk menentukan apakah cadangan konsisten aplikasi, konsisten crash, atau gagal:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di bawah Akun saya di navigasi kiri, klik Pekerjaan.
3. Status `Completed` menunjukkan pekerjaan yang sukses yang konsisten dengan aplikasi (VSS).

   Status `Completed with issues` menunjukkan bahwa operasi VSS telah gagal, jadi hanya cadangan yang konsisten dengan kerusakan yang berhasil. Status ini juga akan memiliki pesan popover. `"Windows VSS Backup Job Error encountered, trying for regular backup"`

   Jika cadangan tidak berhasil, statusnya akan`Failed`.
4. Untuk melihat detail tambahan dari pekerjaan cadangan, klik pada pekerjaan individu. Misalnya, detailnya dapat dibaca`Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`.

Pencadangan berkemampuan VSS dengan target yang non-Windows atau komponen non-VSS Windows yang berhasil pekerjaannya akan crash konsisten tanpa VSS.

Instans Amazon EC2 yang tidak didukung

Jenis instans Amazon EC2 berikut tidak didukung untuk pencadangan Windows berkemampuan VSS karena merupakan instance kecil dan mungkin tidak berhasil mengambil cadangan.

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro

- t2.nano
- t2.micro

Amazon EBS dan AWS Backup

Proses pencadangan untuk sumber daya Amazon EBS mirip dengan langkah-langkah yang digunakan untuk mencadangkan jenis sumber daya lainnya:

- Buat cadangan sesuai permintaan
- Buat cadangan terjadwal

Informasi khusus sumber daya dicatat di bagian berikut.

Tingkat Arsip Amazon EBS untuk penyimpanan dingin

EBS adalah salah satu sumber daya yang mendukung transisi backup ke cold storage. Untuk informasi selengkapnya, lihat Siklus hidup dan tingkatan penyimpanan.

> **Note**
>
> Fitur ini tidak tersedia di Wilayah China (Beijing), China (Ningxia), AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

Amazon EBS multi-volume, backup yang konsisten crash

Secara default, AWS Backup membuat cadangan volume Amazon EBS yang konsisten dengan crash yang dilampirkan ke instans Amazon EC2. Konsistensi crash berarti bahwa snapshot untuk setiap volume Amazon EBS yang dilampirkan ke instans Amazon EC2 yang sama diambil pada saat yang sama. Anda tidak perlu lagi menghentikan instans atau berkoordinasi di antara beberapa volume Amazon EBS untuk memastikan konsistensi crash pada status aplikasi Anda.

Karena snapshot multi-volume dan konsisten crash adalah AWS Backup fungsionalitas default, Anda tidak perlu melakukan hal lain untuk menggunakan fitur ini. Anda dapat mencadangkan volume Amazon EBS menggunakan salah satu prosedur berikut:

Peran yang digunakan untuk membuat titik pemulihan snapshot EBS akan dikaitkan dengan snapshot itu. Peran yang sama ini harus gunakan yang untuk menghapus titik pemulihan yang dibuat olehnya atau untuk mentransisikan titik pemulihan ke tingkat arsip.

Kunci Snapshot Amazon EBS dan AWS Backup

AWS Backup snapshot Amazon EBS terkelola dan snapshot yang terkait dengan AWS Backup Amazon EC2 AMI terkelola yang menerapkan Amazon EBS Snapshot Lock mungkin tidak dihapus sebagai bagian dari siklus hidup titik pemulihan jika durasi kunci snapshot melebihi siklus hidup pencadangan. Sebaliknya, titik pemulihan ini akan berstatus`EXPIRED`. Poin pemulihan ini dapat dihapus secara manual jika Anda memilih untuk menghapus kunci snapshot Amazon EBS terlebih dahulu.

Memulihkan sumber daya Amazon EBS

Untuk memulihkan volume Amazon EBS Anda, ikuti langkah-langkah dalam Memulihkan volume Amazon EBS.

Menyalin tag ke cadangan

Secara umum, AWS Backup menyalin tag dari sumber daya yang dilindunginya ke titik pemulihan Anda. Untuk informasi selengkapnya tentang cara menyalin tag selama pemulihan, lihat Menyalin tag selama pemulihan.

Misalnya, saat Anda mencadangkan volume Amazon EC2, AWS Backup menyalin tag sumber daya grup dan individual ke snapshot yang dihasilkan, tunduk pada hal berikut:

- Untuk daftar izin khusus sumber daya yang diperlukan untuk menyimpan tag metadata pada cadangan, lihat Izin yang diperlukan untuk menetapkan tag ke cadangan.
- Tag yang awalnya dikaitkan dengan sumber daya dan tag yang ditetapkan selama pencadangan ditetapkan ke titik pemulihan yang disimpan dalam brankas cadangan, hingga maksimum 50 (ini adalah AWS batasan). Tag yang ditetapkan selama pencadangan memiliki prioritas, dan kedua set tag disalin dalam urutan abjad.
- DynamoDB tidak mendukung penetapan tag ke cadangan kecuali Anda mengaktifkan terlebih dahulu. Cadangan DynamoDB tingkat lanjut
- Volume Amazon EBS yang dilampirkan ke instans Amazon EC2 adalah sumber daya bersarang. Tag pada volume Amazon EBS yang dilampirkan ke instans Amazon EC2 adalah tag bersarang. AWS Backup melakukan upaya terbaik untuk menyalin tag bersarang, tetapi jika tidak berhasil, itu membuat cadangan tanpa tag dan melaporkan Status Selesai.

- Saat cadangan Amazon EC2 membuat titik pemulihan gambar dan satu set snapshot, AWS Backup menyalin tag ke AMI yang dihasilkan. AWS Backup juga melakukan upaya terbaik untuk menyalin tag dari volume yang terkait dengan instans Amazon EC2 ke snapshot yang dihasilkan.

Jika Anda menyalin cadangan Anda ke yang lain Wilayah AWS, AWS Backup salin semua tag cadangan asli ke tujuan Wilayah AWS.

Menghentikan pekerjaan cadangan

Anda dapat menghentikan pekerjaan cadangan AWS Backup setelah dimulai. Ketika Anda melakukan ini, cadangan tidak dibuat, dan catatan pekerjaan cadangan dipertahankan dengan status dibatalkan.

Untuk menghentikan pekerjaan cadangan menggunakan AWS Backup konsol

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi di sebelah kiri, pilih Jobs.
3. Pilih pekerjaan cadangan yang ingin Anda hentikan.
4. Di panel backup job details, pilih Stop.

Salin cadangan

Anda dapat menyalin cadangan ke beberapa Akun AWS atau sesuai permintaan atau Wilayah AWS secara otomatis sebagai bagian dari rencana pencadangan terjadwal untuk sebagian besar jenis sumber daya. Untuk spesifik lihatthe section called “Ketersediaan fitur berdasarkan sumber daya”.

Anda juga dapat mengotomatiskan urutan salinan lintas akun dan lintas wilayah untuk sebagian besar sumber daya yang didukung, kecuali Amazon RDS dan Aurora. Untuk snapshot Amazon RDS dan Aurora AWS Backup , hanya mendukung otomatisasi salinan lintas akun atau lintas wilayah karena cara layanan tersebut membuat kunci enkripsi mereka (menyalin snapshot cluster DB Multi-AZ tidak didukung).

Beberapa jenis sumber daya memiliki kemampuan pencadangan berkelanjutan dan salinan lintas wilayah dan lintas akun tersedia. Ketika salinan lintas wilayah atau lintas akun dari cadangan berkelanjutan dibuat, titik pemulihan yang disalin (cadangan) menjadi cadangan snapshot (periodik).

Bergantung pada jenis sumber daya, snapshot mungkin berupa salinan tambahan atau salinan lengkap. PITR (Point-in-Time Restore) tidak tersedia untuk salinan ini.

Salinan mempertahankan konfigurasi sumbernya, termasuk tanggal pembuatan dan periode retensi. Tanggal pembuatan mengacu pada kapan sumber dibuat, bukan saat salinan dibuat.

CATATAN: Konfigurasi sumber mengganti setelan kedaluwarsa salinannya, meskipun salinan disetel ke tidak pernah kedaluwarsa; salinan yang disetel ke tidak pernah kedaluwarsa akan tetap mempertahankan tanggal kedaluwarsa sumbernya.

Jika Anda ingin salinan cadangan Anda tidak pernah kedaluwarsa, setel cadangan sumber Anda agar tidak pernah kedaluwarsa atau tentukan salinan Anda kedaluwarsa 100 tahun setelah pembuatannya.

Daftar Isi

Membuat salinan cadangan di seluruh Wilayah AWS

Dengan menggunakan AWS Backup, Anda dapat menyalin cadangan ke beberapa Wilayah AWS sesuai permintaan atau secara otomatis sebagai bagian dari rencana pencadangan terjadwal. Replikasi Lintas Wilayah sangat berharga jika Anda memiliki kelangsungan bisnis atau persyaratan kepatuhan untuk menyimpan cadangan jarak minimum dari data produksi Anda. Untuk tutorial video, lihat Mengelola salinan cadangan lintas wilayah.

Saat Anda menyalin cadangan ke yang baru Wilayah AWS untuk pertama kalinya, AWS Backup salin cadangan secara penuh. Secara umum, jika suatu layanan mendukung pencadangan tambahan, salinan cadangan berikutnya dalam hal yang sama Wilayah AWS akan bersifat inkremental. AWS Backup akan mengenkripsi ulang salinan Anda menggunakan kunci yang dikelola pelanggan dari brankas tujuan Anda.

Pengecualian adalah Amazon EBS, yang menyatakan bahwa, mengubah status enkripsi snapshot selama operasi penyalinan menghasilkan salinan penuh (bukan tambahan).

Persyaratan

- Sebagian besar sumber daya AWS Backup yang didukung mendukung pencadangan lintas wilayah. Untuk spesifik, lihat Ketersediaan fitur berdasarkan sumber daya.

- Sebagian besar AWS Wilayah mendukung cadangan Lintas wilayah. Untuk spesifik, lihat Ketersediaan fitur oleh Wilayah AWS.
- AWS Backup tidak mendukung salinan lintas wilayah untuk penyimpanan dalam tingkatan dingin.

Pertimbangan salinan Lintas Wilayah dengan sumber daya tertentu

Amazon RDS

Anda tidak dapat menyalin grup opsi ke grup lain Wilayah AWS. Jika ini dicoba, Anda bisa mendapatkan kesalahan, seperti “Snapshot memerlukan grup opsi target dengan opsi berikut:...”

Anda harus memasukkan grup opsi yang sama di target Wilayah AWS saat membuat salinan Lintas wilayah baru dari snapshot Amazon RDS.

Melakukan pencadangan lintas wilayah sesuai permintaan

Untuk menyalin cadangan yang ada sesuai permintaan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pilih Brankas Cadangan.
3. Pilih brankas yang berisi titik pemulihan yang ingin Anda salin.
4. Di bagian Backup, pilih titik pemulihan untuk disalin.
5. Menggunakan tombol dropdown Tindakan, pilih Salin.
6. Masukkan nilai berikut:

   Salin ke tujuan

   Pilih tujuan Wilayah AWS untuk salinan. Anda dapat menambahkan aturan salinan baru per salinan ke tujuan baru.

   Brankas Cadangan Tujuan

   Pilih brankas cadangan tujuan untuk salinan.

   Transisi ke penyimpanan dingin

   Pilih kapan harus mentransisikan salinan cadangan ke penyimpanan dingin. Cadangan yang dialihkan ke cold storage harus disimpan di sana selama minimal 90 hari. Nilai ini tidak dapat diubah setelah salinan dialihkan ke penyimpanan dingin.

Untuk melihat daftar sumber daya yang dapat Anda transisi ke penyimpanan dingin, lihat bagian “Siklus Hidup ke penyimpanan dingin” pada Ketersediaan fitur berdasarkan sumber daya tabel. Ekspresi cold storage diabaikan untuk sumber daya lain.

Periode penahanan

Pilih menentukan jumlah hari setelah pembuatan bahwa salinan dihapus. Nilai ini harus lebih besar dari 90 hari di luar nilai Transisi ke penyimpanan dingin. Periode penyimpanan Selalu mempertahankan salinan Anda tanpa batas waktu.

Peran IAM

Pilih peran IAM yang AWS Backup akan digunakan saat membuat salinan. Peran juga harus AWS Backup terdaftar sebagai entitas tepercaya, yang memungkinkan AWS Backup untuk mengambil peran. Jika Anda memilih Default dan peran AWS Backup default tidak ada di akun Anda, satu akan dibuat untuk Anda dengan izin yang benar.

7. Pilih Salin.

Penjadwalan Pencadangan lintas wilayah

Anda dapat menggunakan rencana pencadangan terjadwal untuk menyalin cadangan. Wilayah AWS

Untuk menyalin cadangan menggunakan rencana cadangan terjadwal

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di Akun Saya, pilih Paket Cadangan, lalu pilih Buat paket Cadangan.
3. Pada halaman Buat Rencana Cadangan, pilih Buat paket baru.
4. Untuk nama paket Backup, masukkan nama untuk paket cadangan Anda.
5. Di bagian Konfigurasi aturan Backup, tambahkan aturan cadangan yang menentukan jadwal cadangan, jendela cadangan, dan aturan siklus hidup. Anda dapat menambahkan lebih banyak aturan cadangan nanti.

   a. Untuk nama aturan Backup, masukkan nama untuk aturan Anda.

   b. Untuk Backup vault, pilih vault dari daftar. Poin pemulihan untuk cadangan ini akan disimpan di brankas ini. Anda dapat membuat brankas cadangan baru.

   c. Untuk frekuensi Backup, pilih seberapa sering Anda ingin mengambil backup.

d. Untuk layanan yang mendukung PITR, jika Anda menginginkan fitur ini, pilih Aktifkan cadangan berkelanjutan untuk point-in-time pemulihan (PITR). Untuk daftar layanan yang mendukung PITR, lihat bagian Ketersediaan fitur berdasarkan sumber daya tabel tersebut.

e. Untuk jendela Backup, pilih Gunakan default jendela cadangan - direkomendasikan. Anda dapat menyesuaikan jendela cadangan.

f. Untuk Salin ke tujuan, Pilih tujuan Wilayah AWS untuk salinan cadangan Anda. Cadangan Anda akan disalin ke Wilayah ini. Anda dapat menambahkan aturan salinan baru per salinan ke tujuan baru. Kemudian masukkan nilai-nilai berikut:

   Salin ke brankas akun lain

   Jangan beralih opsi ini. Untuk mempelajari lebih lanjut tentang salinan lintas akun, lihat Membuat salinan cadangan di seluruh Akun AWS

   Brankas Cadangan Tujuan

   Pilih brankas cadangan di Wilayah tujuan tempat AWS Backup akan menyalin cadangan Anda.

   Jika Anda ingin membuat brankas cadangan baru untuk salinan Lintas wilayah, pilih Buat brankas Cadangan baru. Masukkan informasi di wizard. Kemudian pilih Create Backup vault.

6. Pilih Buat paket.

Membuat salinan cadangan di seluruh Akun AWS

Dengan menggunakan AWS Backup, Anda dapat mencadangkan hingga beberapa Akun AWS sesuai permintaan atau secara otomatis sebagai bagian dari rencana pencadangan terjadwal. Gunakan cadangan lintas akun jika Anda ingin menyalin cadangan dengan aman ke satu atau lebih Akun AWS di organisasi Anda untuk alasan operasional atau keamanan. Jika cadangan asli Anda terhapus, Anda dapat menyalin cadangan dari akun tujuannya ke akun sumbernya, lalu memulai pemulihan. Sebelum Anda dapat melakukan ini, Anda harus memiliki dua akun milik organisasi yang sama dalam AWS Organizations layanan. Untuk informasi selengkapnya, lihat Tutorial: Membuat dan mengonfigurasi organisasi di Panduan Pengguna Organizations.

Di akun tujuan, Anda harus membuat brankas cadangan. Kemudian, Anda menetapkan kunci terkelola pelanggan untuk mengenkripsi cadangan di akun tujuan, dan kebijakan akses berbasis sumber daya untuk memungkinkan mengakses sumber daya yang ingin AWS Backup Anda salin. Di

akun sumber, jika sumber daya Anda dienkripsi dengan kunci yang dikelola pelanggan, Anda harus membagikan kunci yang dikelola pelanggan ini dengan akun tujuan. Anda kemudian dapat membuat rencana cadangan dan memilih akun tujuan yang merupakan bagian dari unit organisasi Anda AWS Organizations.

Saat Anda menyalin cadangan ke akun silang untuk pertama kalinya, AWS Backup salin cadangan secara penuh. Secara umum, jika layanan mendukung pencadangan tambahan, salinan cadangan berikutnya di akun yang sama bersifat inkremental. AWS Backup mengenkripsi ulang salinan Anda menggunakan kunci terkelola pelanggan dari brankas tujuan Anda.

Persyaratan

- Sebelum Anda mengelola sumber daya Akun AWS di beberapa akun AWS Backup, akun Anda harus milik organisasi yang sama dalam AWS Organizations layanan.
- Sebagian besar sumber daya yang didukung oleh AWS Backup dukungan cadangan lintas akun. Untuk spesifik, lihat Ketersediaan fitur berdasarkan sumber daya.
- Sebagian besar AWS Wilayah mendukung pencadangan lintas akun. Untuk spesifik, lihat Ketersediaan fitur oleh Wilayah AWS.
- AWS Backup tidak mendukung salinan lintas akun untuk penyimpanan di tingkat dingin.

Menyiapkan cadangan lintas akun

Apa yang Anda butuhkan untuk membuat cadangan lintas akun?

- Akun sumber

  Akun sumber adalah akun tempat AWS sumber daya produksi dan cadangan utama Anda berada.

  Pengguna akun sumber memulai operasi pencadangan lintas akun. Pengguna atau peran akun sumber harus memiliki izin API yang sesuai untuk memulai operasi. Izin yang sesuai mungkin kebijakan AWS terkelola`AWSBackupFullAccess`, yang memungkinkan akses penuh ke AWS Backup operasi, atau kebijakan terkelola pelanggan yang memungkinkan tindakan seperti`ec2:ModifySnapshotAttribute`. Untuk informasi selengkapnya tentang jenis kebijakan, lihat Kebijakan AWS Backup Terkelola.
- Akun tujuan

Akun tujuan adalah akun tempat Anda ingin menyimpan salinan cadangan Anda. Anda dapat memilih lebih dari satu akun tujuan. Akun tujuan harus berada di organisasi yang sama dengan akun sumber di AWS Organizations.

Anda harus "Izinkan" kebijakan akses `backup:CopyIntoBackupVault` untuk brankas cadangan tujuan Anda. Tidak adanya kebijakan ini akan menolak upaya untuk menyalin ke akun tujuan.

- Akun manajemen di AWS Organizations

  Akun manajemen adalah akun utama di organisasi Anda, sebagaimana didefinisikan oleh AWS Organizations, yang Anda gunakan untuk mengelola cadangan lintas akun di seluruh akun Anda Akun AWS. Untuk menggunakan cadangan lintas akun, Anda juga harus mengaktifkan kepercayaan layanan. Setelah mengaktifkan kepercayaan layanan, Anda dapat menggunakan akun apa pun di organisasi sebagai akun tujuan. Dari akun tujuan, Anda dapat memilih brankas mana yang akan digunakan untuk pencadangan lintas akun.
- Aktifkan pencadangan lintas akun di konsol AWS Backup

Untuk informasi tentang keamanan, lihatPertimbangan keamanan untuk pencadangan lintas akun.

Untuk menggunakan cadangan lintas akun, Anda harus mengaktifkan fitur pencadangan lintas akun. Kemudian, Anda harus "Izinkan" kebijakan akses `backup:CopyIntoBackupVault` ke brankas cadangan tujuan Anda.

Aktifkan pencadangan lintas akun

1. Masuk menggunakan kredensil akun AWS Organizations manajemen Anda. Pencadangan lintas akun hanya dapat diaktifkan atau dinonaktifkan menggunakan kredensyal ini.
2. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
3. Di Akun saya, pilih Pengaturan.
4. Untuk pencadangan lintas akun, pilih Aktifkan.
5. Di brankas Cadangan, pilih brankas tujuan Anda.

   Untuk salinan lintas akun, brankas sumber dan brankas tujuan berada di akun yang berbeda. Beralih ke akun yang memiliki akun tujuan, jika perlu.
6. Di bagian Kebijakan akses, "Izinkan"`backup:CopyIntoBackupVault`. Misalnya, pilih Tambahkan izin, lalu Izinkan akses ke brankas Cadangan dari organisasi. Setiap tindakan lintas akun selain `backup:CopyIntoBackupVault` akan ditolak.

7. Sekarang, akun apa pun di organisasi Anda dapat membagikan konten brankas cadangan mereka dengan akun lain di organisasi Anda. Untuk informasi selengkapnya, lihat Berbagi brankas cadangan dengan akun lain AWS. Untuk membatasi akun mana yang dapat menerima konten brankas cadangan akun lain, lihat. Mengonfigurasi akun Anda sebagai akun tujuan

Menjadwalkan pencadangan lintas akun

Anda dapat menggunakan rencana pencadangan terjadwal untuk menyalin cadangan. Akun AWS

Untuk menyalin cadangan menggunakan rencana cadangan terjadwal

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di Akun Saya, pilih Paket Cadangan, lalu pilih Buat paket Cadangan.
3. Pada halaman Buat Rencana Cadangan, pilih Buat paket baru.
4. Untuk nama paket Backup, masukkan nama untuk paket cadangan Anda.
5. Di bagian Konfigurasi aturan Backup, tambahkan aturan cadangan yang menentukan jadwal cadangan, jendela cadangan, dan aturan siklus hidup. Anda dapat menambahkan lebih banyak aturan cadangan nanti.

   Untuk nama Aturan, masukkan nama untuk aturan Anda.
6. Di bagian Jadwal di bawah Frekuensi, pilih seberapa sering Anda ingin cadangan diambil.
7. Untuk jendela Backup, pilih Gunakan default jendela cadangan (disarankan). Anda dapat menyesuaikan jendela cadangan.
8. Untuk Backup vault, pilih vault dari daftar. Poin pemulihan untuk cadangan ini akan disimpan di brankas ini. Anda dapat membuat brankas cadangan baru.
9. Di bagian Hasilkan salinan - opsional, masukkan nilai berikut:

   Wilayah Tujuan

   Pilih tujuan Wilayah AWS untuk salinan cadangan Anda. Cadangan Anda akan disalin ke Wilayah ini. Anda dapat menambahkan aturan salinan baru per salinan ke tujuan baru.

   Salin ke brankas akun lain

   Beralih untuk memilih opsi ini. Opsi berubah menjadi biru saat dipilih. Opsi ARN brankas Eksternal akan muncul.

Brankas eksternal ARN

Masukkan Nama Sumber Daya Amazon (ARN) dari akun tujuan. ARN adalah string yang berisi ID akun dan nya. Wilayah AWS AWS Backup akan menyalin cadangan ke brankas akun tujuan. Daftar wilayah Tujuan secara otomatis diperbarui ke Wilayah di ARN vault eksternal.

Untuk Izinkan akses brankas Cadangan, pilih Izinkan. Kemudian pilih Izinkan di wizard yang terbuka.

AWS Backup membutuhkan izin untuk mengakses akun eksternal untuk menyalin cadangan ke nilai yang ditentukan. Wizard menunjukkan contoh kebijakan berikut yang menyediakan akses ini.

```
{
  "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"
      }
    }
  ]
}
```

Transisi ke penyimpanan dingin

Pilih kapan harus mentransisikan salinan cadangan ke penyimpanan dingin dan kapan harus kedaluwarsa (menghapus) salinannya. Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Nilai ini tidak dapat diubah setelah salinan dialihkan ke penyimpanan dingin.

Untuk melihat daftar sumber daya yang dapat Anda transisi ke penyimpanan dingin, lihat bagian “Siklus Hidup ke penyimpanan dingin” pada Ketersediaan fitur berdasarkan sumber daya tabel. Ekspresi cold storage diabaikan untuk sumber daya lain.

Kedaluwarsa menentukan jumlah hari setelah pembuatan bahwa salinan dihapus. Nilai ini harus lebih besar dari 90 hari di luar nilai Transisi ke penyimpanan dingin.

> **Note**
>
> Saat pencadangan kedaluwarsa dan ditandai untuk dihapus sebagai bagian dari kebijakan siklus hidup Anda, AWS Backup hapus cadangan pada titik yang dipilih secara acak selama 8 jam berikutnya. Jendela ini membantu memastikan kinerja yang konsisten.

10. Pilih Tag yang ditambahkan ke titik pemulihan untuk menambahkan tag ke titik pemulihan Anda.
11. Untuk pengaturan cadangan lanjutan, pilih Windows VSS untuk mengaktifkan snapshot sadar aplikasi untuk perangkat lunak pihak ketiga yang dipilih yang berjalan di EC2.
12. Pilih Buat paket.

Melakukan pencadangan lintas akun sesuai permintaan

Anda dapat menyalin cadangan ke permintaan Akun AWS yang berbeda.

Untuk menyalin cadangan sesuai permintaan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Untuk akun Saya, pilih Backup vault untuk melihat semua brankas cadangan Anda terdaftar. Anda dapat memfilter berdasarkan nama atau tag brankas cadangan.
3. Pilih ID titik pemulihan cadangan yang ingin Anda salin.
4. Pilih Salin.
5. Perluas detail Backup untuk melihat informasi tentang titik pemulihan yang Anda salin.
6. Di bagian Salin konfigurasi, pilih opsi dari daftar wilayah Tujuan.
7. Pilih Salin ke brankas akun lain. Opsi berubah menjadi biru saat dipilih.
8. Masukkan Nama Sumber Daya Amazon (ARN) dari akun tujuan. ARN adalah string yang berisi ID akun dan nya. Wilayah AWS AWS Backup akan menyalin cadangan ke brankas akun tujuan. Daftar wilayah Tujuan secara otomatis diperbarui ke Wilayah di ARN vault eksternal.
9. Untuk Izinkan akses brankas Cadangan, pilih Izinkan. Kemudian pilih Izinkan di wizard yang terbuka.

Untuk membuat salinan, AWS Backup perlu izin untuk mengakses akun sumber. Wizard menunjukkan contoh kebijakan yang menyediakan akses ini. Kebijakan ini ditampilkan sebagai berikut.

```
{
  "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. Untuk Transisi ke penyimpanan dingin, pilih kapan harus mentransisikan salinan cadangan ke penyimpanan dingin dan kapan harus kedaluwarsa (menghapus) salinannya. Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Nilai ini tidak dapat diubah setelah salinan dialihkan ke penyimpanan dingin.

    Untuk melihat daftar sumber daya yang dapat Anda transisi ke penyimpanan dingin, lihat bagian “Siklus Hidup ke penyimpanan dingin” pada Ketersediaan fitur berdasarkan sumber daya tabel. Ekspresi cold storage diabaikan untuk sumber daya lain.

    Kedaluwarsa menentukan jumlah hari setelah pembuatan bahwa salinan dihapus. Nilai ini harus lebih besar dari 90 hari di luar nilai Transisi ke penyimpanan dingin.

11. Untuk peran IAM, tentukan peran IAM (seperti peran default) yang memiliki izin untuk membuat cadangan Anda tersedia untuk disalin. Tindakan menyalin dilakukan oleh peran terkait layanan akun tujuan Anda.

12. Pilih Salin. Bergantung pada ukuran sumber daya yang Anda salin, proses ini bisa memakan waktu beberapa jam untuk menyelesaikannya. Ketika pekerjaan copy selesai, Anda akan melihat salinan di tab Copy jobs di menu Jobs.

Kunci enkripsi dan salinan lintas akun

Kunci enkripsi salinan lintas akun bergantung pada jenis sumber daya. Sumber daya yang telah AWS Backup Manajemen penuh menggunakan kunci enkripsi brankas cadangan sumber. Kunci KMS yang dikelola pelanggan dapat digunakan untuk enkripsi salinan lintas akun dari jenis sumber daya ini.

Jenis sumber daya yang tidak sepenuhnya dikelola oleh AWS Backup memiliki kunci KMS sumber dan kunci KMS sumber daya yang sama. Salinan lintas akun dengan kunci KMS AWS terkelola tidak didukung untuk jenis sumber daya ini yang tidak sepenuhnya dikelola oleh. AWS Backup

Untuk bantuan tambahan pemecahan masalah kegagalan penyalinan lintas akun, silakan lihat Pusat Pengetahuan.AWS

Selama salinan lintas akun, kebijakan kunci KMS akun sumber harus mengizinkan akun tujuan pada kebijakan kunci KMS.

Memulihkan cadangan dari satu Akun AWS ke yang lain

AWS Backup tidak mendukung pemulihan sumber daya dari satu Akun AWS ke yang lain. Namun, Anda dapat menyalin cadangan dari satu akun ke akun lain dan kemudian mengembalikannya di akun itu. Misalnya, Anda tidak dapat memulihkan cadangan dari akun A ke akun B, tetapi Anda dapat menyalin cadangan dari akun A ke akun B, dan kemudian mengembalikannya di akun B.

Memulihkan cadangan dari satu akun ke akun lainnya adalah proses dua langkah.

Untuk mengembalikan cadangan dari satu akun ke akun lainnya

1. Salin cadangan dari sumber Akun AWS ke akun yang ingin Anda pulihkan. Untuk petunjuk, lihat Menyiapkan cadangan lintas akun.
2. Gunakan instruksi yang sesuai untuk sumber daya Anda untuk memulihkan cadangan.

Berbagi brankas cadangan dengan akun lain AWS

AWS Backup memungkinkan Anda berbagi brankas cadangan dengan satu atau beberapa akun, atau seluruh organisasi Anda. AWS Organizations Anda dapat membagikan brankas cadangan tujuan dengan AWS akun sumber, pengguna, atau peran IAM.

Untuk membagikan brankas Cadangan tujuan

1. Pilih AWS Backup, lalu pilih Backup vaults.

2. Pilih nama brankas cadangan yang ingin Anda bagikan.
3. Di panel Kebijakan akses, pilih menu tarik-turun Tambah izin.
4. Pilih Izinkan akses level akun ke brankas Cadangan. Atau, Anda dapat memilih untuk mengizinkan akses tingkat organisasi atau tingkat peran.
5. Masukkan accountID akun yang ingin Anda bagikan dengan brankas cadangan tujuan ini.
6. Pilih Simpan kebijakan.

Anda dapat menggunakan kebijakan IAM untuk membagikan brankas cadangan.

Bagikan brankas cadangan tujuan dengan peran Akun AWS atau IAM

Kebijakan berikut membagikan brankas cadangan dengan nomor akun `4444555566666` dan peran IAM `SomeRole` dalam nomor akun. `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":"*"
    }
  ]
}
```

Bagikan brankas cadangan tujuan unit organisasi di AWS Organizations

Kebijakan berikut membagikan brankas cadangan dengan unit organisasi yang menggunakannya. `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/*"
          ]
        }
      }
    }
  ]
}
```

Bagikan brankas cadangan tujuan dengan organisasi di AWS Organizations

Kebijakan berikut membagikan brankas cadangan dengan organisasi dengan `PrincipalOrgID` “o-a1b2c3d4e5".

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

Mengonfigurasi akun Anda sebagai akun tujuan

Saat pertama kali mengaktifkan pencadangan lintas akun menggunakan akun AWS Organizations manajemen Anda, setiap pengguna akun anggota dapat mengonfigurasi akun mereka menjadi akun tujuan. Sebaiknya setel satu atau beberapa kebijakan kontrol layanan (SCP) berikut AWS Organizations untuk membatasi akun tujuan Anda. Untuk mempelajari selengkapnya tentang melampirkan kebijakan kontrol layanan ke AWS Organizations node, lihat Melampirkan dan melepaskan kebijakan kontrol layanan.

Batasi akun tujuan menggunakan tag

Saat dilampirkan ke AWS Organizations root, OU, atau akun individual, kebijakan ini membatasi tujuan salinan dari root, OU, atau akun tersebut hanya ke akun dengan brankas cadangan yang telah Anda tag. `DestinationBackupVault` Izin `"backup:CopyIntoBackupVault"` mengontrol perilaku brankas cadangan dan, dalam hal ini, brankas cadangan tujuan mana yang valid. Gunakan kebijakan ini, bersama dengan tag terkait yang diterapkan pada brankas tujuan yang disetujui, untuk mengontrol tujuan salinan lintas akun hanya ke akun yang disetujui dan brankas cadangan.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

Batasi akun tujuan menggunakan nomor akun dan nama brankas

Saat dilampirkan ke akun AWS Organizations root, OU, atau individu, kebijakan ini membatasi salinan yang berasal dari root, OU, atau akun tersebut hanya ke dua akun tujuan. Izin `"backup:CopyFromBackupVault"` mengontrol bagaimana titik pemulihan di brankas cadangan berperilaku, dan, dalam hal ini, tujuan tempat Anda dapat menyalin titik pemulihan tersebut. Brankas

sumber hanya akan mengizinkan salinan ke akun tujuan pertama (112233445566) jika satu atau beberapa nama brankas cadangan tujuan dimulai dengan. `cab-` Brankas sumber hanya akan mengizinkan salinan ke akun tujuan kedua (123456789012) jika tujuannya adalah brankas cadangan tunggal bernama. `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"
          ]
        }
      }
    }
  ]
}
```

Batasi akun tujuan menggunakan unit organisasi di AWS Organizations

Saat dilampirkan ke AWS Organizations root atau OU yang berisi akun sumber Anda, atau saat dilampirkan ke akun sumber Anda, kebijakan berikut membatasi akun tujuan ke akun tersebut dalam dua OU yang ditentukan.

```
{
  "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/*"
```

```
            ]
          }
        }
      }
    ]
}
```

Pertimbangan keamanan untuk pencadangan lintas akun

Perhatikan hal-hal berikut saat menggunakan pencadangan lintas akun di: AWS Backup

- Brankas tujuan tidak bisa menjadi vault default. Ini karena vault default dienkripsi dengan kunci yang tidak dapat dibagikan dengan akun lain.
- Pencadangan lintas akun mungkin masih berjalan hingga 15 menit setelah Anda menonaktifkan pencadangan lintas akun. Ini karena konsistensi akhirnya, dan mungkin mengakibatkan beberapa pekerjaan lintas akun dimulai atau diselesaikan bahkan setelah Anda menonaktifkan pencadangan lintas akun.
- Jika akun tujuan meninggalkan organisasi di kemudian hari, akun tersebut akan menyimpan cadangan. Untuk menghindari potensi kebocoran data, letakkan izin penolakan atas `organizations:LeaveOrganization` izin dalam kebijakan kontrol layanan (SCP) yang dilampirkan ke akun tujuan. Untuk informasi selengkapnya tentang SCP, lihat Menghapus akun anggota dari organisasi Anda di Panduan Pengguna Organizations.
- Jika Anda menghapus peran pekerjaan salin selama salinan lintas akun, tidak AWS Backup dapat membatalkan pembagian snapshot dari akun sumber saat pekerjaan penyalinan selesai. Dalam hal ini, pekerjaan pencadangan selesai, tetapi status pekerjaan salin ditampilkan sebagai Gagal untuk membatalkan pembagian snapshot.

Menghapus cadangan

Sebaiknya gunakan AWS Backup untuk secara otomatis menghapus cadangan yang tidak lagi Anda perlukan dengan mengonfigurasi siklus hidup Anda saat membuat paket cadangan. Misalnya, jika Anda mengatur siklus hidup paket cadangan untuk mempertahankan titik pemulihan selama satu tahun, AWS Backup akan secara otomatis menghapus pada 1 Januari 2022 titik pemulihan yang dibuatnya pada atau dalam beberapa jam sejak 1 Januari 2021. (AWS Backup mengacak penghapusannya dalam waktu 8 jam setelah kedaluwarsa titik pemulihan untuk mempertahankan kinerja.) Untuk mempelajari lebih lanjut tentang mengonfigurasi kebijakan retensi siklus hidup Anda, lihat Membuat paket cadangan.

Namun, Anda mungkin ingin menghapus satu atau lebih titik pemulihan secara manual. Sebagai contoh:

- Anda memiliki poin `EXPIRED` pemulihan. Ini AWS Backup adalah titik pemulihan yang tidak dapat dihapus secara otomatis karena Anda menghapus atau mengubah kebijakan IAM asli yang Anda gunakan untuk membuat paket cadangan. Ketika AWS Backup mencoba untuk menghapusnya, itu tidak memiliki izin untuk melakukannya.

  Titik pemulihan yang kedaluwarsa juga dapat dibuat jika titik pemulihan Amazon EBS atau Amazon EC2 yang AWS dikelola memiliki Kunci Snapshot Amazon EBS diterapkan AWS Backup dan tidak dapat menyelesaikan proses siklus hidup yang biasanya mengakibatkan titik pemulihan dihapus. Perhatikan bahwa titik pemulihan yang kedaluwarsa ini dapat dipulihkan dari konsol Amazon EC2 dan API atau konsol dan API Amazon EBS.

  > **Warning**
  >
  > Anda akan terus menyimpan poin pemulihan yang kedaluwarsa di akun Anda. Hal ini dapat meningkatkan biaya penyimpanan Anda.

  Setelah 6 Agustus 2021, AWS Backup akan menampilkan titik pemulihan target sebagai Kedaluwarsa di brankas cadangannya. Anda dapat mengarahkan mouse ke status kedaluwarsa merah untuk pesan status popover yang menjelaskan mengapa tidak dapat menghapus cadangan. Anda juga dapat memilih Refresh untuk menerima informasi terbaru.
- Anda tidak lagi ingin rencana cadangan beroperasi seperti yang Anda konfigurasikan. Memperbarui rencana cadangan memengaruhi titik pemulihan masa depan yang akan dibuatnya, tetapi tidak memengaruhi titik pemulihan yang sudah dibuatnya. Untuk mempelajari lebih lanjut, lihat Memperbarui paket cadangan.
- Anda perlu membersihkan setelah menyelesaikan tes atau tutorial.

Menghapus cadangan secara manual

Untuk menghapus titik pemulihan secara manual

1. Di AWS Backup konsol, di panel navigasi, pilih Backup vaults.
2. Pada halaman Backup vaults, pilih brankas cadangan tempat Anda menyimpan cadangan.
3. Pilih titik pemulihan, pilih dropdown Tindakan, lalu pilih Hapus.

4. 1. Jika daftar Anda berisi cadangan berkelanjutan, pilih salah satu opsi berikut. Setiap cadangan berkelanjutan memiliki satu titik pemulihan.

   - Hapus data cadangan saya secara permanen atau Hapus titik pemulihan. Dengan memilih salah satu opsi ini, Anda menghentikan pencadangan berkelanjutan di masa depan dan juga menghapus data cadangan berkelanjutan yang ada.

     > **Note**
     >
     > Lihat Pencadangan dan point-in-time pemulihan berkelanjutan (PITR) pertimbangan pencadangan berkelanjutan Amazon S3, Amazon RDS, dan Aurora.

   - Simpan data cadangan berkelanjutan saya atau Putuskan titik pemulihan. Dengan memilih salah satu opsi ini, Anda menghentikan pencadangan berkelanjutan masa depan tetapi mempertahankan data cadangan berkelanjutan yang ada hingga kedaluwarsa seperti yang ditentukan oleh periode retensi Anda.

     Titik pemulihan berkelanjutan Amazon S3 yang terputus (cadangan) akan tetap berada di brankas cadangannya, tetapi statusnya akan beralih ke. `STOPPED`

   2. Untuk menghapus semua titik pemulihan yang terdaftar, ketik hapus, lalu pilih Hapus titik pemulihan.
   3. AWS Backup mulai mengirimkan poin pemulihan Anda untuk dihapus dan menampilkan bilah kemajuan. Biarkan tab browser Anda tetap terbuka dan jangan menjauh dari halaman ini selama proses pengiriman.
   4. Di akhir proses pengiriman, beri AWS Backup Anda status di spanduk. Statusnya bisa:
      - Berhasil dikirimkan. Anda dapat memilih untuk Melihat kemajuan tentang status penghapusan setiap titik pemulihan.
      - Gagal mengirimkan. Anda dapat memilih untuk Melihat kemajuan tentang status penghapusan setiap titik pemulihan atau Coba lagi dengan kiriman Anda.
      - Hasil yang beragam di mana beberapa poin pemulihan berhasil diajukan sementara poin pemulihan lainnya gagal dikirimkan.
   5. Jika Anda memilih Lihat kemajuan, Anda dapat meninjau status Penghapusan setiap cadangan. Jika status penghapusan Gagal atau Kedaluwarsa, Anda dapat mengklik status tersebut untuk melihat alasannya. Anda juga dapat memilih untuk Mencoba lagi penghapusan yang gagal.

Pemecahan masalah penghapusan manual

Dalam situasi yang jarang terjadi, AWS Backup mungkin tidak menyelesaikan permintaan penghapusan Anda. AWS Backup menggunakan peran terkait layanan `AWSServiceRoleForBackup` untuk melakukan penghapusan.

Jika permintaan penghapusan Anda gagal, verifikasi bahwa peran IAM Anda memiliki izin untuk membuat peran terkait layanan. Secara khusus, verifikasi peran IAM Anda memiliki `iam:CreateServiceLinkedRole` tindakan. Jika tidak, tambahkan izin ini ke peran yang digunakan untuk membuat cadangan. Menambahkan izin ini memungkinkan AWS Backup untuk melakukan penghapusan manual.

Jika, setelah Anda mengonfirmasi bahwa peran IAM Anda memiliki `iam:CreateServiceLinkedRole` tindakan, titik pemulihan Anda masih terjebak dalam `DELETING` status, kami kemungkinan akan menyelidiki masalah Anda. Selesaikan penghapusan manual Anda dengan langkah-langkah berikut:

1. Siapkan pengingat untuk kembali dalam 2-3 hari.
2. Setelah 2-3 hari, periksa titik `EXPIRED` penghapusan baru-baru ini yang merupakan hasil dari operasi penghapusan manual pertama Anda.
3. Hapus titik `EXPIRED` pemulihan tersebut secara manual.

Untuk informasi selengkapnya tentang peran, lihat Menggunakan peran terkait layanan serta Menambahkan dan menghapus izin identitas IAM.

Mengedit cadangan

Setelah Anda membuat cadangan menggunakan AWS Backup, Anda dapat mengubah siklus hidup atau tag cadangan. Siklus hidup menentukan kapan cadangan dialihkan ke penyimpanan dingin dan kapan cadangan kedaluwarsa. AWS Backup transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Untuk melihat daftar sumber daya yang dapat Anda transisi ke penyimpanan dingin, lihat bagian “Siklus Hidup ke penyimpanan dingin” pada Ketersediaan fitur berdasarkan sumber daya tabel. Ekspresi cold storage diabaikan untuk sumber daya lain.

> **Note**
>
> Mengedit tag cadangan menggunakan AWS Backup konsol hanya didukung untuk cadangan sistem file Amazon Elastic File System (Amazon EFS) dan Advanced Amazon DynamoDB. Tag yang ditambahkan ke titik pemulihan pada pembuatan untuk sumber daya lain masih akan muncul, tetapi akan berwarna abu-abu dan tidak dapat diedit. Meskipun tag ini tidak dapat diedit di AWS Backup konsol, Anda dapat mengedit tag cadangan layanan lain ini menggunakan konsol atau API layanan.

Cadangan yang dialihkan ke cold storage harus disimpan dalam cold storage selama minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Saat Anda memperbarui pengaturan “transisi ke dingin setelah hari”, nilainya harus minimal usia cadangan ditambah satu hari. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Berikut ini adalah contoh cara memperbarui siklus hidup cadangan.

Untuk mengedit siklus hidup cadangan

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Di bagian Backup, pilih cadangan.
4. Pada halaman detail cadangan, pilih Edit.
5. Konfigurasikan pengaturan siklus hidup, lalu pilih Simpan.

Memulihkan cadangan

Cara mengembalikan

Untuk petunjuk pemulihan konsol dan tautan ke dokumentasi untuk setiap jenis sumber daya yang AWS Backup didukung, lihat tautan di bagian bawah halaman ini.

Untuk memulihkan cadangan secara terprogram, gunakan operasi StartRestoreJob API.

Nilai konfigurasi (“restore metadata”) yang Anda butuhkan untuk memulihkan sumber daya bervariasi tergantung pada sumber daya yang ingin Anda pulihkan. Untuk mendapatkan metadata konfigurasi

tempat cadangan Anda dibuat, Anda dapat menelepon. GetRecoveryPointRestoreMetadata Contoh metadata pemulihan juga tersedia di tautan di bagian bawah halaman ini.

Memulihkan dari cold storage biasanya membutuhkan waktu 4 jam lebih banyak daripada memulihkan dari penyimpanan hangat.

Untuk setiap pemulihan, pekerjaan pemulihan dibuat dengan ID pekerjaan yang unik—misalnya,. `1323657E-2AA4-1D94-2C48-5D7A423E7394`

> **Note**
>
> AWS Backup tidak menyediakan perjanjian tingkat layanan (SLA) apa pun untuk waktu pemulihan. Waktu pemulihan dapat bervariasi berdasarkan beban dan kapasitas sistem, bahkan untuk pemulihan yang mengandung sumber daya yang sama.

Pemulihan non-destruktif

Ketika Anda menggunakan AWS Backup untuk memulihkan cadangan, itu menciptakan sumber daya baru dengan cadangan yang Anda pulihkan. Ini untuk melindungi sumber daya Anda yang ada agar tidak dihancurkan oleh aktivitas pemulihan Anda.

Kembalikan pengujian

Anda dapat melakukan tes pada sumber daya Anda untuk mensimulasikan pengalaman pemulihan. Ini membantu menentukan apakah Anda memenuhi Objektif Waktu Pemulihan (RTO) organisasi Anda dan membantu mempersiapkan kebutuhan pemulihan di masa depan.

Untuk informasi selengkapnya, lihat Mengembalikan pengujian.

Salin tag selama pemulihan

> **Note**
>
> Pemulihan Amazon DynamoDB, Amazon S3, SAP HANA pada instans Amazon EC2, mesin virtual, dan sumber daya Amazon Timestream saat ini tidak memiliki fitur ini.

Pengantar

Anda dapat menyalin tag saat memulihkan sumber daya jika tag milik sumber daya yang dilindungi pada saat pencadangan. Tag, yang merupakan label yang berisi pasangan kunci dan nilai, dapat membantu Anda mengidentifikasi dan mencari sumber daya. Saat Anda memulai pekerjaan pemulihan, tag milik sumber daya cadangan asli dapat ditambahkan ke sumber daya yang dipulihkan.

Saat Anda memilih untuk menyertakan tag selama pekerjaan pemulihan, langkah ini dapat menggantikan overhead dan tenaga kerja menerapkan tag secara manual ke sumber daya setelah pekerjaan pemulihan selesai. Perhatikan bahwa ini berbeda dengan menambahkan tag baru ke sumber daya yang dipulihkan.

Saat Anda memulihkan cadangan di alur konsol, tag sumber Anda akan disalin secara default. Di konsol, hapus centang pada kotak jika Anda ingin memilih keluar dari menyalin tag ke sumber daya yang dipulihkan

Dalam operasi API`StartRestoreJob`, parameter `CopySourceTagsToRestoredResource` diatur ke secara `false` default, yang akan mengecualikan tag sumber asli dari sumber daya yang Anda pulihkan. Jika Anda ingin menyertakan tag dari sumber asli, atur ini ke`True`.

Pertimbangan

- Sumber daya dapat memiliki hingga 50 tag, termasuk sumber daya yang dipulihkan. Silakan lihat Menandai AWS sumber daya Anda untuk informasi selengkapnya tentang batas tag.
- Pastikan izin yang benar ada dalam peran yang digunakan untuk mengembalikan untuk menyalin tag. Peran default untuk pemulihan berisi izin yang diperlukan. Peran khusus harus menyertakan izin tambahan untuk menandai sumber daya.
- Sumber daya berikut saat ini tidak didukung untuk memulihkan penyertaan tag: VMware Cloud™ aktif AWS, VMware Cloud™ aktif, sistem lokal, SAP HANA di instans Amazon EC2 AWS Outposts, Timestream, DynamoDB, Advanced DynamoDB, dan Amazon S3.
- Untuk pencadangan berkelanjutan, tag pada sumber daya asli pada cadangan terbaru akan disalin ke sumber daya yang dipulihkan.
- Tag tidak akan disalin untuk pemulihan tingkat item.
- Tag yang ditambahkan ke cadangan setelah pekerjaan pencadangan selesai tetapi tidak ada pada sumber asli sebelum pencadangan tidak akan disalin ke sumber daya yang dipulihkan. Hanya Cadangan yang dibuat setelah 22 Mei 2023 yang memenuhi syarat untuk salinan tag saat pemulihan.

Tag interaksi dengan sumber daya tertentu

- Amazon EC2
  - Tag yang diterapkan ke instans Amazon EC2 yang dipulihkan juga diterapkan ke volume Amazon EBS yang dipulihkan terlampir.
  - Tag yang diterapkan pada volume EBS yang dilampirkan ke instance sumber tidak disalin ke volume yang dilampirkan ke instance yang dipulihkan. Jika Anda memiliki kebijakan IAM yang mengizinkan atau menolak akses pengguna ke volume EBS berdasarkan tag mereka, Anda harus menetapkan ulang tag yang diperlukan secara manual ke volume yang dipulihkan untuk memastikan kebijakan Anda tetap berlaku.
- Saat Anda memulihkan sumber daya Amazon EFS, itu harus disalin ke sistem file baru. Restorasi ke sistem file yang ada tidak dapat memiliki tag yang disalin ke dalamnya.
- Amazon RDS
  - Jika klaster RDS yang dicadangkan masih aktif, tag dari cluster ini akan disalin.
  - Jika cluster asli tidak lagi aktif, tag dari snapshot cluster akan disalin sebagai gantinya.
  - Tag yang ada pada sumber daya pada saat pencadangan akan disalin selama pemulihan terlepas dari apakah parameter Boolean untuk `CopySourceTagsToRestoredResource` diatur ke `True` atau. `False` Namun, jika snapshot tidak mengandung tag, maka pengaturan Boolean di atas akan digunakan.
- Cluster Amazon Redshift, secara default, selalu menyertakan tag selama pekerjaan pemulihan.

Salin tag melalui konsol

1. Buka konsol AWS Backup
2. Di panel navigasi, pilih Sumber daya yang dilindungi, dan pilih ID sumber daya Amazon S3 yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, Anda akan melihat daftar titik pemulihan untuk ID sumber daya yang dipilih. Untuk memulihkan sumber daya:

   a. Di panel Backup, pilih ID titik pemulihan sumber daya.

   b. Di sudut kanan atas panel, pilih Pulihkan (sebagai alternatif, Anda dapat pergi ke brankas cadangan, temukan titik pemulihan, lalu klik Tindakan lalu klik Pulihkan).
4. Pada halaman Restore backup, cari panel bernama Restore with tags. Untuk menyertakan semua tag dari sumber asli, pertahankan centang kotak (perhatikan di konsol kotak ini dicentang secara default).

5. Klik Pulihkan cadangan setelah Anda memilih semua pengaturan dan peran pilihan Anda.

Untuk memasukkan tag secara terprogram

Gunakan operasi API`StartRestoreJob`. Pastikan parameter Boolean berikut diatur ke`True`:

```
CopySourceTagsToRestoredResource = true
```

Jika parameter boolean `CopySourceTagsToRestoredResource` =`True`, pekerjaan pemulihan akan menyalin tag dari sumber daya asli ke materi yang dipulihkan.

> **Important**
>
> Pekerjaan pemulihan akan gagal jika parameter ini disertakan untuk sumber daya yang tidak didukung (VMware,, sistem lokal, SAP HANA pada instans AWS Outposts EC2, Timestream, DynamoDB, Advanced DynamoDB, dan 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
}
```

Memecahkan masalah pemulihan tag

ERROR: Izin Tidak Cukup

REMEDY: Pastikan Anda memiliki izin yang diperlukan dalam peran pemulihan sehingga Anda dapat menyertakan tag pada sumber daya yang dipulihkan. Kebijakan peran layanan AWS terkelola default untuk pemulihan AWSBackupServiceRolePolicyForRestores, berisi izin yang diperlukan untuk tugas ini.

Jika Anda memilih untuk menggunakan peran kustom, pastikan izin berikut ada:

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

Untuk informasi selengkapnya, lihat izin API.

Kembalikan status pekerjaan

Anda dapat melihat status pekerjaan pemulihan di halaman Pekerjaan AWS Backup konsol. Memulihkan status pekerjaan termasuk tertunda, berjalan, selesai, dibatalkan, dan gagal.

Topik

- Memulihkan data S3
- Memulihkan mesin virtual menggunakan AWS Backup
- Memulihkan sistem file FSX
- Memulihkan volume Amazon EBS
- Memulihkan sistem file Amazon EFS
- Memulihkan tabel Amazon DynamoDB
- Memulihkan database RDS
- Memulihkan cluster Amazon Aurora
- Memulihkan instans Amazon EC2
- Memulihkan volume Storage Gateway

- Memulihkan tabel Amazon Timestream
- Memulihkan klaster Amazon Redshift
- Memulihkan database SAP HANA pada instans Amazon EC2
- Memulihkan cluster DocumentDB
- Memulihkan cluster Neptunus
- Kembalikan cadangan CloudFormation tumpukan

Memulihkan data S3

Anda dapat memulihkan data S3 yang Anda backup menggunakan AWS Backup ke kelas penyimpanan Standar S3. Anda dapat mengembalikan semua objek dalam ember atau objek tertentu. Anda dapat mengembalikannya ke ember yang sudah ada atau baru.

Izin pemulihan Amazon S3

Sebelum Anda mulai memulihkan sumber daya, pastikan peran yang Anda gunakan memiliki izin yang memadai.

Untuk informasi selengkapnya, lihat entri kebijakan berikut:

1. `AWSBackupServiceRolePolicyForS3Restore`
2. `AWSBackupServiceRolePolicyForRestores`
3. Kebijakan terkelola untuk AWS Backup

Amazon S3 mengembalikan pertimbangan

- AWS Backup membuat cadangan semua versi S3 Anda, tetapi hanya mengembalikan versi terbaru dari tumpukan versi kapan saja.
- Daftar Kontrol Akses (ACL) harus diaktifkan di bucket tujuan, atau pekerjaan akan gagal jika tidak. Untuk mengaktifkan ACL, ikuti petunjuk di halaman Mengonfigurasi ACL.
- Pemulihan objek dilewati jika bucket sumber memiliki objek dengan nama atau ID versi yang sama.
- Jika Anda memulihkan objek tertentu, Anda dapat mengembalikan versi objek saat ini.
- Saat Anda mengembalikan ke ember S3 asli,
  - AWS Backup tidak melakukan pemulihan destruktif, yang berarti tidak AWS Backup akan menempatkan objek ke dalam ember di tempat objek yang sudah ada, terlepas dari versinya.

  - Penanda hapus dalam versi saat ini diperlakukan sebagai objek sebagai tidak ada, sehingga pemulihan dapat terjadi.
  - AWS Backup tidak menghapus objek (tanpa menghapus penanda) dari ember selama pemulihan (contoh: kunci yang saat ini ada di ember yang tidak ada selama pencadangan akan tetap ada).
- Memulihkan salinan Lintas wilayah
  - Sementara cadangan S3 dapat disalin Lintas wilayah, pekerjaan pemulihan hanya terjadi di Wilayah yang sama di mana cadangan atau salinan asli berada.

    Example

    Contoh: Bucket S3 yang dibuat di Wilayah AS Timur (Virginia N.) dapat disalin ke Wilayah Kanada (Tengah). Pekerjaan pemulihan dapat dimulai menggunakan bucket asli di Wilayah AS Timur (Virginia N.) dan dikembalikan ke Wilayah tersebut, atau pekerjaan pemulihan dapat dimulai menggunakan salinan di Wilayah Kanada (Tengah) dan dikembalikan ke Wilayah tersebut.
  - Metode enkripsi asli tidak dapat digunakan untuk memulihkan titik pemulihan (cadangan) yang disalin dari Wilayah lain. AWS KMS Enkripsi salinan Lintas Wilayah tidak tersedia untuk sumber daya Amazon S3; sebagai gantinya, gunakan jenis enkripsi yang berbeda untuk pekerjaan pemulihan.

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Amazon S3

Untuk memulihkan data Amazon S3 Anda menggunakan konsol: AWS Backup

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi, dan pilih ID sumber daya Amazon S3 yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, Anda akan melihat daftar titik pemulihan untuk ID sumber daya yang dipilih. Untuk memulihkan sumber daya:

   a. Di panel Backup, pilih ID titik pemulihan sumber daya.

   b. Di sudut kanan atas panel, pilih Pulihkan.

      (Atau, Anda dapat pergi ke brankas cadangan, menemukan titik pemulihan, dan kemudian klik Tindakan lalu klik Pulihkan.)

4. Jika Anda memulihkan cadangan berkelanjutan, di panel Restore time, pilih salah satu opsi:

   a. Terima default untuk mengembalikan ke waktu restorable terbaru.

   b. Tentukan tanggal dan waktu untuk memulihkan.

5. Di panel Pengaturan, tentukan apakah akan Mengembalikan seluruh bucket atau melakukan Pemulihan level Item.

   a. Jika Anda memilih Pemulihan level Item, Anda memulihkan hingga 5 item (objek atau folder dalam ember) per tugas pemulihan dengan menentukan URI S3 setiap item yang secara unik mengidentifikasi objek tersebut.

      (Untuk informasi selengkapnya tentang URI bucket S3, lihat Metode untuk mengakses bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.)

   b. Pilih Tambahkan item untuk menentukan item lain untuk dipulihkan.

6. Pilih tujuan Restore Anda. Anda dapat Mengembalikan ke bucket sumber, Menggunakan bucket yang ada, atau Buat bucket baru.

   > **Note**
   >
   > Bucket tujuan pemulihan Anda harus mengaktifkan versi. AWS Backup memberi tahu Anda jika bucket yang Anda pilih tidak memenuhi persyaratan ini.

   a. Jika Anda memilih Gunakan bucket yang ada, pilih bucket S3 tujuan dari menu tarik-turun yang menampilkan semua bucket yang ada di Region Anda saat ini. AWS

   b. Jika Anda memilih Buat bucket baru, ketik nama bucket baru. Bucket baru default ke versi S3 diaktifkan. Pengaturan Block Public Access (BPA) akan dimatikan secara default. Anda dapat mengubah pengaturan ini setelah membuat bucket di S3.

7. Untuk enkripsi objek di bucket S3 Anda, Anda dapat memilih enkripsi objek yang Dipulihkan. Gunakan kunci enkripsi asli (default), kunci Amazon S3 (SSE-S3), atau AWS Key Management Service kunci (SSE-KMS).

   Pengaturan ini hanya berlaku untuk enkripsi objek di bucket S3. Ini tidak mempengaruhi enkripsi untuk bucket itu sendiri.

a. Gunakan kunci enkripsi asli (default) mengembalikan objek dengan kunci enkripsi yang sama yang digunakan oleh objek sumber. Jika objek sumber tidak dienkripsi, metode ini mengembalikan objek tanpa enkripsi.

   Opsi pemulihan ini memungkinkan Anda memilih kunci enkripsi pengganti secara opsional untuk mengenkripsi objek pemulihan jika kunci asli tidak tersedia.

b. Jika Anda memilih kunci Amazon S3 (SSE-S3), Anda tidak perlu menentukan opsi lain.

c. Jika Anda memilih AWS Key Management Service kunci (SSE-KMS), Anda dapat membuat pilihan berikut: Kunci yang dikelola AWS (aws/s3), Pilih dari kunci Anda AWS KMS , atau Masukkan kunci ARN. AWS KMS

   i. Jika Anda memilih Kunci yang dikelola AWS (aws/s3), Anda tidak perlu menentukan opsi lain.

   ii. Jika Anda Pilih dari AWS KMS tombol Anda, pilih AWS KMS tombol dari menu tarik-turun. Atau, pilih Create key.

   iii. Jika Anda Masukkan AWS KMS kunci ARN, ketik ARN ke dalam kotak teks. Atau, pilih Create key.

8. Di panel Pulihkan peran, pilih peran IAM yang AWS Backup akan diasumsikan untuk pemulihan ini.
9. Pilih Pulihkan cadangan. Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Amazon S3

Gunakan `StartRestoreJob`. Anda dapat menentukan metadata berikut selama pemulihan Amazon S3:

```
// 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
```

Status titik pemulihan

Poin pemulihan akan memiliki status yang menunjukkan keadaan mereka.

`PARTIAL`status menunjukkan tidak AWS Backup dapat membuat titik pemulihan sebelum jendela cadangan ditutup. Untuk meningkatkan jendela paket cadangan menggunakan API, lihat UpdateBackupPlan. Anda juga dapat meningkatkan jendela paket cadangan menggunakan Konsol dengan memilih dan mengedit paket cadangan Anda.

`EXPIRED`Status menunjukkan bahwa titik pemulihan telah melebihi periode retensi, tetapi AWS Backup tidak memiliki izin atau sebaliknya tidak dapat menghapusnya. Untuk menghapus titik pemulihan ini secara manual, lihat Langkah 3: Hapus titik pemulihan di bagian Bersihkan sumber daya Memulai.

`STOPPED`status terjadi pada pencadangan berkelanjutan di mana pengguna telah mengambil beberapa tindakan yang menyebabkan pencadangan berkelanjutan dinonaktifkan. Hal ini dapat disebabkan oleh penghapusan izin, mematikan versi, mematikan acara yang dikirim ke Amazon EventBridge, atau menonaktifkan EventBridge aturan yang diberlakukan oleh. AWS Backup

Untuk menyelesaikan `STOPPED` status, pastikan semua izin yang diminta sudah ada dan pembuatan versi diaktifkan di bucket S3. Setelah kondisi ini terpenuhi, contoh berikutnya dari aturan cadangan yang berjalan akan menghasilkan titik pemulihan berkelanjutan baru yang dibuat. Poin pemulihan dengan status STOPTED tidak perlu dihapus.

Memulihkan mesin virtual menggunakan AWS Backup

Anda dapat memulihkan mesin virtual ke VMware, VMware Cloud on, VMware Cloud on AWS, volume Amazon EBS, AWS Outposts atau ke instans Amazon EC2. Memulihkan (atau memigrasikan) mesin virtual ke EC2 memerlukan lisensi. Secara default, AWS akan mencakup lisensi (biaya berlaku). Untuk informasi selengkapnya, lihat Opsi lisensi di Panduan Pengguna Impor/Ekspor VM.

Anda dapat mengembalikan mesin virtual VMware menggunakan AWS Backup konsol atau melalui. AWS CLI Ketika mesin virtual dipulihkan, folder VMware Tools tidak disertakan. Lihat dokumentasi VMware untuk menginstal ulang VMware Tools.

AWS Backup pemulihan mesin virtual bersifat non-destruktif, artinya AWS Backup tidak menimpa mesin virtual yang ada selama pemulihan. Sebagai gantinya, pekerjaan pemulihan menyebarkan mesin virtual baru.

Tugas

- Pertimbangan saat memulihkan VM ke instans Amazon EC2
- Gunakan AWS Backup konsol untuk memulihkan titik pemulihan mesin virtual
- Gunakan AWS CLI untuk mengembalikan titik pemulihan mesin virtual

Pertimbangan saat memulihkan VM ke instans Amazon EC2

- Memulihkan (atau memigrasikan) mesin virtual ke EC2 memerlukan lisensi. Secara default, surat AWS wasiat menyertakan lisensi (dikenakan biaya). Untuk informasi selengkapnya, lihat Opsi lisensi di Panduan Pengguna Impor/Ekspor VM.
- Ada batas maksimum 5 TB (terabyte) untuk setiap disk mesin virtual.
- Anda tidak dapat menentukan key pair saat mengembalikan mesin virtual ke sebuah instance. Anda dapat menambahkan key pair `authorized_keys` selama peluncuran (melalui data pengguna instans) atau setelah peluncuran (seperti yang dijelaskan di bagian pemecahan masalah ini di Panduan Pengguna Amazon EC2).
- Konfirmasikan sistem operasi Anda didukung untuk impor ke dan ekspor dari Amazon EC2 di Panduan Pengguna Impor/Ekspor VM.
- Tinjau batasan yang terkait dengan Mengimpor VM ke Amazon EC2 di Panduan Pengguna Impor/Ekspor VM.
- Saat mengembalikan ke instans Amazon EC2 menggunakan AWS CLI, Anda harus menentukan. `"RestoreTo":"EC2Instance"` Semua atribut lainnya memiliki nilai default.

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan mesin virtual

Anda dapat memulihkan mesin virtual dari beberapa lokasi di panel navigasi kiri AWS Backup konsol:

- Pilih Hypervisor untuk melihat titik pemulihan untuk mesin virtual yang dikelola oleh hypervisor yang terhubung. AWS Backup

- Pilih mesin Virtual untuk melihat titik pemulihan untuk mesin virtual di semua hypervisor Anda yang terhubung. AWS Backup
- Pilih Backup vaults untuk melihat titik pemulihan yang disimpan di brankas tertentu AWS Backup .
- Pilih sumber daya yang dilindungi untuk melihat titik pemulihan di semua sumber daya yang AWS Backup dilindungi.

Jika Anda perlu memulihkan mesin virtual yang tidak lagi memiliki koneksi dengan gateway Backup, pilih Brankas Cadangan atau Sumber daya yang dilindungi untuk menemukan titik pemulihan Anda.

Opsi

- Kembalikan ke VMware
- Pulihkan ke volume Amazon EBS
- Pulihkan ke instans Amazon EC2

Untuk mengembalikan mesin virtual ke VMware, VMware Cloud on, dan VMware Cloud on AWSAWS Outposts

1. Dalam tampilan Hypervisors atau mesin Virtual, pilih nama VM untuk dipulihkan. Dalam tampilan Sumber daya yang dilindungi, pilih ID Sumber Daya mesin virtual untuk dipulihkan.
2. Pilih tombol radial di sebelah ID titik Pemulihan untuk memulihkan.
3. Pilih Pulihkan.
4. Pilih jenis Restore.
    a. Pemulihan penuh mengembalikan semua disk mesin virtual.
    b. Pemulihan tingkat disk mengembalikan pilihan satu atau lebih disk yang ditentukan pengguna. Gunakan menu tarik-turun untuk memilih disk mana yang akan dipulihkan.
5. Pilih lokasi Restore. Pilihannya adalah VMware, VMware Cloud on AWS, dan VMware Cloud on. AWS Outposts
6. Jika Anda melakukan pemulihan penuh, lompat ke langkah berikutnya. Jika Anda melakukan pemulihan tingkat disk, akan ada menu drop-down di bawah disk VM. Pilih satu atau lebih volume yang dapat di-boot untuk dipulihkan.
7. Pilih Hypervisor dari menu tarik-turun untuk mengelola mesin virtual yang dipulihkan

8. Untuk mesin virtual yang dipulihkan, gunakan praktik terbaik mesin virtual organisasi Anda untuk menentukan:

    a. Nama

    b. Jalan (seperti`/datacenter/vm`)

    c. Hitung nama sumber daya (seperti VMHost atau Cluster)

    Jika host adalah bagian dari cluster maka Anda tidak dapat mengembalikan ke host tetapi hanya ke cluster yang diberikan.

    d. Datastore

9. Untuk peran Pulihkan, pilih peran Default (disarankan) atau Pilih peran IAM menggunakan menu tarik-turun.
10. Pilih Pulihkan cadangan.
11. Opsional: Periksa kapan pekerjaan pemulihan Anda memiliki status`Completed`. Di menu navigasi kiri, pilih Jobs.

Untuk mengembalikan mesin virtual ke volume Amazon EBS

1. Dalam tampilan Hypervisors atau mesin Virtual, pilih nama VM untuk dipulihkan. Dalam tampilan Sumber daya yang dilindungi, pilih ID Sumber Daya mesin virtual untuk dipulihkan.
2. Pilih tombol radial di sebelah ID titik Pemulihan untuk memulihkan.
3. Pilih Pulihkan.
4. Pilih jenis Restore.

    - Pemulihan disk mengembalikan pilihan satu disk yang ditentukan pengguna. Gunakan menu tarik-turun untuk memilih disk mana yang akan dipulihkan.

5. Pilih lokasi Pulihkan sebagai Amazon EBS.
6. Di bawah menu tarik-turun disk VM, pilih volume yang dapat di-boot untuk dipulihkan.
7. Di bawah tipe Volume EBS, pilih jenis volume.
8. Pilih Availability Zone Anda.
9. Enkripsi (opsional). Centang kotak jika Anda memilih untuk mengenkripsi volume EBS.
10. Pilih tombol KMS Anda dari menu.
11. Untuk Memulihkan peran, pilih peran Default (disarankan) atau Pilih peran IAM.

12. Pilih Pulihkan cadangan.
13. Opsional: Periksa kapan pekerjaan pemulihan Anda memiliki status`Completed`. Di menu navigasi kiri, pilih Jobs.
14. Opsional: Kunjungi Bagaimana cara membuat volume logis LVM pada seluruh volume Amazon EBS? untuk mempelajari lebih lanjut tentang cara memasang volume terkelola dan mengakses data pada volume Amazon EBS yang dipulihkan.

Untuk mengembalikan mesin virtual ke instans Amazon EC2

1. Dalam tampilan Hypervisors atau mesin Virtual, pilih nama VM untuk dipulihkan. Dalam tampilan Sumber daya yang dilindungi, pilih ID Sumber Daya mesin virtual untuk dipulihkan.
2. Pilih tombol radial di sebelah ID titik Pemulihan untuk memulihkan.
3. Pilih Pulihkan.
4. Pilih jenis Restore.
   - Pemulihan penuh mengembalikan sistem file sepenuhnya, termasuk folder dan file tingkat root.
5. Pilih lokasi Pulihkan sebagai Amazon EC2.
6. Untuk tipe Instance, pilih kombinasi komputasi dan memori yang diperlukan untuk menjalankan aplikasi Anda pada instance baru Anda.

   > **Tip**
   >
   > Pilih jenis instance yang cocok atau melebihi spesifikasi mesin virtual asli. Untuk informasi selengkapnya, lihat Panduan Jenis Instans Amazon EC2.

7. Untuk Virtual Private Cloud (VPC), pilih virtual private cloud (VPC), yang mendefinisikan lingkungan jaringan untuk instance.
8. Untuk Subnet, pilih salah satu subnet di VPC. Instans Anda menerima alamat IP pribadi dari rentang alamat subnet.
9. Untuk grup keamanan, pilih grup keamanan, yang bertindak sebagai firewall untuk lalu lintas ke instans Anda.
10. Untuk Memulihkan peran, pilih peran Default (disarankan) atau Pilih peran IAM.

11. Opsional: Untuk menjalankan skrip pada instans Anda saat peluncuran, perluas Pengaturan lanjutan dan masukkan skrip dalam data Pengguna.
12. Pilih Pulihkan cadangan.
13. Opsional: Periksa kapan pekerjaan pemulihan Anda memiliki status`Completed`. Di menu navigasi kiri, pilih Jobs.

Gunakan AWS CLI untuk mengembalikan titik pemulihan mesin virtual

Gunakan `StartRestoreJob`.

Anda dapat menentukan metadata berikut untuk pemulihan mesin virtual ke Amazon EC2 dan Amazon EBS:

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

Anda dapat menentukan metadata berikut untuk pemulihan mesin virtual ke VMware, VMware Cloud on, dan VMware cloud di Outpost AWS: AWS

```
RestoreTo
HypervisorArn
```

```
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

Contoh ini menunjukkan cara melakukan pemulihan penuh ke 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"}'
```

Memulihkan sistem file FSX

Opsi pemulihan yang tersedia saat Anda gunakan AWS Backup untuk memulihkan sistem file Amazon FSx sama dengan menggunakan cadangan Amazon FSx asli. Anda dapat menggunakan titik pemulihan cadangan untuk membuat sistem file baru dan mengembalikan point-in-time snapshot dari sistem file lain.

Saat memulihkan sistem file Amazon FSx AWS Backup , buat sistem file baru dan isi dengan data (Amazon FSx NetApp untuk ONTAP memungkinkan mengembalikan volume ke sistem file yang ada). Ini mirip dengan bagaimana Amazon FSx asli mencadangkan dan memulihkan sistem file. Memulihkan backup ke sistem file yang baru menghabiskan waktu yang sama dengan membuat sistem file baru. Data yang dipulihkan dari cadangan dimuat dengan lambat ke sistem file. Oleh karena itu, Anda mungkin mengalami latensi yang sedikit lebih tinggi selama proses tersebut.

> **Note**
>
> Anda tidak dapat memulihkan ke sistem file Amazon FSx yang ada, dan Anda tidak dapat memulihkan file atau folder individual.
> FSx untuk ONTAP tidak mendukung pencadangan jenis volume tertentu, termasuk volume DP (perlindungan data), volume LS (berbagi beban), volume penuh, atau volume pada sistem file yang penuh. Untuk informasi lebih lanjut, silakan lihat FSx untuk ONTAP Bekerja dengan cadangan.
> AWS Backup brankas yang berisi titik pemulihan sistem file Amazon FSx terlihat di luar. AWS Backup Anda dapat memulihkan titik pemulihan menggunakan Amazon FSx tetapi Anda tidak dapat menghapusnya.

Anda dapat melihat cadangan yang dibuat oleh fungsionalitas pencadangan otomatis Amazon FSx bawaan dari konsol. AWS Backup Anda juga dapat memulihkan cadangan ini menggunakan. AWS Backup Namun, Anda tidak dapat menghapus cadangan ini atau mengubah jadwal pencadangan otomatis sistem file Amazon FSx Anda menggunakan. AWS Backup

Anda dapat memulihkan cadangan yang dibuat dengan AWS Backup menggunakan AWS Backup konsol, API, atau. AWS CLI Bagian ini menunjukkan cara menggunakan AWS Backup konsol untuk memulihkan sistem file Amazon FSx.

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Amazon FSx

Memulihkan sistem file FSx for Windows File Server

Untuk memulihkan sistem file FSx for Windows File Server

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi, lalu pilih ID sumber daya Amazon FSx yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Pilih ID titik pemulihan sumber daya.
4. Di sudut kanan atas panel, pilih Pulihkan untuk membuka halaman Pulihkan cadangan.
5. Di bagian Detail sistem file, ID cadangan Anda ditampilkan di bawah ID Cadangan, dan jenis sistem file ditampilkan di bawah Jenis sistem file. Anda dapat memulihkan sistem file FSx for Windows File Server dan FSx for Lustre.
6. Untuk jenis Deployment, terima default. Anda tidak dapat mengubah jenis penyebaran sistem file selama pemulihan.
7. Pilih jenis Penyimpanan yang akan digunakan. Jika kapasitas penyimpanan sistem file Anda kurang dari 2.000 GiB, Anda tidak dapat menggunakan jenis penyimpanan HDD.
8. Untuk kapasitas Throughput, pilih Kapasitas throughput yang disarankan untuk menggunakan laju 16 MB per detik (MBps) yang disarankan, atau pilih Tentukan kapasitas throughput dan masukkan tarif baru.
9. Di bagian Jaringan dan keamanan, berikan informasi yang diperlukan.
10. Jika Anda memulihkan sistem file FSx for Windows File Server, berikan informasi otentikasi Windows yang digunakan untuk mengakses sistem file, atau Anda dapat membuat yang baru.

> **Note**
>
> Saat memulihkan cadangan, Anda tidak dapat mengubah jenis Active Directory pada sistem file.

Untuk informasi selengkapnya tentang Microsoft Active Directory, lihat Bekerja dengan Active Directory di Amazon FSx for Windows File Server dalam Panduan Pengguna Amazon FSx for Windows File Server.

11. (Opsional) Di bagian Cadangan dan pemeliharaan, berikan informasi untuk mengatur preferensi cadangan Anda.
12. Di bagian Pulihkan peran, pilih peran IAM yang AWS Backup akan digunakan untuk membuat dan mengelola cadangan Anda atas nama Anda. Kami menyarankan Anda memilih peran Default. Jika tidak ada peran default, satu akan dibuat untuk Anda dengan izin yang benar. Anda juga dapat memberikan peran IAM Anda sendiri.
13. Verifikasi semua entri Anda, dan pilih Pulihkan Cadangan.

Memulihkan sistem file Amazon FSx for Lustre

AWS Backup mendukung sistem file Amazon FSx for Lustre yang memiliki tipe penyebaran penyimpanan persisten dan tidak ditautkan ke repositori data seperti Amazon S3.

Untuk mengembalikan sistem file Amazon FSx for Lustre

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi, lalu pilih ID sumber daya Amazon FSx yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Pilih ID titik pemulihan sumber daya.
4. Di sudut kanan atas panel, pilih Pulihkan untuk membuka halaman Kembalikan cadangan ke sistem file baru.
5. Di bagian Pengaturan, ID cadangan Anda ditampilkan di bawah ID Cadangan, dan jenis sistem file ditampilkan di bawah Jenis sistem file. Jenis sistem file harus Lustre.
6. (Opsional) Masukkan nama untuk sistem file Anda.

7. Pilih jenis Deployment. AWS Backup hanya mendukung jenis penerapan persisten. Anda tidak dapat mengubah jenis penyebaran sistem file selama pemulihan.

   Jenis penerapan persisten adalah untuk penyimpanan jangka panjang. Untuk informasi mendetail tentang opsi penyebaran FSx for Lustre, lihat Menggunakan Opsi Penerapan yang Tersedia untuk Amazon FSx for Lustre File Systems di Panduan Pengguna Amazon FSx for Lustre.
8. Pilih Throughput per unit penyimpanan yang ingin Anda gunakan.
9. Tentukan kapasitas Penyimpanan yang akan digunakan. Masukkan kapasitas antara 32 GiB dan 64.436 GiB.
10. Di bagian Jaringan dan keamanan, berikan informasi yang diperlukan.
11. (Opsional) Di bagian Cadangan dan pemeliharaan, berikan informasi untuk mengatur preferensi cadangan Anda.
12. Di bagian Pulihkan peran, pilih peran IAM yang AWS Backup akan digunakan untuk membuat dan mengelola cadangan Anda atas nama Anda. Kami menyarankan Anda memilih peran Default. Jika tidak ada peran default, satu akan dibuat untuk Anda dengan izin yang benar. Anda juga dapat memberikan peran IAM Anda.
13. Verifikasi semua entri Anda, dan pilih Pulihkan Cadangan.

Memulihkan Amazon FSx NetApp untuk volume ONTAP

Untuk memulihkan Amazon FSx untuk volume NetApp ONTAP:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi, lalu pilih ID sumber daya Amazon FSx yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Pilih ID titik pemulihan sumber daya.
4. Di sudut kanan atas panel, pilih Pulihkan untuk membuka halaman Pulihkan.

   Bagian pertama, rincian sistem file, menampilkan ID titik pemulihan, ID sistem file, dan jenis sistem file.
5. Di bawah opsi Pulihkan, ada beberapa pilihan. Pertama, pilih sistem File dari menu dropdown.
6. Selanjutnya, pilih mesin virtual Penyimpanan yang disukai dari menu tarik-turun.
7. Masukkan nama untuk volume Anda.

8. Tentukan Jalur Persimpangan, yang merupakan lokasi dalam sistem file Anda di mana volume Anda akan dipasang.
9. Tentukan ukuran Volume dalam megabyte (MB) yang Anda buat.
10. (Opsional) Anda dapat memilih untuk Mengaktifkan efisiensi penyimpanan dengan mencentang kotak. Ini akan memungkinkan deduplikasi, kompresi, dan pemadatan.
11. Di menu tarik-turun kebijakan tiering kumpulan kapasitas, pilih preferensi tiering.
12. Dalam izin Pulihkan, pilih peran IAM yang AWS Backup akan digunakan untuk memulihkan cadangan.
13. Verifikasi semua entri Anda, dan pilih Pulihkan Cadangan.

Memulihkan Amazon FSx untuk sistem file OpenZFS

Untuk mengembalikan sebuah FSx untuk sistem file OpenZFS

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi, lalu pilih ID sumber daya Amazon FSx yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Pilih ID titik pemulihan sumber daya.
4. Di sudut kanan atas panel, pilih Pulihkan untuk membuka halaman Pulihkan cadangan.

   Di bagian Detail sistem file, ID cadangan Anda ditampilkan di bawah ID Cadangan, dan jenis sistem file ditampilkan di bawah Jenis sistem file. Jenis sistem file harus FSx untuk OpenZFS.
5. Di bawah opsi Pemulihan, Anda dapat memilih Pemulihan cepat atau Pemulihan standar. Pemulihan cepat akan menggunakan pengaturan default sistem file sumber. Jika Anda melakukan Quick Restore, lewati ke Langkah 7.

   Jika Anda memilih Pemulihan standar, tentukan konfigurasi tambahan berikut:

   a. IOPS SSD yang disediakan: Anda dapat memilih tombol radio Otomatis atau Anda dapat memilih opsi yang disediakan Pengguna jika tersedia.
   b. Kapasitas throughput: Anda dapat memilih kapasitas throughput yang disarankan 64 MB/detik atau Anda dapat memilih untuk Menentukan kapasitas throughput.
   c. (Opsional) Grup keamanan VPC: Anda dapat menentukan grup keamanan VPC untuk dikaitkan dengan antarmuka jaringan sistem file Anda.

d. Kunci enkripsi: Tentukan AWS Key Management Service kunci untuk melindungi data sistem file yang dipulihkan saat istirahat.

e. (Opsional) Konfigurasi Volume Root: Konfigurasi ini diciutkan secara default. Anda dapat memperluasnya dengan mengklik karat yang mengarah ke bawah (panah). Membuat sistem file dari cadangan akan membuat sistem file baru; volume dan snapshot akan mempertahankan konfigurasi sumbernya.

f. (Opsional) Pencadangan dan pemeliharaan: Untuk mengatur cadangan terjadwal, klik karat penunjuk ke bawah (panah) untuk memperluas bagian. Anda dapat memilih jendela cadangan, jam dan menit, periode retensi, dan jendela pemeliharaan mingguan.

6. (Opsional) Anda dapat memasukkan nama untuk volume Anda.
7. Kapasitas Penyimpanan SSD akan menampilkan kapasitas penyimpanan sistem file.
8. Pilih Virtual Private Cloud (VPC) dari mana sistem file Anda dapat diakses.
9. Di menu dropdown Subnet, pilih subnet tempat antarmuka jaringan sistem file Anda berada.
10. Di bagian Pulihkan peran, pilih peran IAM yang AWS Backup akan digunakan untuk membuat dan mengelola cadangan Anda atas nama Anda. Kami menyarankan Anda memilih peran Default. Jika tidak ada peran default, satu akan dibuat untuk Anda dengan izin yang benar. Anda juga dapat memilih peran IAM.
11. Verifikasi semua entri Anda, dan pilih Pulihkan Cadangan.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Amazon FSx

Untuk memulihkan Amazon FSx menggunakan API atau CLI, gunakan. `StartRestoreJob` Anda dapat menentukan metadata berikut selama pemulihan Amazon FSx apa pun:

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
```

```
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

fsX for Windows File Server mengembalikan metadata

Anda dapat menentukan metadata berikut selama pemulihan FSx for Windows File Server:

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

FSx for Lustre restore metadata

Anda dapat menentukan berikut `PerUnitStorageThroughput` dan `DriveCacheType` selama FSx for Lustre restore.

fsX untuk metadata pemulihan ONTAP

Anda dapat menentukan metadata berikut selama fsX untuk pemulihan ONTAP:

- Nama #name volume yang akan dibuat
- OntapConfiguration: # konfigurasi ontap
- `junctionPath`
- `sizeInMegabytes`
- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

FSx untuk OpenZFS mengembalikan metadata

Anda dapat menentukan metadata berikut selama fsX untuk pemulihan OpenZFS:

- `ThroughputCapacity`
- `DesklopsConfiguration`

- Jika Iops jika ditentukan, Anda harus menyertakan nilai antara 0 dan 160.000, tetapi tidak termasuk Mode.

Contoh perintah pemulihan 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\"}"'
```

Contoh mengembalikan metadata:

```
"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\\\"]\"}"
```

Memulihkan volume Amazon EBS

Saat memulihkan snapshot Amazon Elastic Block Store (Amazon EBS), AWS Backup buat volume Amazon EBS baru yang dapat Anda lampirkan ke instans Amazon EC2 Anda.

Anda dapat memilih untuk mengembalikan snapshot sebagai volume EBS atau sebagai AWS Storage Gateway volume.

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Amazon EBS

Untuk memulihkan volume Amazon EBS

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi lalu pilih ID sumber daya EBS yang ingin dipulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.

4. Tentukan parameter pemulihan untuk sumber daya Anda. Parameter pemulihan yang Anda masukkan khusus untuk jenis sumber daya yang Anda pilih.

   Untuk jenis Sumber Daya, pilih AWS sumber daya yang akan dibuat saat memulihkan cadangan ini.

5. Jika Anda memilih volume EBS, berikan nilai untuk tipe Volume, Ukuran (GiB), dan pilih zona Ketersediaan.

   - Setelah Throughput, akan ada kotak centang opsional Enkripsi volume ini. Opsi ini akan tetap aktif jika titik pemulihan EBS dienkripsi.

     Anda dapat menentukan kunci KMS atau Anda dapat membuat AWS KMS kunci.

   Jika Anda memilih volume Storage Gateway, pilih Gateway dalam status yang dapat dijangkau. Juga pilih nama target iSCSI Anda.

   - Untuk gateway yang disimpan Volume, pilih Id Disk.
   - Untuk gateway Volume yang di-cache, pilih kapasitas yang setidaknya sebesar sumber daya yang dilindungi.

6. Untuk peran Restore, pilih peran IAM yang AWS Backup akan diasumsikan untuk pemulihan ini.

   > **Note**
   >
   > Jika peran AWS Backup default tidak ada di akun Anda, peran Default dibuat untuk Anda dengan izin yang benar. Anda dapat menghapus peran default ini atau membuatnya tidak dapat digunakan.

7. Pilih Pulihkan cadangan.

   Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.

Memulihkan snapshot EBS yang diarsipkan memindahkannya dari penyimpanan dingin ke penyimpanan hangat sementara untuk membuat volume EBS baru. Jenis pemulihan ini menimbulkan biaya pengambilan satu kali. Biaya penyimpanan untuk penyimpanan hangat dan dingin ditagih selama periode pemulihan ini. Volume EBS di cold storage tidak dapat dikembalikan ke volume gateway Backup.

Anda dapat memulihkan snapshot EBS yang diarsipkan di cold storage dengan menggunakan AWS Backup konsol atau baris perintah. Pemulihan dari cold storage bisa memakan waktu hingga 72 jam. Untuk informasi selengkapnya, lihat Mengarsipkan snapshot Amazon EBS di Panduan Pengguna Amazon EBS.

Console

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Arahkan ke Brankas Cadangan > ***Vault*** > Pulihkan snapshot EBS yang diarsipkan.
3. Di bagian Pengaturan, masukkan nilai dari 0 hingga 180, inklusif, yang menentukan jumlah hari untuk memulihkan snapshot yang diarsipkan sementara.
4. Masukkan pengaturan lain: jenis volume, ukuran, IOPS, zona ketersediaan, throughput, dan enkripsi.
5. Pilih peran pemulihan Anda.
6. Pilih Pulihkan cadangan. Pada pop up konfirmasi, konfirmasikan snapshot dan mengembalikan jenis. Kemudian, pilih Pulihkan snapshot.

AWS CLI

1. Gunakan `start-restore-job`
2. Sertakan parameternya.
3.
4.
5.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Amazon EBS

Untuk memulihkan Amazon EBS menggunakan API atau CLI, gunakan. `StartRestoreJob` Anda dapat menentukan metadata berikut selama pemulihan Amazon EBS:

```
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
```

Contoh:

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

Memulihkan sistem file Amazon EFS

Jika memulihkan instans Amazon Elastic File System (Amazon EFS), Anda dapat melakukan pemulihan penuh atau pemulihan tingkat item.

Pemulihan Penuh

Ketika Anda melakukan pemulihan penuh, seluruh sistem file dipulihkan.

AWS Backup tidak mendukung pemulihan destruktif dengan Amazon EFS. Restore destruktif adalah ketika sistem file yang dipulihkan menghapus atau menimpa sumber atau sistem file yang ada. Sebagai gantinya, AWS Backup kembalikan sistem file Anda ke direktori pemulihan dari direktori root.

Pemulihan Tingkat Item

Saat Anda melakukan pemulihan tingkat item, AWS Backup mengembalikan file atau direktori tertentu. Anda harus menentukan jalur relatif terhadap root sistem file. Misalnya, jika sistem file dipasang `/user/home/myname/efs` dan jalur file`user/home/myname/efs/file1`, Anda masuk**`/file1`**. Jalur peka huruf besar/kecil. Karakter wildcard dan string regex tidak didukung. Jalur Anda mungkin berbeda dari apa yang ada di host jika sistem file dipasang menggunakan titik akses.

Anda dapat memilih hingga 10 item saat menggunakan konsol untuk melakukan pemulihan EFS. Tidak ada batasan item saat Anda menggunakan CLI untuk memulihkan; Namun, ada batas 200 KB pada panjang metadata pemulihan yang dapat dilewatkan.

Anda dapat mengembalikan item tersebut ke sistem file baru atau yang sudah ada. Either way, AWS Backup buat direktori Amazon EFS (`aws-backup-restore_`*`datetime`*) baru dari direktori root untuk memuat item. Hirarki penuh dari item yang ditentukan dipertahankan dalam direktori pemulihan. Misalnya, jika direktori A berisi subdirektori B, C, dan D, AWS Backup mempertahankan

struktur hierarkis ketika A, B, C, dan D dipulihkan. Terlepas dari apakah Anda melakukan pemulihan tingkat item Amazon EFS ke sistem file yang ada atau ke sistem file baru, setiap upaya pemulihan membuat direktori pemulihan baru dari direktori root untuk berisi file yang dipulihkan. Jika Anda mencoba beberapa pemulihan untuk jalur yang sama, beberapa direktori yang berisi item yang dipulihkan mungkin ada.

> **Note**
>
> Jika Anda hanya menyimpan satu cadangan mingguan, Anda hanya dapat mengembalikan ke keadaan sistem file pada saat Anda mengambil cadangan itu. Anda tidak dapat mengembalikan ke backup inkremental sebelumnya.

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Amazon EFS

Untuk memulihkan sistem file Amazon EFS

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Vault cadangan EFS Anda menerima kebijakan akses `Deny backup:StartRestoreJob` saat pembuatan. Jika memulihkan brankas cadangan untuk pertama kalinya, Anda harus mengubah kebijakan akses sebagai berikut.

   a. Pilih Brankas Cadangan.

   b. Pilih brankas cadangan yang berisi titik pemulihan yang ingin Anda pulihkan.

   c. Gulir ke bawah ke kebijakan Akses vault

   d. Jika ada, hapus `backup:StartRestoreJob` dari`Statement`. Lakukan ini dengan memilih Edit, menghapus`backup:StartRestoreJob`, lalu memilih Simpan kebijakan.
3. Di panel navigasi, pilih Sumber daya yang dilindungi dan ID sistem file EFS yang ingin Anda pulihkan.
4. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sistem file yang dipilih ditampilkan. Untuk mengembalikan sistem file, di panel Backups, pilih tombol radio di sebelah ID titik pemulihan sistem file. Di sudut kanan atas panel, pilih Pulihkan.
5. Tentukan parameter pemulihan untuk sistem file Anda. Parameter pemulihan yang Anda masukkan khusus untuk jenis sumber daya yang Anda pilih.

   Anda dapat melakukan Pemulihan penuh, yang mengembalikan seluruh sistem file. Atau, Anda dapat memulihkan file dan direktori tertentu menggunakan pemulihan tingkat Item.

- Pilih opsi Pemulihan penuh untuk memulihkan sistem file secara keseluruhan termasuk semua folder dan file tingkat root.
- Pilih opsi Pemulihan tingkat item untuk memulihkan file atau direktori tertentu. Anda dapat memilih dan memulihkan hingga lima item dalam Amazon EFS Anda.

  Untuk mengembalikan file atau direktori tertentu, Anda harus menentukan jalur relatif yang terkait dengan titik pemasangan. Misalnya, jika sistem file dipasang `/user/home/myname/efs` dan jalur file`user/home/myname/efs/file1`, masukkan**`/file1`**. Jalur peka huruf besar/kecil dan tidak dapat berisi karakter khusus, karakter wildcard, dan string regex.

  1. Di kotak teks Jalur item, masukkan jalur untuk file atau folder Anda.
  2. Pilih Tambahkan item untuk menambahkan file atau direktori tambahan. Anda dapat memilih dan memulihkan hingga lima item dalam sistem file EFS Anda.

6. Untuk Pulihkan lokasi

   - Pilih Pulihkan ke direktori di sistem file sumber jika Anda ingin mengembalikan ke sistem file sumber.
   - Pilih Pulihkan ke sistem file baru jika Anda ingin mengembalikan ke sistem file yang berbeda.

7. Untuk tipe sistem File

   - (Disarankan) Pilih Regional jika Anda ingin memulihkan sistem file Anda di beberapa AWS Availability Zone.
   - Pilih One Zone jika Anda ingin mengembalikan sistem file Anda ke Availability Zone tunggal. Kemudian, di dropdown Availability Zone, pilih tujuan pemulihan Anda.

   Untuk informasi selengkapnya, lihat Mengelola kelas penyimpanan Amazon EFS di Panduan Pengguna Amazon EFS.

8. Untuk Kinerja

   - Jika Anda memilih untuk melakukan pemulihan Regional, pilih salah satu (Disarankan) Tujuan umum atau Max I/O.
   - Jika Anda memilih untuk melakukan pemulihan One Zone, Anda harus memilih (Disarankan) Tujuan umum. Pemulihan One Zone tidak mendukung Max I/O.

9. Untuk Aktifkan enkripsi

- Pilih Aktifkan enkripsi, jika Anda ingin mengenkripsi sistem file Anda. ID kunci KMS dan alias muncul dalam daftar setelah dibuat menggunakan konsol AWS Key Management Service (AWS KMS).
- Di kotak teks kunci KMS, pilih kunci yang ingin Anda gunakan dari daftar.

10. Untuk peran Restore, pilih peran IAM yang AWS Backup akan diasumsikan untuk pemulihan ini.

> **Note**
>
> Jika peran AWS Backup default tidak ada di akun Anda, peran Default dibuat untuk Anda dengan izin yang benar. Anda dapat menghapus peran default ini atau membuatnya tidak dapat digunakan.

11. Pilih Pulihkan cadangan.

    Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.

> **Note**
>
> Jika Anda hanya menyimpan satu cadangan mingguan, Anda hanya dapat mengembalikan ke keadaan sistem file pada saat Anda mengambil cadangan itu. Anda tidak dapat mengembalikan ke backup inkremental sebelumnya.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Amazon EFS

Gunakan `StartRestoreJob`. Saat memulihkan instans Amazon EFS, Anda dapat memulihkan seluruh sistem file atau file atau direktori tertentu. Untuk memulihkan sumber daya Amazon EFS, Anda memerlukan informasi berikut:

- `file-system-id`— ID sistem file Amazon EFS yang didukung oleh AWS Backup. Kembali masuk`GetRecoveryPointRestoreMetadata`. Ini tidak diperlukan ketika sistem file baru dipulihkan (nilai ini diabaikan jika parameter `newFileSystem`True).
- `Encrypted`— Nilai Boolean yang, jika benar, menentukan bahwa sistem file dienkripsi. Jika `KmsKeyId` ditentukan, `Encrypted` harus diatur ke`true`.

- `KmsKeyId`— Menentukan AWS KMS kunci yang digunakan untuk mengenkripsi sistem file dipulihkan.
- `PerformanceMode`— Menentukan modus throughput dari sistem file.
- `CreationToken`— Nilai yang disediakan pengguna yang memastikan keunikan (idempotensi) permintaan.
- `newFileSystem`— Nilai Boolean yang, jika benar, menentukan bahwa titik pemulihan dikembalikan ke sistem file Amazon EFS baru.
- `ItemsToRestore` — Array hingga lima string di mana setiap string adalah jalur file. Gunakan `ItemsToRestore` untuk mengembalikan file atau direktori tertentu daripada seluruh sistem file. Parameter ini bersifat opsional.

Anda juga dapat memasukkan`aws:backup:request-id`.

Pemulihan One Zone dapat dilakukan dengan memasukkan parameter:

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

Untuk informasi selengkapnya tentang nilai konfigurasi Amazon EFS, lihat create-file-system.

Menonaktifkan pencadangan otomatis di Amazon EFS

Secara default, Amazon EFS membuat cadangan data secara otomatis. Cadangan ini direpresentasikan sebagai titik pemulihan di. AWS Backup Upaya untuk menghapus titik pemulihan akan menghasilkan pesan kesalahan yang mencatat ada hak istimewa yang tidak memadai untuk melakukan tindakan.

Ini adalah praktik terbaik untuk menjaga pencadangan otomatis ini tetap aktif. Khususnya dalam kasus penghapusan data yang tidak disengaja, cadangan ini memungkinkan pemulihan konten sistem file ke tanggal titik pemulihan terakhir dibuat.

Jika Anda ingin menonaktifkannya, kebijakan akses harus diubah dari `"Effect": "Deny"` ke`"Effect": "Allow"`. Lihat Panduan Pengguna Amazon EFS untuk informasi selengkapnya tentang mengaktifkan atau menonaktifkan pencadangan otomatis.

Memulihkan tabel Amazon DynamoDB

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan DynamoDB

Untuk mengembalikan tabel DynamoDB

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi dan ID sumber daya DynamoDB yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.
4. Untuk Pengaturan, kolom teks nama tabel baru, masukkan nama tabel baru.
5. Untuk peran Restore, pilih peran IAM yang AWS Backup akan diasumsikan untuk pemulihan ini.
6. Untuk pengaturan Enkripsi:

   a. Jika cadangan Anda dikelola oleh DynamoDB (ARN-nya dimulai `arn:aws:dynamodb` dengan) AWS Backup , mengenkripsi tabel yang dipulihkan menggunakan kunci yang dimiliki. AWS

      Untuk memilih kunci yang berbeda untuk mengenkripsi tabel yang dipulihkan, Anda dapat menggunakan AWS Backup StartRestoreJoboperasi atau melakukan pemulihan dari konsol DynamoDB.

   b. Jika cadangan Anda mendukung AWS Backup manajemen penuh (ARN dimulai dengan`arn:aws:backup`), Anda dapat memilih salah satu opsi enkripsi berikut untuk melindungi tabel yang dipulihkan:

      - (Default) Kunci KMS milik DynamoDB (tidak ada biaya tambahan untuk enkripsi)
      - Kunci KMS yang dikelola DynamoDB (dikenakan biaya KMS)
      - Kunci KMS yang dikelola pelanggan (dikenakan biaya KMS)

      Kunci “dimiliki DynamoDB” dan “dikelola DynamoDB” masing-masing sama dengan kunci “AWS-owned” dan “-managed”.AWS Untuk klarifikasi, lihat Enkripsi saat Istirahat: Cara Kerjanya di Panduan Pengembang Amazon DynamoDB.

Untuk informasi selengkapnya tentang AWS Backup manajemen lengkap, lihatCadangan DynamoDB tingkat lanjut.

> **Note**
>
> Panduan berikut hanya berlaku jika Anda mengembalikan cadangan yang disalin DAN ingin mengenkripsi tabel yang dipulihkan dengan kunci yang sama yang Anda gunakan untuk mengenkripsi tabel asli Anda.
> Saat memulihkan cadangan Lintas wilayah, untuk mengenkripsi tabel yang dipulihkan menggunakan kunci yang sama yang Anda gunakan untuk mengenkripsi tabel asli Anda, kunci Anda harus berupa kunci Multi-wilayah. AWS-owned dan AWS-managed keys bukan kunci Multi-region. Untuk mempelajari selengkapnya, lihat Kunci Multi-Wilayah di Panduan AWS Key Management Service Pengembang.
> Saat memulihkan cadangan lintas akun, untuk mengenkripsi tabel yang dipulihkan menggunakan kunci yang sama yang Anda gunakan untuk mengenkripsi tabel asli Anda, Anda harus membagikan kunci di akun sumber Anda dengan akun tujuan Anda. AWS kunci -owned dan AWS-managed tidak dapat dibagikan antar akun. Untuk mempelajari lebih lanjut, lihat Mengizinkan pengguna di akun lain menggunakan kunci KMS di Panduan AWS Key Management Service Pengembang.

7. Pilih Pulihkan cadangan.

   Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan DynamoDB

Gunakan `StartRestoreJob`. Anda dapat menentukan metadata berikut selama DynamoDB restore. Metadata tidak peka huruf besar/kecil.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

Berikut ini adalah contoh `restoreMetadata` argumen untuk `StartRestoreJob` operasi di 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
```

Contoh sebelumnya mengenkripsi tabel dipulihkan menggunakan kunci -owned. AWS Bagian dari metadata pemulihan yang menentukan enkripsi menggunakan kunci yang AWS dimiliki adalah:. `\"encryptionType\":\"Default\","kmsMasterKeyArn\":\"Not Applicable\"`

Untuk mengenkripsi tabel yang dipulihkan menggunakan kunci AWS-managed, tentukan metadata pemulihan berikut:. `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"Not Applicable\"`

Untuk mengenkripsi tabel yang dipulihkan menggunakan kunci yang dikelola pelanggan, tentukan metadata pemulihan berikut:. `"encryptionType \":\"KMS\",\"kmsMasterKeyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`

Memulihkan database RDS

Memulihkan database Amazon RDS memerlukan penentuan beberapa opsi pemulihan. Untuk informasi selengkapnya tentang opsi ini, lihat Mencadangkan dan Memulihkan Instans Amazon RDS DB di Panduan Pengguna Amazon RDS.

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Amazon RDS

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi dan ID sumber daya Amazon RDS yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.

4. Di panel spesifikasi Instans, terima default atau tentukan opsi untuk engine DB, Model Lisensi, kelas instans DB, Multi AZ, dan pengaturan tipe Penyimpanan. Misalnya, jika Anda menginginkan instance database siaga, tentukan Multi AZ.
5. Di panel Pengaturan, tentukan nama yang unik untuk semua instans dan kluster DB yang dimiliki oleh Anda Akun AWS di Wilayah saat ini. Pengidentifikasi instans DB tidak peka huruf kecil, tetapi disimpan sebagai semua huruf kecil, seperti pada "". `mydbinstance` Bidang ini harus diisi.
6. Di panel Jaringan & Keamanan, terima default atau tentukan opsi untuk Virtual Private Cloud (VPC), grup Subnet, Aksesibilitas Publik (biasanya Ya), dan pengaturan zona ketersediaan.
7. Di panel opsi Database, terima default atau tentukan opsi untuk port Database, grup parameter DB, Grup Opsi, Salin tag ke snapshot, dan pengaturan Diaktifkan Autentikasi DB IAM.
8. Di panel Enkripsi, gunakan pengaturan default. Jika instance database sumber untuk snapshot dienkripsi, instance database yang dipulihkan juga akan dienkripsi. Enkripsi ini tidak dapat dihapus.
9. Di panel ekspor Log, pilih jenis log yang akan dipublikasikan ke Amazon CloudWatch Logs. Peran IAM sudah ditentukan.
10. Di panel Pemeliharaan, terima default atau tentukan opsi untuk Upgrade versi minor otomatis.
11. Di panel Pulihkan peran, pilih peran IAM yang AWS Backup akan diasumsikan untuk pemulihan ini.
12. Setelah semua pengaturan telah ditentukan, pilih Pulihkan cadangan.

    Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Amazon RDS

Gunakan `StartRestoreJob`. Untuk informasi tentang metadata dan nilai yang diterima, lihat `RestoreDBInstanceFromDBSnapshot`di Referensi API Amazon RDS. Selain itu, AWS Backup menerima atribut informasi saja berikut. Namun, termasuk mereka tidak akan mempengaruhi pemulihan:

```
EngineVersion
KmsKeyId
Encrypted
```

```
vpcId
```

Memulihkan cluster Amazon Aurora

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Aurora

AWS Backup mengembalikan klaster Aurora Anda; itu tidak membuat atau melampirkan instans Amazon RDS ke cluster Anda. Pada langkah-langkah berikut, Anda akan membuat dan melampirkan instans Amazon RDS ke cluster Aurora yang dipulihkan menggunakan CLI.

Memulihkan klaster Aurora mengharuskan Anda menentukan beberapa opsi pemulihan. Untuk informasi tentang opsi ini, lihat Ikhtisar Mencadangkan dan Memulihkan Cluster DB Aurora di Panduan Pengguna Amazon Aurora. Spesifikasi untuk opsi pemulihan dapat ditemukan di panduan API untuk `RestoreDBClusterFromSnapshot`.

Untuk memulihkan cluster Amazon Aurora

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi dan ID sumber daya Aurora yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.
4. Di panel Spesifikasi instans, terima default atau tentukan opsi untuk mesin DB, versi mesin DB, dan pengaturan tipe Kapasitas.

   > **Note**
   >
   > Jika tipe kapasitas tanpa server dipilih, panel pengaturan Kapasitas akan muncul. Tentukan opsi untuk unit kapasitas Aurora Minimum dan pengaturan unit kapasitas Aurora Maksimum, atau pilih opsi berbeda dari bagian Konfigurasi penskalaan tambahan.

5. Di panel Pengaturan, tentukan nama yang unik untuk semua instance cluster DB yang dimiliki oleh Anda Akun AWS di Wilayah saat ini.
6. Di panel Network & Security, terima default atau tentukan opsi untuk pengaturan Virtual Private Cloud (VPC), grup Subnet, dan Availability zone.

7. Di panel opsi Database, terima default atau tentukan opsi untuk port Database, grup parameter cluster DB, dan pengaturan IAM DB Authentication Enabled.
8. Di panel Backup, terima default atau tentukan opsi untuk pengaturan Salin tag ke snapshot.
9. Di panel Backtrack, terima default atau tentukan opsi untuk pengaturan Aktifkan Backtrack atau Nonaktifkan Backtrack.
10. Di panel Enkripsi, terima default atau tentukan opsi untuk Aktifkan enkripsi atau Nonaktifkan pengaturan enkripsi.
11. Di panel ekspor Log, pilih jenis log yang akan dipublikasikan ke Amazon CloudWatch Logs. Peran IAM sudah ditentukan.
12. Di panel Pulihkan peran, pilih peran IAM yang AWS Backup akan diasumsikan untuk pemulihan ini.
13. Setelah menentukan semua pengaturan Anda, pilih Pulihkan cadangan.

    Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.
14. Setelah pemulihan selesai, lampirkan klaster Aurora yang dipulihkan ke instans Amazon RDS.

    Menggunakan AWS CLI:

    - Untuk Linux, macOS, atau 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
      ```

    - Untuk 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
      ```

Lihat pencadangan dan point-in-time pemulihan berkelanjutan (PITR) untuk informasi tentang pencadangan berkelanjutan dan pemulihan ke titik waktu yang dipilih.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Aurora

Gunakan `StartRestoreJob`. Anda dapat menentukan metadata berikut selama pemulihan Aurora:

```
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;
```

Contoh:

```
"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\":\"[]\"}"
```

Memulihkan instans Amazon EC2

Saat memulihkan instans EC2, AWS Backup buat Amazon Machine Image (AMI), instance, volume root Amazon EBS, volume data Amazon EBS (jika sumber daya yang dilindungi memiliki volume data), dan snapshot Amazon EBS. Anda dapat menyesuaikan beberapa pengaturan instans menggunakan AWS Backup konsol, atau sejumlah besar pengaturan menggunakan AWS CLI atau AWS SDK.

Pertimbangan berikut berlaku untuk memulihkan instans EC2:

- AWS Backup mengonfigurasi instance yang dipulihkan untuk menggunakan key pair yang sama dengan sumber daya yang dilindungi yang digunakan pada awalnya. Anda tidak dapat menentukan key pair yang berbeda untuk instance yang dipulihkan selama proses pemulihan.
- AWS Backup tidak mencadangkan dan memulihkan data pengguna yang digunakan saat meluncurkan instans Amazon EC2.
- Saat mengonfigurasi instans yang dipulihkan, Anda dapat memilih antara menggunakan profil instance yang sama dengan yang digunakan sumber daya yang dilindungi pada awalnya atau diluncurkan tanpa profil instance. Ini untuk mencegah kemungkinan eskalasi hak istimewa. Anda dapat memperbarui profil instans untuk instans yang dipulihkan menggunakan konsol Amazon EC2.

  Jika Anda menggunakan profil instans asli, Anda harus memberikan AWS Backup izin berikut, di mana ARN sumber daya adalah ARN dari peran IAM yang terkait dengan profil instance.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

- Selama pemulihan, semua kuota Amazon EC2 dan batasan konfigurasi berlaku.
- Jika vault yang berisi titik pemulihan Amazon EC2 Anda memiliki kunci vault, Pertimbangan keamanan tambahan lihat untuk informasi selengkapnya.

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Amazon EC2

Anda dapat memulihkan seluruh instans Amazon EC2 dari satu titik pemulihan, termasuk volume root, volume data, dan beberapa pengaturan konfigurasi instans, seperti jenis instans dan key pair.

Untuk memulihkan sumber daya Amazon EC2 menggunakan konsol AWS Backup

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi, lalu pilih ID sumber daya Amazon EC2 untuk membuka halaman detail sumber daya.
3. Di panel Titik pemulihan, pilih tombol radio di sebelah ID titik pemulihan untuk memulihkan. Di sudut kanan atas panel, pilih Pulihkan.

4. Di panel pengaturan Jaringan, kami menggunakan pengaturan dari instance yang dilindungi untuk memilih nilai default untuk jenis instance, VPC, subnet, grup keamanan, dan peran IAM instance. Anda dapat menggunakan nilai default ini atau mengubahnya sesuai kebutuhan.
5. Di panel Pulihkan peran, gunakan peran Default atau gunakan Pilih peran IAM untuk menentukan peran IAM yang memberikan AWS Backup izin untuk memulihkan cadangan.
6. Di panel Tag sumber daya yang dilindungi, kami memilih Salin tag dari sumber daya yang dilindungi ke sumber daya yang dipulihkan secara default. Jika Anda tidak ingin menyalin tag ini, kosongkan kotak centang.
7. Di panel Pengaturan lanjutan, terima nilai default untuk pengaturan instans atau ubah sesuai kebutuhan. Untuk informasi tentang pengaturan ini, pilih Info untuk pengaturan untuk membuka panel bantuannya.
8. Saat Anda selesai mengonfigurasi instance, pilih Pulihkan cadangan.

Kembalikan Amazon EC2 dengan AWS CLI

Di antarmuka baris perintah, `start-restore-job`memungkinkan Anda memulihkan hingga 32 parameter (termasuk beberapa parameter yang tidak dapat disesuaikan melalui AWS Backup konsol).

Daftar berikut adalah metadata yang diterima yang dapat Anda lewati untuk memulihkan titik pemulihan 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 menerima atribut informasi saja berikut. Namun, termasuk mereka tidak akan mempengaruhi pemulihan:

```
vpcId
```

Anda juga dapat memulihkan instans Amazon EC2 tanpa menyertakan parameter yang tersimpan. Opsi ini tersedia di tab Sumber daya yang dilindungi di AWS Backup konsol.

Memulihkan volume Storage Gateway

Jika memulihkan snapshot AWS Storage Gateway volume, Anda dapat memilih untuk mengembalikan snapshot sebagai volume Storage Gateway atau sebagai volume Amazon EBS. Ini karena AWS Backup terintegrasi dengan kedua layanan, dan snapshot Storage Gateway apa pun dapat dikembalikan ke volume Storage Gateway atau volume Amazon EBS.

Kembalikan Storage Gateway melalui AWS Backup konsol

Untuk memulihkan volume Storage Gateway

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi lalu pilih ID sumber daya Storage Gateway yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.
4. Tentukan parameter pemulihan untuk sumber daya Anda. Parameter pemulihan yang Anda masukkan khusus untuk jenis sumber daya yang Anda pilih.

Untuk jenis Sumber Daya, pilih AWS sumber daya yang akan dibuat saat memulihkan cadangan ini.

5. Jika Anda memilih volume Storage Gateway, pilih Gateway dalam status yang dapat dijangkau. Juga pilih nama target iSCSI Anda.

   1. Untuk gateway “Volume tersimpan”, pilih Id Disk.
   2. Untuk gateway “Volume cache”, pilih kapasitas yang setidaknya sebesar sumber daya terlindungi Anda.

   Jika Anda memilih volume EBS, berikan nilai untuk tipe Volume, Ukuran (GiB), dan pilih zona Ketersediaan.

6. Untuk peran Restore, pilih peran IAM yang AWS Backup akan diasumsikan untuk pemulihan ini.

   > **Note**
   >
   > Jika peran AWS Backup default tidak ada di akun Anda, peran Default dibuat untuk Anda dengan izin yang benar. Anda dapat menghapus peran default ini atau membuatnya tidak dapat digunakan.

7. Pilih Pulihkan cadangan.

   Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.

Kembalikan Storage Gateway dengan AWS CLI

Di antarmuka baris perintah, `start-restore-job`memungkinkan Anda mengembalikan volume Storage Gateway.

Daftar berikut adalah metadata yang diterima.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and Wilayah AWS.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
```

```
diskId
```

Memulihkan tabel Amazon Timestream

Saat Anda memulihkan tabel Amazon Timestream, ada beberapa opsi untuk dikonfigurasi, termasuk nama tabel baru, database tujuan, preferensi alokasi penyimpanan Anda (memori dan penyimpanan magnetik), dan peran mana yang akan Anda gunakan untuk menyelesaikan pekerjaan pemulihan. Anda juga dapat memilih bucket Amazon S3 untuk menyimpan log kesalahan. Penulisan penyimpanan magnetik bersifat asinkron, jadi Anda mungkin ingin mencatat kesalahan.

Penyimpanan data Timestream memiliki dua tingkatan: penyimpanan memori dan penyimpanan magnetik. Penyimpanan memori diperlukan, tetapi Anda memiliki opsi untuk mentransfer tabel yang dipulihkan ke penyimpanan magnetik setelah waktu memori yang ditentukan selesai. Penyimpanan memori dioptimalkan untuk penulisan data throughput tinggi dan point-in-time kueri cepat. Penyimpanan magnetik dioptimalkan untuk penulisan data kedatangan terlambat throughput yang lebih rendah, penyimpanan data jangka panjang, dan kueri analitik cepat.

Saat mengembalikan tabel Timestream, Anda menentukan berapa lama Anda ingin tabel tetap berada di setiap tingkat penyimpanan. Menggunakan konsol atau API, Anda dapat mengatur waktu penyimpanan untuk keduanya. Perhatikan bahwa penyimpanannya linier dan berurutan. Timestream akan menyimpan tabel yang dipulihkan di penyimpanan memori terlebih dahulu, kemudian secara otomatis mentransisikannya ke penyimpanan magnetik ketika waktu penyimpanan memori telah tercapai.

> **Note**
>
> Periode retensi penyimpanan magnetik harus sama atau lebih besar dari periode retensi asli (ditampilkan di kanan atas konsol), atau data akan hilang.

Contoh: Anda mengatur alokasi penyimpanan memori untuk menyimpan data selama satu minggu dan mengatur alokasi penyimpanan magnetik untuk menyimpan data yang sama selama satu tahun. Ketika data di penyimpanan memori menjadi berumur seminggu, secara otomatis dipindahkan ke penyimpanan magnetik. Itu kemudian disimpan di toko magnet selama setahun. Pada akhir waktu itu, itu dihapus dari Timestream dan dari AWS Backup.

Untuk memulihkan tabel Amazon Timestream menggunakan konsol AWS Backup

Anda dapat memulihkan tabel Timestream di AWS Backup konsol yang dibuat oleh AWS Backup.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi dan ID sumber daya Amazon Timestream yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.
4. Tentukan pengaturan konfigurasi tabel baru Anda, termasuk:
   a. Nama tabel baru, terdiri dari 2 hingga 256 karakter (huruf, angka, tanda hubung, titik, dan garis bawah).
   b. Database tujuan, dipilih dari menu drop-down.
5. Alokasi penyimpanan: Atur jumlah waktu tabel yang dipulihkan pertama-tama akan berada di penyimpanan memori, dan atur jumlah waktu tabel yang dipulihkan kemudian akan berada di penyimpanan magnetik. Penyimpanan memori dapat diatur ke jam, hari, minggu, atau bulan. Penyimpanan magnetik dapat diatur ke hari, minggu, bulan, atau tahun.
6. (Opsional) Aktifkan penulisan penyimpanan magnetik: Anda memiliki opsi untuk mengizinkan penulisan penyimpanan magnetik. Dengan opsi ini dicentang, data yang tiba terlambat, yang merupakan data dengan stempel waktu di luar periode penyimpanan penyimpanan memori, akan ditulis langsung ke penyimpanan magnetik.
7. (Opsional) Lokasi log kesalahan Amazon S3: Anda dapat menentukan lokasi S3 tempat log kesalahan Anda akan disimpan. Jelajahi file S3 Anda atau salin dan tempel jalur file S3.

   > **Note**
   >
   > Jika Anda memilih untuk menentukan lokasi log kesalahan S3, peran yang Anda gunakan untuk pemulihan ini harus memiliki izin untuk menulis ke bucket S3 atau harus berisi kebijakan dengan izin tersebut.

8. Pilih peran IAM yang akan diteruskan untuk melakukan pemulihan. Anda dapat menggunakan peran IAM default atau menentukan yang berbeda.
9. Klik Pulihkan cadangan.

Pekerjaan pemulihan Anda akan terlihat di bawah sumber daya yang dilindungi. Anda dapat melihat status pekerjaan pemulihan Anda saat ini dengan mengklik tombol refresh atau CTRL-R.

Untuk memulihkan tabel Amazon Timestream menggunakan API, CLI, atau SDK

Gunakan `StartRestoreJob`untuk memulihkan tabel Timestream melalui API. .

Untuk memulihkan Timestream menggunakan AWS CLI, gunakan operasi `start-restore-job.` dan tentukan metadata berikut:

```
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
```

Berikut adalah contoh template:

```
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
```

Anda juga dapat menggunakan `DescribeRestoreJob`untuk membantu memulihkan informasi.

Dalam AWS CLI, gunakan operasi `describe-restore-job` dan gunakan metadata berikut:

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
```

Berikut adalah contoh template:

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Memulihkan klaster Amazon Redshift

Anda dapat memulihkan snapshot otomatis dan manual di AWS Backup konsol atau melalui CLI.

Saat memulihkan kluster Amazon Redshift, pengaturan cluster asli akan dimasukkan ke konsol secara default. Anda dapat menentukan pengaturan yang berbeda untuk konfigurasi di bawah ini. Saat memulihkan tabel, Anda harus menentukan basis data sumber dan target. Untuk informasi selengkapnya tentang konfigurasi ini, lihat Memulihkan klaster dari snapshot di Panduan Manajemen Pergeseran Merah Amazon.

- Tabel tunggal atau cluster: Anda dapat memilih untuk mengembalikan seluruh cluster atau satu tabel. Jika Anda memilih untuk mengembalikan satu tabel, database sumber, skema sumber, dan nama tabel sumber diperlukan, serta klaster target, skema, dan nama tabel baru.
- Tipe node: Setiap cluster Amazon Redshift terdiri dari node pemimpin dan setidaknya satu node komputasi. Saat Anda memulihkan cluster, Anda perlu menentukan jenis node yang memenuhi persyaratan Anda untuk CPU, RAM, kapasitas penyimpanan, dan jenis drive.
- Jumlah node: Saat memulihkan cluster, Anda perlu menentukan jumlah node yang dibutuhkan.
- Ringkasan konfigurasi
- Izin Cluster

Untuk memulihkan klaster atau tabel Amazon Redshift menggunakan konsol AWS Backup

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Pengaturan dan ID sumber daya Amazon Redshift yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Poin Pemulihan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.
4. Pulihkan Opsi

a. Kembalikan cluster dari snapshot, atau

b. Kembalikan tabel tunggal dalam snapshot ke cluster baru. Jika Anda memilih opsi ini, maka Anda harus mengonfigurasi yang berikut:

   i. Aktifkan atau nonaktifkan nama peka huruf besar/kecil.

   ii. Masukkan nilai tabel sumber, termasuk database, skema, dan tabel. Informasi tabel sumber dapat ditemukan di konsol Amazon Redshift.

   iii. Masukkan nilai tabel target, termasuk database, skema, dan nama tabel baru.

5. Tentukan pengaturan konfigurasi cluster baru Anda.

   a. Untuk pemulihan cluster: pilih Cluster identifier, Node type, dan jumlah node.

   b. Tentukan zona ketersediaan dan jendela pemeliharaan.

   c. Anda dapat mengaitkan peran tambahan dengan mengklik peran IAM Associate.

6. Opsional: Konfigurasi tambahan:

   a. Penggunaan default diaktifkan secara default.

   b. Gunakan menu tarik-turun untuk memilih pengaturan untuk Jaringan dan keamanan, grup keamanan VPC, grup subnet Cluster, dan zona Ketersediaan.

   c. Aktifkan atau nonaktifkan perutean VPC yang Ditingkatkan.

   d. Tentukan apakah Anda ingin membuat titik akhir cluster Anda dapat diakses publik. Jika ya, instance dan perangkat di luar VPC dapat terhubung ke database Anda melalui titik akhir cluster. Jika ini diaktifkan, masukkan alamat IP elastis.

7. Opsional: Konfigurasi basis data. Anda dapat memilih untuk memasukkan

   a. Port database (dengan mengetik ke dalam bidang teks)

   b. Grup parameter

8. Pemeliharaan: Anda dapat memilih

   a. Periode pemeliharaan

   b. Jalur pemeliharaan, dari antara saat ini, trailing, atau pratinjau. Ini mengontrol versi cluster mana yang diterapkan selama jendela pemeliharaan.

9. Snapshot otomatis diatur ke default.

   a. Periode retensi snapshot otomatis. Periode retensi harus 0 hingga 35 hari. Pilih 0 untuk tidak membuat snapshot otomatis.

b. Periode retensi snapshot manual adalah 1 hingga 3653 hari.

c. Ada kotak centang opsional untuk relokasi cluster. Jika ini dicentang, ini memungkinkan kemampuan untuk memindahkan cluster Anda di Availability Zone lain. Setelah Anda mengaktifkan relokasi, Anda dapat menggunakan titik akhir VPC.

10. Pemantauan: Setelah cluster dipulihkan, Anda dapat mengatur pemantauan melalui CloudWatch atau Amazon Redshift.
11. Pilih peran IAM yang akan diteruskan untuk melakukan pemulihan. Anda dapat menggunakan peran default, atau Anda dapat menentukan yang lain.

Pekerjaan pemulihan Anda akan terlihat di bawah Pekerjaan. Anda dapat melihat status pekerjaan pemulihan Anda saat ini dengan mengklik tombol refresh atau CTRL-R.

Memulihkan klaster Amazon Redshift menggunakan API, CLI, atau SDK

Gunakan `StartRestoreJob`untuk memulihkan cluster Amazon Redshift.

Untuk memulihkan Amazon Redshift menggunakan AWS CLI, gunakan perintah `start-restore-job` dan tentukan metadata berikut:

```
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
```

Untuk informasi selengkapnya, lihat *RestoreFromClusterSnapshot*di Referensi API Amazon Redshift dan *restore-from-cluster-snapshot*di panduan.AWS CLI

Berikut adalah contoh template:

```
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 Wilayah AWS
-\-endpoint-url URL
```

Inilah contohnya:

```
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 \
```

Anda juga dapat menggunakan DescribeRestoreJobuntuk membantu memulihkan informasi.

Dalam AWS CLI, gunakan operasi `describe-restore-job` dan gunakan metadata berikut:

```
Region
```

Berikut adalah contoh template:

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region Wilayah AWS
```

Inilah contohnya:

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
-\-region us-west-2 \
```

Memulihkan database SAP HANA pada instans Amazon EC2

Database SAP HANA pada instans EC2 dapat dipulihkan menggunakan AWS Backup konsol, menggunakan API, atau menggunakan. AWS CLI

Topik

- Memulihkan SAP HANA di database instans Amazon EC2 menggunakan konsol AWS Backup
- StartRestoreJob API untuk SAP HANA di EC2
- CLI untuk SAP HANA di EC2
- Pemecahan Masalah

Memulihkan SAP HANA di database instans Amazon EC2 menggunakan konsol AWS Backup

Perhatikan bahwa pekerjaan pencadangan dan pemulihan pekerjaan yang melibatkan database yang sama tidak dapat terjadi secara bersamaan. Ketika pekerjaan pemulihan database SAP HANA terjadi, upaya untuk membuat cadangan database yang sama kemungkinan akan menghasilkan kesalahan: “Database tidak dapat dicadangkan saat dihentikan.”

1. Akses AWS Backup konsol menggunakan kredensional dari prasyarat.
2. Di bawah menu tarik-turun lokasi pemulihan Target, pilih database untuk ditimpa dengan titik pemulihan yang Anda gunakan untuk memulihkan (perhatikan bahwa instance yang menghosting database target pemulihan juga harus memiliki izin dari prasyarat).

> **Important**
>
> Pemulihan basis data SAP HANA bersifat destruktif. Memulihkan database akan menimpa database di lokasi pemulihan target yang ditentukan.

3. Selesaikan langkah ini hanya jika Anda melakukan pemulihan salinan sistem; jika tidak, lewati ke langkah 4.

   Pemulihan salinan sistem adalah pekerjaan pemulihan yang mengembalikan ke database target yang berbeda dari database sumber yang menghasilkan titik pemulihan. Untuk pemulihan salinan sistem, perhatikan `aws ssm-sap put-resource-permission` perintah yang disediakan untuk Anda di konsol. Perintah ini harus disalin, disisipkan, dan dieksekusi pada mesin yang menyelesaikan prasyarat. Saat menjalankan perintah, gunakan kredensil dari peran dalam prasyarat tempat Anda mengatur izin yang diperlukan untuk mendaftarkan aplikasi.

   ```
   // 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. Setelah Anda memilih lokasi pemulihan, Anda dapat melihat ID Sumber Daya database target, nama Aplikasi, tipe Database, dan instans EC2.
5. Secara opsional, Anda dapat membuka Pengaturan pemulihan lanjutan untuk mengubah opsi pemulihan katalog Anda. Pilihan default adalah mengembalikan katalog terbaru dari AWS Backup.
6. Klik Pulihkan cadangan.
7. Lokasi target akan ditimpa selama pemulihan (“pemulihan destruktif”), jadi Anda harus memberikan konfirmasi bahwa Anda mengizinkan ini di kotak dialog pop-up berikutnya.

   a. Untuk melanjutkan, Anda harus memahami bahwa database yang ada akan ditimpa oleh database yang Anda pulihkan.

   b. Setelah ini dipahami, Anda harus mengakui bahwa data yang ada akan ditimpa. Untuk mengetahui hal ini dan melanjutkan, ketik timpa ke dalam bidang input teks.

8. Klik Pulihkan cadangan.

Jika prosedur berhasil, spanduk biru akan muncul di bagian atas konsol. Ini berarti bahwa pekerjaan pemulihan sedang berlangsung. Anda akan secara otomatis diarahkan ke halaman Pekerjaan di mana pekerjaan pemulihan Anda akan muncul dalam daftar pekerjaan pemulihan. Pekerjaan terbaru ini akan memiliki status`Pending`. Anda dapat mencari dan kemudian mengklik ID pekerjaan pemulihan juga melihat detail dari setiap pekerjaan pemulihan. Anda dapat menyegarkan daftar pekerjaan pemulihan dengan mengklik tombol segarkan untuk melihat perubahan pada status pekerjaan pemulihan.

StartRestoreJob API untuk SAP HANA di EC2

Tindakan ini memulihkan sumber daya tersimpan yang diidentifikasi oleh Amazon Resource Name (ARN).

Permintaan Sintaks

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Parameter Permintaan URI: Permintaan tidak menggunakan parameter URI apa pun.

Request Body: Permintaan menerima data berikut dalam format JSON:

IdempotencyTokenString yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `StartRestoreJob` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

Metadata

Satu set pasangan nilai kunci metadata. Berisi informasi, seperti nama sumber daya, yang diperlukan untuk memulihkan titik pemulihan. Anda bisa mendapatkan metadata konfigurasi tentang sumber

daya pada saat itu dicadangkan dengan menelepon. `GetRecoveryPointRestoreMetadata` Namun, nilai selain yang disediakan oleh `GetRecoveryPointRestoreMetadata` mungkin diperlukan untuk memulihkan sumber daya. Misalnya, Anda mungkin perlu memberikan nama sumber daya baru jika yang asli sudah ada.

Anda perlu menyertakan metadata tertentu untuk memulihkan SAP HANA di instans Amazon EC2. Lihat StartRestoreJob metadata untuk item khusus SAP Hana.

Untuk mengambil metadata yang relevan, Anda dapat menggunakan panggilan. `GetRecoveryPointRestoreMetadata`

Contoh titik pemulihan basis data SAP HANA standar:

```
"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"
    }
```

Contoh titik pemulihan basis data SAP HANA yang berkelanjutan:

```
"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 untuk SAP HANA di EC2

Perintah `start-restore-job` memulihkan sumber daya tersimpan yang diidentifikasi oleh Amazon Resource Name (ARN). CLI akan mengikuti pedoman API di atas.

Sinopsis:

```
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]
```

Pilihan

`--recovery-point-arn`(string) adalah string dalam bentuk Amazon Resource Number (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

`--metadata`(peta): Satu set pasangan nilai kunci metadata. Berisi informasi, seperti nama sumber daya, yang diperlukan untuk memulihkan titik pemulihan. Anda bisa mendapatkan metadata konfigurasi tentang sumber daya pada saat itu dicadangkan dengan menelepon. `GetRecoveryPointRestoreMetadata` Namun, nilai selain yang disediakan oleh `GetRecoveryPointRestoreMetadata` mungkin diperlukan untuk memulihkan sumber daya. Anda perlu menentukan metadata tertentu untuk memulihkan SAP HANA di instans Amazon EC2:

- `aws:backup:request-id`: Ini adalah string UUID yang digunakan untuk idempotensi. Itu tidak mengubah pengalaman pemulihan Anda dengan cara apa pun.
- `aws:backup:TargetDatabaseArn`: Tentukan database yang ingin Anda pulihkan. Ini adalah SAP HANA di database Amazon EC2 ARN.
- `CatalogRestoreOption`: Tentukan dari mana memulihkan katalog Anda. Salah satu`NO_CATALOG`,`LATEST_CATALOG_FROM_AWS_BACKUP`, `CATALOG_FROM_LOCAL_PATH`
- `LocalCatalogPath`: Jika nilai CatalogRestoreOption metadata adalah`CATALOG_FROM_LOCAL_PATH`, maka tentukan jalur ke katalog lokal pada instans EC2 Anda. Ini harus menjadi jalur file yang valid di instans EC2 Anda.
- `RecoveryType`: Saat ini`FULL_DATA_BACKUP_RECOVERY`,`POINT_IN_TIME_RECOVERY`,, dan jenis `MOST_RECENT_TIME_RECOVERY` pemulihan didukung.

kunci = (string); nilai = (string). Sintaks singkatan:

```
KeyName1=string,KeyName2=string
```

Sintaks JSON:

```
{"string": "string"
  ...}
```

`--idempotency-token`adalah string yang dipilih pengguna yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `StartRestoreJob` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

`--resource-type`adalah string yang memulai pekerjaan untuk memulihkan titik pemulihan untuk salah satu sumber daya berikut: `SAP HANA on Amazon EC2` untuk SAP HANA di Amazon EC2. Secara opsional, sumber daya SAP HANA dapat ditandai menggunakan perintah `aws ssm-sap tag-resource`

Output: `RestoreJobId` adalah string yang secara unik mengidentifikasi pekerjaan yang mengembalikan titik pemulihan.

Pemecahan Masalah

Jika salah satu kesalahan berikut terjadi saat mencoba operasi pencadangan, lihat resolusi terkait.

- Kesalahan: Kesalahan log pencadangan berkelanjutan

  Untuk mempertahankan titik pemulihan untuk pencadangan berkelanjutan, log dibuat oleh SAP HANA untuk semua perubahan. Ketika log tidak tersedia, status masing-masing titik pemulihan berkelanjutan ini adalah`STOPPED`. Titik pemulihan terakhir yang layak yang dapat digunakan untuk memulihkan adalah salah satu yang memiliki status. `AVAILABLE` Jika data log hilang untuk waktu antara titik pemulihan dengan `STOPPED` status dan poin dengan`AVAILABLE`, waktu-waktu ini tidak dapat dijamin memiliki pemulihan yang berhasil. Jika Anda memasukkan tanggal dan waktu dalam rentang ini, AWS Backup akan mencoba cadangan, tetapi akan menggunakan waktu restorable terdekat yang tersedia. Kesalahan ini akan ditampilkan oleh pesan `“Encountered an issue with log backups. Please check SAP HANA for details."`

  Resolusi: Di konsol, waktu restorasi terbaru, berdasarkan log, ditampilkan. Anda dapat memasukkan waktu yang lebih baru dari waktu yang ditampilkan. Namun, jika data untuk saat ini tidak tersedia dari log, AWS Backup akan menggunakan waktu restorable terbaru.

- Kesalahan: `Internal error`

  Resolusi: Buat kasus dukungan dari konsol Anda atau kontak AWS Support dengan detail pemulihan Anda seperti ID pekerjaan pemulihan.

- Kesalahan: `The provided role arn:aws:iam::`*`ACCOUNT_ID`*`:role/ServiceLinkedRole cannot be assumed by AWS Backup`

  Resolusi: Pastikan peran yang diasumsikan saat memanggil pemulihan memiliki izin yang diperlukan untuk membuat peran terkait layanan.

- Kesalahan: `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`*`:...`

Resolusi: Pastikan peran yang diasumsikan saat memanggil izin pemulihan yang diuraikan dalam prasyarat dimasukkan dengan benar.

- Kesalahan: `b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n`

  Resolusi: Pastikan agen Backint dipasang dengan benar. Periksa semua prasyarat, terutama Install AWS BackInt Agent dan AWS Systems Manager SAP di server aplikasi SAP Anda dan kemudian coba lagi menginstal Agen lagi. BackInt

- Kesalahan: `IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED`

  Resolusi: Pekerjaan pemulihan dibatalkan oleh alur kerja layanan. Coba lagi memulihkan pekerjaan.

- Kesalahan: `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"`

  Resolusi: Ketidakstabilan jaringan sementara terjadi pada instance. Coba kembali pemulihan. Jika masalah ini terjadi secara konsisten, coba tambahkan `ForceRetry: "true"` ke file konfigurasi agen di `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml`.

Untuk masalah terkait agen AWS Backint lainnya, lihat Troubleshoot Backint AWS Agent For SAP HANA.

Memulihkan cluster DocumentDB

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Amazon DocumentDB

Memulihkan klaster Amazon DocumentDB mengharuskan Anda menentukan beberapa opsi pemulihan. Untuk informasi tentang opsi ini, lihat Memulihkan dari Snapshot Cluster di Panduan Pengembang Amazon DocumentDB.

Untuk memulihkan cluster Amazon DocumentDB

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.

2. Di panel navigasi, pilih Sumber daya yang dilindungi dan ID sumber daya Amazon DocumentDB yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.
4. Di panel Konfigurasi, terima default atau tentukan opsi untuk pengenal Cluster, versi Engine, kelas Instance, dan Jumlah instance.

   - CATATAN: Jika VPC default tidak ada saat memulihkan, Anda harus menentukan subnet di VPC lain.
5. Di panel Jaringan & Keamanan, “Tidak Ada Preferensi” akan ditampilkan.
6. Di ncryption-at-rest panel E, terima default atau tentukan opsi untuk Aktifkan enkripsi atau Nonaktifkan pengaturan enkripsi.
7. Di panel opsi Cluster, ketik Port dan pilih grup parameter Cluster.
8. Di panel Backup, pilih backup berkelanjutan untuk point-in-time pemulihan (PITR), backup snapshot terjadwal, atau keduanya.
9. Di panel ekspor Log, pilih jenis log yang akan dipublikasikan ke Amazon CloudWatch Logs. Peran IAM sudah ditentukan.
10. Di panel Pemeliharaan, tentukan jendela pemeliharaan atau pilih Tidak ada preferensi.
11. Di panel Tag, Anda dapat memilih Tambah tag.
12. Di panel Perlindungan penghapusan, Anda dapat memilih Aktifkan perlindungan penghapusan.
13. Setelah menentukan semua pengaturan Anda, pilih Pulihkan cadangan.

    Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.
14. Setelah pemulihan selesai, lampirkan klaster Amazon DocumentDB yang dipulihkan ke instans Amazon RDS.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Amazon DocumentDB

Pertama, pulihkan cluster Anda. Gunakan `StartRestoreJob`. Anda dapat menentukan metadata berikut selama pemulihan Amazon DocumentDB:

```
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
```

Kemudian, lampirkan cluster Amazon DocumentDB Anda yang dipulihkan ke instans Amazon RDS menggunakan. `create-db-instance`

- Untuk Linux, macOS, atau Unix:

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Untuk Windows:

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Memulihkan cluster Neptunus

Gunakan AWS Backup konsol untuk memulihkan titik pemulihan Amazon Neptunus

Memulihkan database Amazon Neptunus mengharuskan Anda menentukan beberapa opsi pemulihan. Untuk informasi tentang opsi ini, lihat Memulihkan dari Snapshot Cluster DB di Panduan Pengguna Neptunus.

Untuk memulihkan database Neptunus

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi dan ID sumber daya Neptunus yang ingin Anda pulihkan.
3. Pada halaman Rincian sumber daya, daftar titik pemulihan untuk ID sumber daya yang dipilih ditampilkan. Untuk memulihkan sumber daya, di panel Cadangan, pilih tombol radio di sebelah ID titik pemulihan sumber daya. Di sudut kanan atas panel, pilih Pulihkan.
4. Di panel spesifikasi Instans, terima default atau tentukan mesin DB dan Versi.
5. Di panel Pengaturan, tentukan nama yang unik untuk semua instance cluster DB yang dimiliki oleh Anda Akun AWS di Wilayah saat ini. Pengidentifikasi cluster DB tidak peka huruf besar/kecil, tetapi disimpan sebagai semua huruf kecil, seperti pada "". `mydbclusterinstance` Bidang ini harus diisi.
6. Di panel opsi Database, terima default atau tentukan opsi untuk port Database dan grup parameter cluster DB.
7. Di panel Enkripsi, terima default atau tentukan opsi untuk Aktifkan enkripsi atau Nonaktifkan pengaturan enkripsi.
8. Di panel ekspor Log, pilih jenis log yang akan dipublikasikan ke Amazon CloudWatch Logs. Peran IAM sudah ditentukan.
9. Di panel Pulihkan peran, pilih peran IAM yang AWS Backup akan diasumsikan untuk pemulihan ini.
10. Setelah menentukan semua pengaturan Anda, pilih Pulihkan cadangan.

    Panel Pulihkan pekerjaan muncul. Pesan di bagian atas halaman memberikan informasi tentang pekerjaan pemulihan.
11. Setelah pemulihan selesai, lampirkan cluster Neptunus yang dipulihkan ke instans Amazon RDS.

Gunakan AWS Backup API, CLI, atau SDK untuk memulihkan titik pemulihan Neptunus

Pertama, pulihkan cluster Anda. Gunakan `StartRestoreJob`. Anda dapat menentukan metadata berikut selama pemulihan Amazon DocumentDB:

```
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
```

Kemudian, lampirkan cluster Neptunus Anda yang dipulihkan ke instans Amazon RDS menggunakan. `create-db-instance`

- Untuk Linux, macOS, atau 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
```

- Untuk 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
```

Untuk informasi selengkapnya, lihat *RestoreDBClusterFromSnapshot*di referensi API Manajemen Neptunus dan *restore-db-cluster-from-snapshot*di panduan CLI Neptunus.

Kembalikan cadangan CloudFormation tumpukan

Cadangan CloudFormation komposit adalah kombinasi dari CloudFormation template dan semua titik pemulihan bersarang yang terkait. Sejumlah titik pemulihan bersarang dapat dipulihkan, tetapi titik pemulihan komposit (yang merupakan titik pemulihan tingkat atas) tidak dapat dipulihkan.

Saat memulihkan titik pemulihan CloudFormation template, Anda membuat tumpukan baru dengan set perubahan untuk mewakili cadangan.

Kembalikan CloudFormation dengan AWS Backup konsol;

Dari CloudFormation konsol Anda dapat melihat tumpukan baru dan mengubah set. Untuk mempelajari lebih lanjut tentang set perubahan, lihat Memperbarui tumpukan menggunakan set perubahan di Panduan AWS CloudFormation Pengguna.

Tentukan titik pemulihan bersarang mana yang ingin Anda pulihkan dengan CloudFormation tumpukan Anda, lalu pulihkan menggunakan AWS Backup konsol.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Buka Backup vaults, pilih brankas cadangan yang berisi titik pemulihan yang Anda inginkan, lalu klik pada Recovery points.
3. Kembalikan titik pemulihan AWS CloudFormation template.
    a. Klik titik pemulihan komposit yang berisi titik pemulihan bersarang yang ingin Anda pulihkan untuk membuka halaman Detail untuk titik pemulihan komposit.
    b. Di bawah titik pemulihan bersarang, titik pemulihan bersarang akan ditampilkan. Setiap titik pemulihan akan memiliki ID titik pemulihan, status, ID sumber daya, jenis sumber daya, jenis cadangan, dan waktu titik pemulihan dibuat. Klik tombol radio di sebelah titik AWS CloudFormation pemulihan, lalu klik Pulihkan. Pastikan Anda memilih titik pemulihan yang memiliki tipe sumber daya: AWS CloudFormation dan jenis cadangan: cadangan.
4. Setelah pekerjaan pemulihan untuk CloudFormation template selesai, AWS CloudFormation template yang dipulihkan akan terlihat di AWS CloudFormation konsol di bawah Stacks.
5. Di bawah nama Stack Anda harus menemukan template dipulihkan dengan status`REVIEW_IN_PROGRESS`.
6. Klik pada nama tumpukan untuk melihat detail tumpukan.
7. Ada tab di bawah nama tumpukan. Klik pada Ubah set.
8. Jalankan set perubahan.
9. Setelah proses ini, sumber daya di tumpukan asli akan dibuat ulang di tumpukan baru. Sumber daya stateful akan dibuat ulang kosong. Untuk memulihkan sumber daya stateful, kembali ke daftar titik pemulihan di AWS Backup konsol, pilih titik pemulihan yang Anda butuhkan, dan mulai pemulihan.

Kembalikan CloudFormation dengan AWS CLI

Di antarmuka baris perintah, `start-restore-job`memungkinkan Anda mengembalikan CloudFormation tumpukan.

Daftar berikut adalah metadata yang diterima untuk memulihkan sumber daya. CloudFormation

```
// 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
```

Kembalikan pengujian

Topik

- Gambaran Umum
- Kembalikan pengujian dibandingkan dengan proses pemulihan
- Kembalikan manajemen pengujian
- Buat rencana pengujian pemulihan
- Perbarui rencana pengujian pemulihan
- Lihat rencana pengujian pemulihan yang ada
- Lihat pekerjaan pengujian pemulihan
- Hapus rencana pengujian pemulihan
- Pengujian pemulihan audit
- Kembalikan kuota dan parameter pengujian
- Kembalikan pemecahan masalah kegagalan pengujian
- Kembalikan pengujian metadata yang disimpulkan
- Kembalikan validasi pengujian

Gambaran Umum

Restore testing, fitur yang ditawarkan oleh AWS Backup, menyediakan evaluasi otomatis dan berkala dari kelayakan pemulihan, serta kemampuan untuk memantau waktu durasi pekerjaan pemulihan.

Pertama, Anda membuat rencana pengujian pemulihan di mana Anda memberikan nama untuk paket Anda, frekuensi untuk pengujian pemulihan Anda, dan waktu mulai target. Kemudian, Anda menetapkan sumber daya yang ingin Anda sertakan dalam rencana Anda. Anda kemudian memilih untuk memasukkan titik pemulihan spesifik atau acak dalam pengujian Anda. AWS Backup backup secara cerdas menyimpulkan metadata yang akan dibutuhkan agar pekerjaan pemulihan Anda berhasil.

Ketika waktu yang dijadwalkan dalam rencana Anda tiba, AWS Backup mulailah memulihkan pekerjaan berdasarkan rencana Anda dan memantau waktu yang dibutuhkan untuk menyelesaikan pemulihan.

Setelah rencana pengujian pemulihan selesai dijalankan, Anda dapat menggunakan hasilnya untuk menunjukkan kepatuhan terhadap persyaratan organisasi atau tata kelola seperti keberhasilan penyelesaian skenario pengujian pemulihan atau waktu penyelesaian pekerjaan pemulihan.

Secara opsional, Anda dapat menggunakan Kembalikan validasi pengujian untuk mengonfirmasi hasil tes pemulihan.

Setelah validasi opsional selesai atau jendela validasi ditutup, AWS Backup menghapus sumber daya yang terlibat dengan tes pemulihan, dan sumber daya akan dihapus sesuai dengan SLA layanan.

Di akhir proses pengujian, Anda dapat melihat hasil dan waktu penyelesaian tes.

Kembalikan pengujian dibandingkan dengan proses pemulihan

Restore testing berjalan restore jobs dengan cara yang sama seperti on-demand restores dan menggunakan recovery point (backup) yang sama dengan on-demand restore. Anda akan melihat panggilan `StartRestoreJob` masuk CloudTrail (jika ikut serta) untuk setiap pekerjaan yang dimulai dengan memulihkan pengujian

Namun, ada beberapa perbedaan antara pengoperasian tes pemulihan jadwal dan operasi pemulihan sesuai permintaan:

	Kembalikan Pengujian	Memulihkan
Akun	Praktik terbaik yang disarankan adalah menunjuk akun yang akan digunakan untuk tes pemulihan	Anda dapat memulihkan sumber daya dari akun
AWS Backup Audit Manager	Dapat mengaktifkan kontrol untuk mengonfirmasi apakah tes pemulihan memenuhi tujuan pemulihan yang ditentukan	
Irama	Secara berkala sebagai bagian dari rencana yang dijadwalkan.	Sesuai permintaan
Regionalitas	Tersedia di semua Wilayah komersial yang AWS Backup beroperasi kecuali Israel (Tel Aviv) Tidak tersedia AWS GovCloud (AS-Timur), AWS GovCloud (AS-Barat), China (Beijing), dan China (Ningxia).	Tersedia di semua Wilayah komersial di mana AWS Backup beroperasi
Sumber Daya	Jenis sumber daya yang dapat Anda tetapkan ke paket pengujian Anda meliputi: Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, Amazon FSX (Lustre, ONTAP, OpenZFS, Windows), Amazon Neptunus,	Semua sumber daya dapat dipulihkan.

	Kembalikan Pengujian	Memulihkan
	Amazon RDS, dan Amazon S3 3.	
Hasil	Setelah pekerjaan pengujian pemulihan selesai, sumber daya yang dipulihkan akan dihapus setelah Kembalikan validasi pengujian jendela selesai.	Setelah pekerjaan pemulihan selesai, versi sumber daya yang dipulihkan tetap ada.
Tanda	Untuk jenis sumber daya yang mendukung tag pada pemulihan, pengujian menerapkan tag pada pemulihan.	Tag adalah opsional untuk sumber daya yang didukung.

Kembalikan manajemen pengujian

Anda dapat membuat, melihat, memperbarui, atau menghapus rencana pengujian pemulihan di AWS Backup konsol.

Anda dapat menggunakan AWS CLIuntuk melakukan operasi secara terprogram untuk memulihkan rencana pengujian. Setiap CLI khusus untuk AWS layanan di mana ia berasal. Perintah harus ditambahkan dengan. `aws backup`

Penghapusan data

Ketika tes pemulihan selesai, AWS Backup mulai menghapus sumber daya yang terlibat dalam pengujian. Penghapusan ini tidak instan. Setiap sumber daya memiliki konfigurasi dasar yang menentukan bagaimana sumber daya tersebut disimpan dan didaur ulang. Misalnya, jika bucket Amazon S3 merupakan bagian dari pengujian pemulihan, aturan siklus hidup akan ditambahkan ke bucket. Diperlukan waktu hingga beberapa hari untuk menjalankan aturan dan bucket dan objeknya dihapus sepenuhnya, tetapi biaya hanya akan terjadi untuk sumber daya ini hingga hari ketika aturan siklus hidup dimulai (secara default ini adalah 1 hari). Kecepatan penghapusan akan tergantung pada jenis sumber daya.

Sumber daya yang merupakan bagian dari rencana pengujian pemulihan berisi tag yang disebut`awsbackup-restore-test`. Jika pengguna menghapus tag ini, AWS Backup tidak dapat menghapus sumber daya pada akhir periode pengujian dan pengguna harus menghapusnya secara manual sebagai gantinya.

Untuk memeriksa mengapa sumber daya mungkin tidak dihapus seperti yang diharapkan, Anda dapat mencari melalui pekerjaan yang gagal di konsol atau menggunakan antarmuka baris perintah untuk memanggil permintaan API `DescribeRestoreJob` untuk mengambil pesan status penghapusan.

Rencana cadangan (rencana pengujian non-pemulihan) mengabaikan sumber daya yang dibuat oleh pengujian pemulihan (yang memiliki tag `awsbackup-restore-test` atau nama yang dimulai dengan`awsbackup-restore-test`).

Pengendalian biaya

Restore testing memiliki biaya per restore test. Bergantung pada sumber daya apa yang termasuk dalam rencana pengujian pemulihan Anda, pekerjaan pemulihan yang merupakan bagian dari rencana mungkin juga memiliki biaya. Lihat AWS Backup Harga untuk detail selengkapnya.

Saat Anda menyiapkan rencana pengujian pemulihan untuk pertama kalinya, Anda mungkin merasa bermanfaat untuk memasukkan jumlah minimum jenis sumber daya dan sumber daya yang dilindungi untuk membiasakan diri dengan fitur, proses, dan biaya rata-rata yang terlibat. Anda dapat memperbarui paket setelah pembuatannya untuk menambahkan lebih banyak jenis sumber daya dan sumber daya yang dilindungi.

Buat rencana pengujian pemulihan

Rencana pengujian pemulihan memiliki dua bagian: pembuatan rencana dan penetapan sumber daya.

Saat Anda menggunakan konsol, bagian-bagian ini berurutan. Pada bagian pertama, Anda mengatur nama, frekuensi, dan waktu mulai. Selama bagian kedua Anda menetapkan sumber daya untuk rencana pengujian Anda.

Saat menggunakan AWS CLI dan API, gunakan pertama `create-restore-testing-plan`. Setelah Anda menerima respons yang berhasil dan rencana telah dibuat, gunakan `create-restore-testing-selection`, untuk setiap jenis sumber daya yang ingin Anda sertakan dalam paket Anda.

Console

Bagian I: Buat rencana pengujian pemulihan menggunakan konsol

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di navigasi sebelah kiri, cari Restore testing dan pilih.
3. Pilih buat rencana pengujian pemulihan.
4. Umum

    a. Nama: Ketik nama untuk rencana pengujian pemulihan baru Anda. Nama tidak dapat diubah setelah penciptaan. Nama harus terdiri dari hanya karakter alfanumerik dan garis bawah.

    b. Frekuensi pengujian: Pilih frekuensi di mana tes pemulihan akan berjalan.

    c. Waktu Mulai: Atur waktu (dalam jam dan menit) Anda lebih suka tes dimulai. Anda juga dapat mengatur zona waktu lokal di mana Anda ingin rencana pengujian pemulihan beroperasi.

    d. Mulai dalam: Nilai ini (dalam jam) adalah periode waktu di mana tes pemulihan ditunjuk untuk dimulai. AWS Backup melakukan upaya terbaik untuk memulai semua pekerjaan pemulihan yang ditunjuk selama awal dalam waktu dan mengacak waktu mulai dalam periode ini.

5. Pemilihan titik pemulihan: Di sini Anda mengatur brankas sumber, rentang titik pemulihan, dan kriteria pemilihan untuk titik pemulihan (cadangan) mana yang ingin Anda jadikan bagian dari rencana.

    a. Brankas sumber: Pilih apakah akan menyertakan semua brankas yang tersedia atau hanya brankas tertentu untuk membantu memfilter titik pemulihan mana yang ada dalam paket Anda. Jika Anda memilih brankas tertentu, pilih dari menu tarik-turun brankas yang ingin Anda sertakan.

    b. Poin pemulihan yang memenuhi syarat: Tentukan kerangka waktu dari mana titik pemulihan akan dipilih. Anda dapat memilih 1 hingga 365 hari, 1 hingga 52 minggu, 1 hingga 12 bulan, atau 1 tahun.

    c. Kriteria seleksi: Setelah rentang tanggal titik pemulihan Anda ditentukan, Anda dapat memilih apakah akan memasukkan yang terbaru atau satu secara acak dalam paket Anda. Anda mungkin ingin memilih yang acak untuk mengukur kesehatan umum titik pemulihan pada frekuensi yang lebih teratur jika pemulihan ke versi yang lebih lama diperlukan.

d. Poin oint-in-time pemulihan P: Jika paket Anda menyertakan sumber daya yang memiliki titik pencadangan berkelanjutan (point-in-time-restore/PITR), Anda dapat mencentang kotak ini agar rencana pengujian Anda menyertakan pencadangan berkelanjutan sebagai titik pemulihan yang memenuhi syarat (lihat Ketersediaan fitur berdasarkan sumber daya untuk jenis sumber daya yang memiliki fitur ini).

6. (opsional) Tag ditambahkan untuk memulihkan rencana pengujian: Anda dapat memilih untuk menambahkan hingga 50 tag ke rencana pengujian pemulihan Anda. Setiap tag harus ditambahkan secara terpisah. Untuk menambahkan tag baru, pilih Tambahkan tag baru.

Bagian II: Tetapkan sumber daya ke paket menggunakan konsol

Di bagian ini, Anda memilih sumber daya yang telah dicadangkan untuk disertakan dalam rencana pengujian pemulihan Anda. Anda akan memilih nama penetapan sumber daya, memilih peran yang Anda gunakan untuk pengujian pemulihan, dan mengatur periode retensi sebelum pembersihan. Kemudian, Anda akan memilih jenis sumber daya, memilih ruang lingkup, dan secara opsional menyempurnakan pilihan Anda dengan tag.

> **Tip**
>
> Untuk menavigasi kembali ke rencana pengujian pemulihan yang ingin Anda tambahkan sumber daya, Anda dapat pergi ke AWS Backup konsol, pilih Pulihkan pengujian, lalu temukan rencana pengujian pilihan Anda dan pilih.

1. Umum

   a. Nama penetapan sumber daya: Masukkan nama untuk tugas sumber daya ini menggunakan string karakter alfanumerik dan garis bawah, tanpa spasi putih.

   b. Kembalikan peran IAM: Tes harus menggunakan peran Identity and Access Management (IAM) and Access Management (IAM) yang Anda tetapkan. Anda dapat memilih peran AWS Backup default atau yang lain. Jika AWS Backup default belum ada saat Anda menyelesaikan proses ini, AWS Backup akan membuatnya untuk Anda secara otomatis dengan izin yang diperlukan. Peran IAM yang Anda pilih untuk pengujian pemulihan harus berisi izin yang ditemukan. AWSBackupServicePolicyForRestores

   c. Periode retensi sebelum pembersihan: Selama tes pemulihan, data cadangan dipulihkan sementara. Secara default, data ini dihapus setelah tes selesai. Anda memiliki opsi untuk menunda penghapusan data ini jika Anda ingin menjalankan validasi pada pemulihan.

Jika Anda berencana untuk menjalankan validasi, pilih simpan untuk jumlah jam tertentu dan masukkan nilai dari 1 hingga 168 jam, inklusif. Perhatikan bahwa validasi dapat dijalankan secara terprogram tetapi tidak dari konsol. AWS Backup

2. Sumber daya yang dilindungi:

   a. Pilih jenis sumber daya: Pilih jenis sumber daya dan cakupan cadangan jenis tersebut yang akan disertakan dalam rencana pengujian sumber daya. Setiap paket dapat berisi beberapa jenis sumber daya, tetapi setiap jenis sumber daya harus ditetapkan ke rencana secara individual.

   b. Cakupan pemilihan sumber daya: Setelah jenis dipilih, pilih apakah Anda ingin menyertakan semua sumber daya terlindungi yang tersedia dari jenis itu atau jika Anda ingin menyertakan sumber daya terlindungi tertentu saja.

   c. (opsional) Perbaiki pemilihan sumber daya menggunakan tag: Jika cadangan Anda memiliki tag, Anda dapat memfilter berdasarkan tag untuk memilih sumber daya tertentu yang dilindungi. Masukkan kunci tag, kondisi untuk kunci ini dimasukkan atau tidak, dan nilai untuk kunci tersebut. Kemudian, pilih tombol Tambah tag.

      Tag pada sumber daya yang dilindungi dievaluasi dengan memeriksa tag pada titik pemulihan terbaru dalam brankas cadangan yang berisi sumber daya yang dilindungi.

3. Mengembalikan parameter: Sumber daya tertentu memerlukan parameter penentuan dalam persiapan untuk pekerjaan pemulihan. Dalam kebanyakan kasus, AWS Backup akan menyimpulkan nilai berdasarkan cadangan yang disimpan.

   Disarankan dalam banyak kasus untuk mempertahankan parameter ini; Namun, Anda dapat mengubah nilai dengan memilih pilihan yang berbeda dari menu tarik-turun. Contoh di mana mengubah nilai mungkin optimal dapat mencakup kunci enkripsi pengganti, pengaturan Amazon FSx di mana data tidak dapat disimpulkan, dan pembuatan subnet.

   Misalnya, jika database RDS adalah salah satu jenis sumber daya yang Anda tetapkan ke rencana pengujian pemulihan, parameter seperti zona ketersediaan, nama database, kelas instance database, dan grup keamanan VPC akan muncul dengan nilai yang disimpulkan yang dapat Anda ubah jika berlaku.

AWS CLI

Perintah CLI `CreateRestoreTestingPlan` digunakan untuk membuat rencana pengujian pemulihan.

Rencana pengujian harus berisi:

- `RestoreTestingPlan`, yang harus mengandung yang unik `RestoreTestingPlanName`
- `ScheduleExpression`ekspresi cron
- `RecoveryPointSelection`

  Meskipun dinamai sama, ini TIDAK sama dengan`RestoreTestingSelection`.

  `RecoveryPointSelection`memiliki lima parameter (tiga diperlukan dan dua opsional). Nilai yang Anda tentukan menentukan titik pemulihan mana yang termasuk dalam tes pemulihan. Anda harus menunjukkan dengan `Algorithm` apakah Anda menginginkan titik pemulihan terbaru di dalam Anda `SelectionWindowDays` atau jika Anda menginginkan titik pemulihan acak, dan Anda harus menunjukkan melalui `IncludeVaults` brankas mana titik pemulihan dapat dipilih.

Sebuah pilihan dapat memiliki satu atau lebih ARN sumber daya yang dilindungi atau dapat memiliki satu atau lebih kondisi, tetapi tidak dapat memiliki keduanya.

Anda juga dapat memasukkan:

- `ScheduleExpressionTimezone`
- `Tags`
- `CreatorRequestId`
- `StartWindowHours`

Gunakan perintah CLI. `create-restore-testing-plan`

Setelah rencana berhasil dibuat, Anda perlu menetapkan sumber daya untuk menggunakannya `create-restore-testing-selection`.

Ini terdiri dari`RestoreTestingSelectionName`,`ProtectedResourceType`, dan salah satu dari yang berikut:

- `ProtectedResourceArns`

- `ProtectedResourceConditions`

  Setiap jenis sumber daya yang dilindungi dapat memiliki satu nilai tunggal. Pilihan pengujian pemulihan dapat menyertakan nilai wildcard (“*”) untuk `ProtectedResourceArns` bersama dengan`ProtectedResourceConditions`. Atau, Anda dapat menyertakan hingga 30 ARN sumber daya terlindungi tertentu di`ProtectedResourceArns`.

Penentuan titik pemulihan

Setiap kali rencana pengujian berjalan (sesuai dengan frekuensi dan waktu mulai yang Anda tentukan), satu titik pemulihan yang memenuhi syarat per sumber daya yang dilindungi dalam pemilihan dipulihkan oleh pengujian pemulihan. Jika tidak ada titik pemulihan untuk sumber daya yang memenuhi kriteria pemilihan titik pemulihan, sumber daya itu tidak akan dimasukkan dalam pengujian.

Titik pemulihan untuk sumber daya yang dilindungi dalam pemilihan pengujian memenuhi syarat jika memenuhi kriteria untuk kerangka waktu yang ditentukan dan menyertakan brankas dalam rencana pengujian pemulihan.

Sumber daya yang dilindungi dipilih jika pemilihan pengujian sumber daya menyertakan jenis sumber daya dan jika salah satu dari kondisi berikut benar:

- Sumber daya ARN ditentukan dalam seleksi itu; atau,
- Kondisi tag pada pilihan tersebut cocok dengan tag pada titik pemulihan terbaru untuk sumber daya

Perbarui rencana pengujian pemulihan

Anda dapat memperbarui bagian dari rencana pengujian pemulihan dan pilihan sumber daya di dalamnya melalui konsol atau AWS CLI.

Console

Perbarui paket dan pilihan pengujian pemulihan di konsol

Saat Anda melihat halaman detail rencana pengujian pemulihan di konsol, Anda dapat mengedit (memperbarui) banyak pengaturan paket Anda. Untuk melakukan ini,

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.

2. Di navigasi sebelah kiri, cari Restore testing dan pilih.
3. Pilih tombol Edit.
4. Sesuaikan frekuensi, waktu mulai, dan waktu tes akan dimulai di mana tes akan dimulai setelah waktu mulai yang dipilih.
5. Simpan perubahan Anda.

AWS CLI

Perbarui rencana dan pilihan pengujian pemulihan melalui AWS CLI

Permintaan UpdateRestoreTestingPlandan UpdateRestoreTestingSelectiondapat digunakan untuk mengirim pembaruan sebagian ke rencana atau pilihan tertentu. Nama-nama tidak dapat diubah, tetapi Anda dapat memperbarui parameter lainnya. Sertakan hanya parameter yang ingin Anda ubah di setiap permintaan.

Sebelum mengirim permintaan pembaruan, gunakan GetRestoreTestingPlandan GetRestoreTestingSelectionuntuk menentukan apakah Anda RestoreTestingSelection berisi ARN tertentu atau apakah itu menggunakan wildcard dan kondisi.

Jika pilihan pengujian pemulihan Anda telah menentukan ARN (bukan wildcard) dan Anda ingin mengubahnya menjadi wildcard dengan kondisi, permintaan pembaruan harus menyertakan wildcard ARN dan kondisinya. Pilihan dapat memiliki ARN sumber daya yang dilindungi atau menggunakan wildcard dengan kondisi, tetapi tidak dapat memiliki keduanya.

- `get-restore-testing-plan`
- `get-restore-testing-selection`
- `update-restore-testing-plan`
- `update-restore-testing-selection`

Lihat rencana pengujian pemulihan yang ada

Console

Melihat detail tentang rencana pengujian pemulihan yang ada dan sumber daya yang ditetapkan di konsol

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.

2. Pilih Pulihkan pengujian dari navigasi sebelah kiri. Layar menunjukkan rencana pengujian pemulihan Anda. Paket ditampilkan secara default oleh runtime terakhir.
3. Pilih tautan dari rencana untuk melihat detailnya, termasuk ringkasan paket, namanya, frekuensi, waktu mulai, dan mulai dalam nilai.

Anda juga dapat melihat sumber daya yang dilindungi dalam paket ini, pekerjaan pengujian pemulihan dari 30 hari terakhir yang termasuk dalam paket ini, dan tag apa pun yang dapat Anda buat untuk menjadi bagian dari rencana pengujian ini.

AWS CLI

Dapatkan detail tentang rencana pengujian pemulihan yang ada dan pemilihan pengujian menggunakan baris perintah

- `list-restore-testing-plan`
- `list-restore-testing-selections`
- `get-restore-testing-plan`
- `get-restore-testing-selection`

Lihat pekerjaan pengujian pemulihan

Console

Melihat pekerjaan pengujian pemulihan yang ada di konsol

Memulihkan pekerjaan pengujian disertakan pada halaman memulihkan pekerjaan.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Arahkan ke halaman Pekerjaan.

   Atau, Anda dapat memilih Pulihkan pengujian, lalu pilih rencana pengujian pemulihan untuk melihat detailnya dan pekerjaan yang terkait dengan rencana tersebut.
3. Pilih tab Pulihkan pekerjaan.

   Di halaman ini, Anda dapat melihat status, waktu pemulihan, jenis pemulihan, ID sumber daya, jenis sumber daya, mengembalikan rencana pengujian tempat pekerjaan itu berada, waktu pembuatan, dan ID titik pemulihan dari pekerjaan pemulihan.

Pekerjaan yang termasuk dalam rencana pengujian pemulihan memiliki jenis Pengujian pemulihan.

Kembalikan pekerjaan pengujian memiliki beberapa kategori status:

- Jenis status yang memerlukan perhatian digarisbawahi; arahkan kursor ke status untuk melihat detail tambahan jika tersedia.
- Status validasi akan ditampilkan jika Kembalikan validasi pengujian telah dimulai pada pengujian (tidak tersedia di dalam konsol).
- Status penghapusan mencatat status data yang dihasilkan oleh tes pemulihan. Ada tiga kemungkinan status penghapusan: Sukses, Menghapus, dan Gagal.

  Jika penghapusan pekerjaan pengujian pemulihan gagal, Anda harus menghapus sumber daya secara manual karena alur pengujian pemulihan tidak dapat menyelesaikannya secara otomatis. Seringkali, penghapusan yang gagal dipicu jika tag `awsbackup-restore-test` dihapus dari sumber daya.

AWS CLI

Lihat pekerjaan pengujian pemulihan yang ada dari baris perintah

- `list-restore-jobs-by-protected-resource`

Hapus rencana pengujian pemulihan

Console

Hapus paket pengujian pemulihan di konsol

1. Buka Lihat rencana pengujian pemulihan yang ada untuk melihat rencana pengujian pemulihan Anda saat ini.
2. Pada halaman rincian rencana pengujian pemulihan, hapus paket dengan memilih Hapus.
3. Setelah Anda memilih hapus, layar konfirmasi pop-up akan muncul untuk memastikan Anda ingin menghapus paket Anda. Pada layar ini, nama rencana pengujian pemulihan spesifik Anda akan ditampilkan dalam huruf tebal. Untuk melanjutkan, ketikkan nama peka huruf

besar/kecil yang tepat dari rencana pengujian, termasuk garis bawah, tanda hubung, dan titik apa pun.

Jika opsi untuk Hapus rencana pengujian pemulihan tidak dapat dipilih, masukkan kembali nama hingga cocok dengan nama yang ditampilkan. Setelah sama persis, opsi untuk menghapus rencana pengujian pemulihan akan dapat dipilih.

AWS CLI

Hapus rencana pengujian pemulihan melalui baris perintah

Perintah CLI DeleteRestoreTestingSelectiondapat digunakan untuk menghapus pilihan pengujian pemulihan. Termasuk `RestoreTestingPlanName` dan `RestoreTestingSelectionName` dalam permintaan.

Semua pilihan pengujian yang terkait dengan rencana pengujian harus dihapus sebelum Anda menghapus rencana pengujian. Setelah semua pilihan pengujian telah dihapus, Anda dapat menggunakan permintaan API DeleteRestoreTestingPlanuntuk menghapus rencana pengujian pemulihan. Anda perlu memasukkan`RestoreTestingPlanName`.

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

Pengujian pemulihan audit

Pulihkan integrasi pengujian dengan manajer AWS Backup Audit untuk membantu Anda mengevaluasi apakah sumber daya yang dipulihkan selesai dalam waktu pemulihan target Anda.

Untuk informasi selengkapnya, lihat Memulihkan waktu untuk sumber daya yang memenuhi kontrol target di kontrol dan remediasi AWS Backup Audit Manager.

Kembalikan kuota dan parameter pengujian

- 100 mengembalikan rencana pengujian
- 50 tag dapat ditambahkan ke setiap rencana pengujian pemulihan
- 30 pilihan per paket
- 30 ARN sumber daya yang dilindungi per pilihan

- 30 kondisi sumber daya yang dilindungi per pilihan (termasuk yang ada di dalam keduanya `StringEquals` dan`StringNotEquals`)
- 30 pemilih vault per pilihan
- Hari jendela pemilihan maksimum: 365 hari
- Mulai jam jendela: Min: 1 jam; Maks: 168 jam (7 hari)
- Panjang nama paket maks: 50 karakter
- Panjang nama pemilihan maks: 50 karakter

Informasi tambahan mengenai batasan dapat dilihat diAWS Backup kuota.

Kembalikan pemecahan masalah kegagalan pengujian

Jika Anda memiliki pekerjaan pengujian pemulihan dengan status pemulihan`Failed`, alasan berikut dapat membantu Anda menentukan penyebab dan penyembuhannya.

Pesan kesalahan dapat dilihat di AWS Backup konsol di halaman detail status pekerjaan atau dengan menggunakan perintah `list-restore-jobs-by-protected-resource` CLI atau. `list-restore-jobs`

1. Kesalahan: *`No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.`*

   Solusi 1: Perbarui pilihan pengujian pemulihan Anda dan ganti `SubnetId` parameternya. AWS Backup Konsol menampilkan parameter ini sebagai “Subnet”.

   Solusi 2: Buat ulang VPC default.

   Jenis sumber daya yang terpengaruh: Amazon EC2

2. Kesalahan: *`No subnets found for the default VPC [vpc]. Please specify a subnet.`*

   Solusi 1: Perbarui pilihan pengujian pemulihan Anda dan ganti parameter `SubnetId` pemulihan. AWS Backup Konsol menampilkan parameter ini sebagai “Subnet”.

   Solusi 2: Buat subnet default di VPC default.

   Jenis sumber daya yang terpengaruh: Amazon EC2

3. Kesalahan: *`No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.`*

   Solusi 1: Perbarui pilihan pengujian pemulihan Anda dan ganti parameter `DBSubnetGroupName` pemulihan. AWS Backup Konsol menampilkan parameter ini sebagai grup Subnet.

   Solusi 2: Buat subnet default di VPC default.

   Jenis sumber daya yang terpengaruh: Amazon Aurora, Amazon DocumentDB, Amazon RDS, Neptunus

4. Kesalahan:*`IAM Role cannot be assumed by AWS Backup`*.

   Solusi: Peran pemulihan harus diasumsikan oleh AWS Backup. Perbarui kebijakan kepercayaan peran di IAM untuk memungkinkannya diasumsikan oleh `"backup.amazonaws.com"` atau perbarui pilihan pengujian pemulihan Anda untuk menggunakan peran yang dapat diasumsikan oleh. AWS Backup

   Jenis sumber daya yang terpengaruh: semua

5. Kesalahan: *`Access denied to KMS key.`* atau *`The specified AWS KMS key`* `ARN` *`does not exist, is not enabled or you do not have permissions to access it.`*

   Solusi: Verifikasi hal berikut:

   a. Peran pemulihan memiliki akses ke AWS KMS kunci yang digunakan untuk mengenkripsi cadangan Anda dan, jika berlaku, kunci KMS yang digunakan untuk mengenkripsi sumber daya yang dipulihkan.

   b. Kebijakan sumber daya pada kunci KMS di atas memungkinkan peran pemulihan untuk mengaksesnya.

   Jika kondisi di atas belum terpenuhi, konfigurasikan peran pemulihan dan kebijakan sumber daya untuk akses yang sesuai. Kemudian, jalankan pekerjaan pengujian pemulihan lagi.

   Jenis sumber daya yang terpengaruh: semua

6. Kesalahan: *`User ARN is not authorized to perform action on resource because no identity based policy allows the action.`* atau*`Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx`*.

Solusi: Peran pemulihan tidak memiliki izin yang memadai. Perbarui izin di IAM untuk peran pemulihan.

Jenis sumber daya yang terpengaruh: semua

7. Kesalahan: *User ARN is not authorized to perform action on resource because no resource-based policy allows the action.* atau *User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.*

   Solusi: Peran pemulihan tidak memiliki akses yang memadai ke sumber daya yang ditentukan dalam pesan. Perbarui kebijakan sumber daya pada sumber daya yang disebutkan.

   Jenis sumber daya yang terpengaruh: semua

Kembalikan pengujian metadata yang disimpulkan

Memulihkan titik pemulihan membutuhkan metadata pemulihan. Untuk melakukan pengujian pemulihan, AWS Backup secara otomatis menyimpulkan metadata yang kemungkinan akan menghasilkan pemulihan yang berhasil. Perintah ini `get-restore-testing-inferred-metadata` dapat digunakan untuk melihat pratinjau apa yang AWS Backup akan disimpulkan. Perintah `get-restore-job-metadata` mengembalikan set metadata disimpulkan oleh. AWS Backup Perhatikan bahwa untuk beberapa jenis sumber daya (Amazon FSx), AWS Backup tidak dapat menyimpulkan satu set lengkap metadata.

Metadata pemulihan yang disimpulkan ditentukan selama proses pengujian pemulihan.
Anda dapat mengganti kunci metadata pemulihan tertentu dengan memasukkan parameter `RestoreMetadataOverrides` di badan. `RestoreTestingSelection` Beberapa penggantian metadata tidak tersedia di konsol. AWS Backup

Setiap sumber daya yang didukung memiliki kunci dan nilai metadata pemulihan yang disimpulkan, serta kunci metadata pemulihan yang dapat diganti. Hanya pasangan nilai `RestoreMetadataOverrides` kunci atau pasangan nilai kunci bersarang yang ditandai dengan *required untuk pemulihan yang berhasil* yang perlu disertakan; yang lainnya bersifat opsional. Perhatikan bahwa nilai kunci tidak peka huruf besar/kecil.

> **Important**
>
> AWS Backup dapat menyimpulkan bahwa sumber daya harus dikembalikan ke setelan default, seperti instans Amazon EC2 atau kluster Amazon RDS yang dipulihkan ke VPC default. Namun, jika default tidak ada, misalnya VPC atau subnet default telah dihapus dan tidak ada penggantian metadata yang dimasukkan, pemulihan tidak akan berhasil.

Jenis sumber daya	Kunci dan nilai metadata pemulihan yang disimpulkan	Metadata yang dapat diganti

DynamoDB	`deletionProtection` , di mana nilai diatur ke `false`
	
	`encryptionType` diatur ke `Default`
	
	`targetTableName` , di mana nilai diatur ke nilai acak dimulai dengan `awsbackup-restore-test-`
		`encryptionType`
		
		`kmsMasterKeyArn`

Amazon EBS	`availabilityZone` , yang nilainya disetel ke zona ketersediaan acak
	
	`encrypted` , yang nilainya disetel ke `true`
		`availabilityZone`
		
		`kmsKeyId`

Amazon EC2	`disableApiTermination` nilai diatur ke `false`
	
	`instanceType` nilai diatur ke InstanceType dari titik pemulihan yang dipulihkan
	
	`requiredImdsV2` nilai diatur ke `true`
		`iamInstanceProfileName` nilai bisa null atau `UseBackedUpValue`
		
		`instanceType`
		
		`requireImdsV2`
		
		`securityGroupIds`

Jenis sumber daya	Kunci dan nilai metadata pemulihan yang disimpulkan	Metadata yang dapat diganti
		`subnetId`

Amazon EFS	`encrypted` nilai diatur ke `true`
	
	`file-system-id` nilai diatur ke ID sistem file dari titik pemulihan yang dipulihkan
	
	`kmsKeyId` value diatur ke `alias/aws/elasticfilesystem`
	
	`newFileSystem` nilai diatur ke `true`
	
	`performanceMode` nilai diatur ke `generalPurpose`
		`kmsKeyId`

Amazon FSx for Lustre	`lustreConfiguration` memiliki kunci bersarang. Salah satu kunci bersarang adalah`automaticBackupRetentionDays`, nilai yang diatur ke `0`	`kmsKeyId`
		
		`lustreConfiguration` memiliki kunci bersarang `logConfiguration`
		
		`securityGroupIds`
		
		`subnetIds` , *diperlukan untuk pemulihan yang berhasil*

Jenis sumber daya	Kunci dan nilai metadata pemulihan yang disimpulkan	Metadata yang dapat diganti
Amazon FSx untuk ONTAP NetApp	`name`diatur ke nilai acak yang dimulai dengan `awsbackup_restore_test_` `ontapConfiguration` memiliki kunci bersarang, termasuk: • `junctionPath` di `/name` mana nama volume yang dipulihkan • `sizeInMegabytes` , nilai yang diatur ke ukuran dalam megabyte dari titik pemulihan yang dipulihkan • `snapshotPolicy` di mana nilai diatur ke none	`ontapConfiguration` memiliki kunci bersarang khusus yang dapat diganti, termasuk: • `junctionPath` • `ontapVolumeType` • `securityStyle` • `sizeInMegabytes` • `storageEfficiencyEnabled` • `storageVirtualMachineId` , *diperlukan untuk pemulihan yang berhasil* • `tieringPolicy`

Jenis sumber daya	Kunci dan nilai metadata pemulihan yang disimpulkan	Metadata yang dapat diganti

Amazon FSx untuk OpenZFS	`openZfzConfiguration` , yang memiliki kunci bersarang , termasuk:
	• `automaticBackupRetentionDays` dengan nilai ditetapkan ke `0`
	• `deploymentType` dengan nilai yang disetel ke jenis penerapan titik pemulihan yang dipulihkan
	• `throughputCapacity` , yang nilainya didasarkan padadeploymentType . Jika deploymentType yaSINGLE_AZ_1 , nilainya diatur ke64; jika deploymentType adaSINGLE_AZ_2 or MULTI_AZ_1 , nilainya diatur ke 160
		`kmsKeyId`
		`openZfsConfiguration` memiliki kunci bersarang khusus yang dapat diganti, termasuk:
		• `deploymentType`
		• `throughputCapacity`
		• `diskiopsConfiguration`
		`securityGroupIds`
		`subnetIds`

Jenis sumber daya	Kunci dan nilai metadata pemulihan yang disimpulkan	Metadata yang dapat diganti

Amazon FSx for Windows File Server	`windowsConfiguration` , yang memiliki kunci bersarang termasuk:
	• `automaticBackupRetentionDays` dengan nilai ditetapkan ke `0`
	• `deploymentType` dengan nilai yang disetel ke jenis penerapan titik pemulihan yang dipulihkan
	• `throughputCapacity` dengan nilai ditetapkan ke `8`
		`kmsKeyId`
		`securityGroupIds`
		`subnetIds` *diperlukan untuk pemulihan yang berhasil*
		`windowsConfiguration` , dengan kunci bersarang tertentu yang dapat diganti
		• `throughputCapacity`
		• `activeDirectoryId` *diperlukan untuk pemulihan yang berhasil* `selfManagedActiveDirectoryConfiguration` *jika tidak disertakan*
		• `selfManagedActiveDirectoryConfiguration` *diperlukan untuk pemulihan yang berhasil* `activeDirectoryId` *jika tidak disertakan*
		• `preferredSubnetId`

Jenis sumber daya	Kunci dan nilai metadata pemulihan yang disimpulkan	Metadata yang dapat diganti

Amazon RDS, Aurora, Amazon DocumentDB, kluster Amazon Neptunus	`availabilityZones` dengan nilai diatur ke daftar hingga tiga zona ketersediaan acak
	
	`dbClusterIdentifier` dengan nilai acak dimulai dengan `awsbackup-restore-test`
	
	`engine`dengan nilai yang disetel ke mesin titik pemulihan dipulihkan
		`availabilityZones`
		
		`databaseName`
		
		`dbClusterParameterGroupName`
		
		`dbSubnetGroupName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`engine`
		
		`engineMode`
		
		`engineVersion`
		
		`kmskeyId`
		
		`port`
		
		`optionGroupName`
		
		`scalingConfiguration`
		
		`vpcSecurityGroupIds`

Jenis sumber daya	Kunci dan nilai metadata pemulihan yang disimpulkan	Metadata yang dapat diganti

Instans Amazon RDS	`dbInstanceIdentifier` dengan nilai acak dimulai dengan `awsbackup-restore-test-`
	
	`deletionProtection` dengan nilai ditetapkan ke `false`
	
	`multiAz`dengan nilai ditetapkan ke `false`
	
	`publiclyAccessible` dengan nilai disetel ke false
		`allocatedStorage`
		
		`availabilityZones`
		
		`dbInstanceClass`
		
		`dbName`
		
		`dbParameterGroupName`
		
		`dbSubnetGroupName`
		
		`domain`
		
		`domainIamRoleName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`iops`
		
		`licensemodel`
		
		`multiAz`
		
		`optionGroupName`
		
		`port`
		
		`processorFeatures`
		
		`publiclyAccessible`
		
		`storageType`
		
		`vpcSecurityGroupIds`

Jenis sumber daya	Kunci dan nilai metadata pemulihan yang disimpulkan	Metadata yang dapat diganti

Amazon Simple Storage Service (Amazon S3)	`destinationBucketName` dengan nilai acak dimulai dengan `awsbackup-restore-test-`
	
	`encrypted` dengan nilai ditetapkan ke `true`
	
	`encryptionType` dengan nilai ditetapkan ke `SSE-S3`
	
	`newBucket` dengan nilai ditetapkan ke `true`
		`encryptionType`
		
		`kmsKey`

Kembalikan validasi pengujian

Anda memiliki opsi untuk membuat validasi berbasis peristiwa yang berjalan saat pekerjaan pengujian pemulihan selesai.

Pertama, buat alur kerja validasi dengan target apa pun yang didukung oleh Amazon EventBridge, seperti. AWS Lambda Kedua, tambahkan EventBridge aturan yang mendengarkan pekerjaan pemulihan mencapai status`COMPLETED`. Ketiga, buat rencana pengujian pemulihan (atau biarkan yang sudah ada berjalan sesuai jadwal). Terakhir, setelah pengujian pemulihan selesai, pantau log alur kerja validasi untuk memastikannya berjalan seperti yang diharapkan (setelah validasi berjalan, status validasi akan ditampilkan di konsol).AWS Backup

1. Siapkan alur kerja validasi

   Anda dapat mengatur alur kerja validasi menggunakan Lambda atau target lain yang didukung oleh. EventBridge Misalnya, jika Anda memvalidasi pengujian pemulihan yang berisi instans Amazon EC2, Anda dapat menyertakan kode yang melakukan ping pada titik akhir pemeriksaan kesehatan.

   Anda dapat menggunakan detail dalam acara tersebut untuk menentukan sumber daya mana yang akan divalidasi.

Anda dapat menggunakan lapisan Lambda khusus untuk menggunakan SDK terbaru (karena belum `PutRestoreValidationResult` tersedia melalui Lambda SDK).

Berikut ini sampelnya:

```
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. Tambahkan EventBridge aturan

   Buat EventBridge aturan yang mendengarkan `COMPLETED`dacara restore job.

   Secara opsional, Anda dapat memfilter peristiwa berdasarkan jenis sumber daya atau memulihkan rencana pengujian ARN. Tetapkan target aturan ini untuk menjalankan alur kerja validasi yang Anda tentukan di Langkah 1. Inilah contohnya:

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
    "Restore Job State Change"
  ],
```

```
  "detail":{
    "resourceType":[
      "..."
    ],
    "restoreTestingPlanArn":[
      "..."
    ],
    "status":[
      "COMPLETED"
    ]
  }
}
```

3. Biarkan rencana pengujian pemulihan berjalan dan selesai

   Rencana pengujian pemulihan akan berjalan sesuai dengan jadwal yang telah Anda konfigurasikan.

   Lihat Membuat rencana pengujian pemulihan jika Anda belum memilikinya atau Memperbarui rencana pengujian pemulihan jika Anda ingin mengubah pengaturan.

4. Pantau hasilnya

   Setelah rencana pengujian pemulihan berjalan sesuai jadwal, Anda dapat memeriksa log alur kerja validasi Anda untuk memastikannya berjalan dengan benar.

   Anda dapat memanggil API `PutRestoreValidationResult` untuk memposting hasil, yang kemudian akan dapat dilihat di AWS Backup konsol dan melalui panggilan AWS Backup API yang menjelaskan dan mencantumkan pekerjaan pemulihan, seperti `DescribeRestoreJob` atau`ListRestoreJob`.

   Setelah status validasi ditetapkan, itu tidak dapat diubah.

Melihat daftar backup

Anda dapat melihat daftar cadangan Anda menggunakan AWS Backup konsol atau secara terprogram.

Topik

- Mencantumkan cadangan berdasarkan sumber daya yang dilindungi di konsol
- Daftar cadangan dengan brankas cadangan di konsol

- Membuat daftar cadangan secara terprogram

Mencantumkan cadangan berdasarkan sumber daya yang dilindungi di konsol

Ikuti langkah-langkah ini untuk melihat daftar cadangan sumber daya tertentu di konsol. AWS Backup

1. Masuk ke AWS Management Console, dan buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Sumber daya yang dilindungi.
3. Pilih sumber daya yang dilindungi dalam daftar untuk melihat daftar cadangan. Hanya sumber daya yang telah didukung oleh yang AWS Backup terdaftar di bawah Sumber daya yang dilindungi.

Anda dapat melihat cadangan untuk sumber daya. Dari tampilan ini, Anda juga dapat memilih cadangan dan mengembalikannya.

Daftar cadangan dengan brankas cadangan di konsol

Ikuti langkah-langkah ini untuk melihat daftar cadangan yang diatur dalam brankas cadangan.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Di bagian Cadangan, lihat daftar semua cadangan yang diatur dalam brankas cadangan ini. Dalam tampilan ini, Anda dapat mengurutkan cadangan berdasarkan header kolom mana pun (termasuk status), serta memilih cadangan untuk memulihkannya, mengeditnya, atau menghapusnya.

Membuat daftar cadangan secara terprogram

Anda dapat membuat daftar cadangan secara terprogram menggunakan operasi API: `ListRecoveryPoint`

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

Misalnya, perintah AWS Command Line Interface (AWS CLI) berikut mencantumkan semua cadangan Anda dengan status: `EXPIRED`

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

Anda dapat menggunakan AWS Backup Audit Manager untuk mengaudit kepatuhan AWS Backup kebijakan Anda terhadap kontrol yang Anda tetapkan. Kontrol adalah prosedur yang dirancang untuk mengaudit kepatuhan persyaratan cadangan, seperti frekuensi cadangan atau periode retensi cadangan.

AWS Backup Audit Manager membantu Anda menjawab pertanyaan seperti:

- “Apakah saya mencadangkan semua sumber daya saya?”
- “Apakah semua cadangan saya dienkripsi?”
- “Apakah backup saya berlangsung setiap hari?”

Anda dapat menggunakan AWS Backup Audit Manager untuk menemukan aktivitas cadangan dan sumber daya yang belum sesuai dengan kontrol yang Anda tetapkan. Perhatikan bahwa hanya sumber daya aktif yang akan disertakan saat kontrol mengevaluasi sumber daya untuk kepatuhan. Misalnya, instans Amazon EC2 dalam status berjalan akan dievaluasi. Instans EC2 dalam keadaan berhenti tidak akan dimasukkan dalam evaluasi kepatuhan.

Anda juga dapat menggunakannya untuk secara otomatis membuat jejak audit laporan harian dan sesuai permintaan untuk tujuan tata kelola cadangan Anda.

Langkah-langkah berikut memberikan gambaran umum tentang cara menggunakan AWS Backup Audit Manager. Untuk penelusuran terperinci, pilih salah satu topik di akhir halaman ini.

1. Buat kerangka kerja yang berisi satu atau beberapa templat kontrol tata kelola. Pertanyaan-pertanyaan sebelumnya adalah contoh dari tiga template kontrol tata kelola. Anda dapat menyesuaikan parameter dari beberapa template kontrol tata kelola. Misalnya, Anda dapat menyesuaikan kontrol terakhir untuk bertanya, “Apakah cadangan saya berlangsung setiap minggu?” bukannya setiap hari.
2. Lihat kerangka kerja Anda untuk melihat berapa banyak sumber daya Anda yang sesuai (atau tidak sesuai) dengan kontrol yang Anda tetapkan dalam kerangka kerja itu.
3. Buat laporan status cadangan dan kepatuhan Anda. Simpan laporan ini sebagai bukti praktik kepatuhan Anda yang dapat dibuktikan, atau untuk mengidentifikasi aktivitas pencadangan individu dan sumber daya yang belum sesuai.

AWS Backup Audit Manager secara otomatis membuat laporan baru untuk Anda setiap 24 jam dan menerbitkannya ke Amazon S3. Anda juga dapat membuat laporan sesuai permintaan.

> **Note**
>
> Sebelum Anda membuat kerangka kerja terkait kepatuhan pertama Anda, Anda harus mengaktifkan pelacakan sumber daya. Melakukannya memungkinkan AWS Config untuk melacak AWS Backup sumber daya Anda. Untuk dokumentasi teknis tentang cara mengelola pelacakan sumber daya, lihat Menyiapkan AWS Config dengan konsol di Panduan AWS Config Pengembang.
>
> Biaya berlaku saat Anda mengaktifkan pelacakan sumber daya. Untuk informasi tentang penetapan harga dan penagihan sumber daya untuk AWS Backup Audit Manager, lihat Pengukuran, biaya, dan penagihan.

Topik

Bekerja dengan kerangka kerja audit

Framework adalah kumpulan kontrol yang membantu Anda mengevaluasi praktik pencadangan Anda. Anda dapat menggunakan kontrol yang telah dibuat sebelumnya dan dapat disesuaikan untuk menentukan kebijakan dan mengevaluasi apakah praktik pencadangan sesuai dengan kebijakan Anda. Anda juga dapat menyiapkan laporan harian otomatis untuk mendapatkan wawasan tentang status kepatuhan kerangka kerja Anda.

Setiap kerangka berlaku untuk satu akun dan Wilayah AWS. Anda dapat menerapkan maksimal 15 kerangka kerja per akun per Wilayah. Anda tidak dapat menerapkan kerangka kerja duplikat (kerangka kerja yang berisi kontrol dan parameter yang sama).

Ada dua jenis kerangka kerja:

- AWS Backup Kerangka kerja (disarankan) — Gunakan AWS Backup kerangka kerja untuk menerapkan semua kontrol yang tersedia untuk memantau aktivitas pencadangan, cakupan, dan sumber daya Anda terhadap praktik terbaik yang kami rekomendasikan.
- Kerangka kustom yang Anda tentukan — Gunakan kerangka kerja khusus untuk memilih satu atau lebih kontrol spesifik dan untuk menyesuaikan parameter kontrol.

Topik

Memilih kontrol Anda

Tabel berikut mencantumkan kontrol AWS Backup Audit Manager, parameternya yang dapat disesuaikan, dan jenis sumber daya AWS Config perekamannya. Setiap kontrol memerlukan jenis sumber daya perekaman `AWS Config: resource compliance` karena jenis ini mencatat status kepatuhan Anda.

Kontrol yang tersedia

Nama kontrol	Deskripsi kontrol	Parameter yang dapat disesuaikan	AWS Config jenis sumber daya rekaman
Sumber daya cadangan dilindungi oleh rencana cadangan	Mengevaluasi apakah sumber daya dilindungi oleh rencana cadangan.	Tidak ada	`AWS Backup: backup selection`
Paket Backup memiliki frekuensi	Mengevaluasi apakah frekuensi cadangan	Frekuensi backup; periode retensi	`AWS Backup: backup plans`

Nama kontrol	Deskripsi kontrol	Parameter yang dapat disesuaikan	AWS Config jenis sumber daya rekaman
minimum dan retensi minimum	setidaknya [1 hari] dan periode retensi setidaknya [35 hari].		
Vaults mencegah penghapusan manual titik pemulihan	Mengevaluasi jika brankas cadangan tidak mengizinkan penghapusan titik pemulihan secara manual kecuali oleh peran tertentu AWS Identity and Access Management (IAM). Secara default, tidak ada pengecualian peran IAM. Juga tidak ada pengecualian peran IAM saat Anda menerapkan kontrol ini dengan kerangka kerja. AWS Backup	Hingga 5 peran IAM yang memungkinkan penghapusan manual titik pemulihan	`AWS Backup: backup vaults`
Poin pemulihan dienkripsi	Mengevaluasi apakah titik pemulihan dienkripsi.	Tidak ada	`AWS Backup: recovery points`
Retensi minimum ditetapkan untuk titik pemulihan	Mengevaluasi jika periode retensi titik pemulihan setidaknya [35 hari].	Periode retensi titik pemulihan	`AWS Backup: recovery points`

Nama kontrol	Deskripsi kontrol	Parameter yang dapat disesuaikan	AWS Config jenis sumber daya rekaman
Salinan cadangan Lintas Wilayah dijadwalkan	Mengevaluasi jika sumber daya dikonfigurasi untuk membuat salinan cadangannya ke yang lain. Wilayah AWS	Wilayah AWS	`AWS Backup: backup selection`
Salinan cadangan lintas akun dijadwalkan	Mengevaluasi jika sumber daya memiliki salinan cadangan lintas akun yang dikonfigurasi.	AWS ID akun	`AWS Backup: backup selection`
Cadangan dilindungi oleh AWS Backup Vault Lock	Mengevaluasi jika sumber daya dikonfigurasi untuk memiliki cadangan di brankas cadangan yang terkunci.	Hari Retensi Min; Hari Retensi Maks	`AWS Backup: backup selection`
Titik pemulihan terakhir dibuat	Mengevaluasi jika titik pemulihan dibuat dalam kerangka waktu yang ditentukan.	Nilai dalam jam [1ke744] atau hari [1ke31].	`AWS Backup recovery points`
Mengembalikan waktu untuk sumber daya memenuhi target	Mengevaluasi jika pekerjaan pengujian pemulihan selesai dalam waktu pemulihan target	Nilai dalam hitungan menit	Tidak ada

Untuk informasi rinci tentang kontrol ini, lihatKontrol dan remediasi.

Untuk daftar sumber daya yang AWS Backup didukung yang tidak mendukung semua kontrol, lihat bagian AWS Backup Audit Manager pada Ketersediaan fitur berdasarkan sumber daya tabel.

> **Note**
>
> Jika Anda tidak ingin menggunakan salah satu kontrol sebelumnya, Anda masih dapat menggunakan AWS Backup Audit Manager untuk membuat laporan harian pencadangan, menyalin, dan memulihkan pekerjaan Anda. Lihat Bekerja dengan laporan audit.

Mengaktifkan pelacakan sumber daya

Sebelum Anda membuat kerangka kerja terkait kepatuhan pertama Anda, Anda harus mengaktifkan pelacakan sumber daya. Melakukannya memungkinkan AWS Config untuk melacak AWS Backup sumber daya Anda. Untuk dokumentasi teknis tentang cara mengelola pelacakan sumber daya, lihat Menyiapkan AWS Config dengan konsol di Panduan AWS Config Pengembang.

Biaya berlaku saat Anda mengaktifkan pelacakan sumber daya. Untuk informasi tentang penetapan harga dan penagihan sumber daya untuk AWS Backup Audit Manager, lihat Pengukuran, biaya, dan penagihan.

Topik

- Mengaktifkan pelacakan sumber daya menggunakan konsol
- Mengaktifkan pelacakan sumber daya menggunakan AWS Command Line Interface (AWS CLI)
- Mengaktifkan pelacakan sumber daya menggunakan AWS CloudFormation templat

Mengaktifkan pelacakan sumber daya menggunakan konsol

Untuk mengaktifkan pelacakan sumber daya menggunakan konsol:

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, di bawah Audit Manager, pilih Frameworks.
3. Aktifkan pelacakan sumber daya dengan memilih Kelola pelacakan sumber daya.
4. Pilih Buka AWS Config Pengaturan.
5. Pilih Aktifkan atau nonaktifkan perekaman.

6. Pilih Aktifkan perekaman untuk semua jenis sumber daya berikut, atau pilih untuk mengaktifkan perekaman untuk beberapa jenis sumber daya. Lihat kontrol dan remediasi AWS Backup Audit Manager untuk jenis sumber daya yang diperlukan untuk kontrol Anda.

   - `AWS Backup: backup plans`
   - `AWS Backup: backup vaults`
   - `AWS Backup: recovery points`
   - `AWS Backup: backup selection`

   > **Note**
   >
   > AWS Backup Audit Manager membutuhkan `AWS Config: resource compliance` untuk setiap kontrol.

7. Pilih Tutup.
8. Tunggu spanduk biru dengan teks Menghidupkan pelacakan sumber daya untuk transisi ke spanduk hijau dengan teks Pelacakan sumber daya aktif.

Anda dapat memeriksa apakah Anda telah mengaktifkan pelacakan sumber daya dan, jika demikian, jenis sumber daya yang Anda rekam, di dua tempat di AWS Backup konsol. Di panel navigasi kiri, baik:

- Pilih Kerangka, lalu pilih teks di bawah status AWS Config perekam.
- Pilih Pengaturan, lalu pilih teks di bawah status AWS Config perekam.

Mengaktifkan pelacakan sumber daya menggunakan AWS Command Line Interface (AWS CLI)

Jika Anda belum onboard AWS Config, mungkin lebih cepat untuk onboard menggunakan. AWS CLI

Untuk mengaktifkan pelacakan sumber daya menggunakan AWS CLI:

1. Ketik perintah berikut untuk menentukan apakah Anda sudah mengaktifkan AWS Config perekam Anda.

```
$ aws configservice describe-configuration-recorders
```

a. Jika `ConfigurationRecorders` daftar Anda kosong seperti ini:

```
{
  "ConfigurationRecorders": []
}
```

Perekam Anda tidak diaktifkan. Lanjutkan ke langkah 2 untuk membuat perekam Anda.

b. Jika Anda sudah mengaktifkan perekaman untuk semua sumber daya, `ConfigurationRecorders` output Anda akan terlihat seperti ini:

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
}
```

Karena Anda mengaktifkan semua sumber daya, Anda sudah mengaktifkan pelacakan sumber daya. Anda tidak perlu menyelesaikan sisa prosedur ini untuk menggunakan AWS Backup Audit Manager.

c. Jika Anda `ConfigurationRecorders` tidak kosong, tetapi Anda belum mengaktifkan perekaman untuk semua sumber daya, tambahkan sumber daya cadangan ke perekam yang ada menggunakan perintah berikut. Kemudian lewati ke langkah 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. Membuat AWS Config perekam dengan tipe sumber daya 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. Jelaskan AWS Config perekam Anda.

```
$ aws configservice describe-configuration-recorders
```

Verifikasi bahwa ia memiliki tipe sumber daya AWS Backup Audit Manager dengan membandingkan output Anda dengan output yang diharapkan berikut.

```
{
  "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. Buat bucket Amazon S3 sebagai tujuan untuk menyimpan file AWS Config konfigurasi.

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. Gunakan *policy.json* untuk memberikan AWS Config izin untuk mengakses bucket Anda. Lihat contoh *policy.json* berikut.

```
$ 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. Konfigurasikan bucket Anda sebagai saluran AWS Config pengiriman

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. Aktifkan AWS Config perekaman

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. Verifikasi bahwa `"FrameworkStatus":"ACTIVE"` di baris terakhir `DescribeFramework` output Anda sebagai berikut.

```
$ 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"
}
```

Mengaktifkan pelacakan sumber daya menggunakan AWS CloudFormation templat

Untuk AWS CloudFormation templat yang mengaktifkan pelacakan sumber daya, lihat Menggunakan AWS Backup Audit Manager dengan AWS CloudFormation.

Membuat kerangka kerja menggunakan konsol AWS Backup

Setelah mengaktifkan pelacakan sumber daya, buat kerangka kerja menggunakan langkah-langkah berikut.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Frameworks.
3. Pilih Buat Kerangka.
4. Untuk nama Framework, masukkan nama unik. Nama kerangka kerja harus antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).
5. (Opsional) Masukkan deskripsi Framework.
6. Di Kontrol, kontrol aktif Anda akan ditampilkan. Secara default, semua kontrol yang memenuhi syarat untuk sumber daya dicantumkan.

   Untuk mengubah kontrol mana yang aktif, klik Edit kontrol.

   a. Kotak centang pertama menunjukkan apakah kontrol dihidupkan. Untuk mematikan kontrol, hapus centang pada kotak.

   b. Di bawah Pilih sumber daya untuk dievaluasi, Anda dapat memilih cara memilih sumber daya, menurut jenis, tag, atau dengan sumber daya tunggal.

Daftar kontrol AWS Backup Audit Manager menjelaskan opsi penyesuaian untuk setiap kontrol.

7. (Opsional) Tandai kerangka kerja Anda dengan memilih Tambahkan tag baru. Anda dapat menggunakan tag untuk mencari dan memfilter kerangka kerja Anda atau melacak biaya Anda.
8. Pilih Buat kerangka kerja.

AWS Backup Audit Manager mungkin membutuhkan waktu beberapa menit untuk membuat kerangka kerja.

Jika kesalahan `AlreadyExists` terjadi, kerangka kerja dengan kontrol dan parameter yang sama sudah ada. Agar berhasil membuat kerangka kerja baru, setidaknya satu kontrol atau parameter harus berbeda dari kerangka kerja yang ada.

Membuat kerangka kerja menggunakan API AWS Backup

Tabel berikut berisi contoh permintaan API CreateFramework untuk setiap kontrol, bersama dengan respons API sampel untuk DescribeFramework permintaan terkait. Untuk bekerja dengan AWS Backup Audit Manager secara terprogram, Anda dapat merujuk ke cuplikan kode ini.

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
`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_`

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
	["RDS"] // Evaluate only RDS instances } }], "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }	PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["RDS"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
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": {

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
	<pre>"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>	<pre>"Tags": {"key1": "prod"} } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }</pre>

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
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

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
	"Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }	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"} }

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
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":

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
		<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>

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
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"} }

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
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"} }

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
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"} }

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
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"} }

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
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"} }

Kontrol	**CreateFramework** permintaan	**DescribeFramework** respon
	}	

Melihat status kepatuhan kerangka kerja

Setelah Anda membuat kerangka kerja audit, itu muncul di tabel Frameworks Anda. Anda dapat melihat tabel ini dengan memilih Frameworks di panel navigasi kiri konsol. AWS Backup Untuk melihat hasil audit untuk framework Anda, pilih nama Framework. Melakukan hal itu akan membawa Anda ke halaman detail Framework, yang memiliki dua bagian: Ringkasan dan Kontrol.

Bagian Ringkasan mencantumkan status berikut dari kiri ke kanan:

- Status kepatuhan adalah status kepatuhan keseluruhan kerangka audit Anda sebagaimana ditentukan oleh status kepatuhan masing-masing kontrolnya. Status kepatuhan setiap kontrol ditentukan oleh status kepatuhan dari setiap sumber daya yang dievaluasi.

  Status kepatuhan kerangka kerja `Compliant` hanya jika semua sumber daya dalam lingkup evaluasi kontrol Anda telah lulus evaluasi tersebut. Jika satu atau lebih sumber daya gagal dalam evaluasi kontrol, status kepatuhan akan menjadi`Non-Compliant`. Untuk informasi tentang cara menemukan sumber daya yang tidak sesuai, lihat Menemukan sumber daya yang tidak sesuai. Untuk informasi tentang cara mematuhinya sumber daya Anda, lihat bagian remediasi kontrol dan remediasi AWS Backup Audit Manager.
- Status kerangka kerja mengacu pada apakah Anda telah mengaktifkan pelacakan sumber daya untuk semua sumber daya Anda. Status yang mungkin muncul adalah:
  - `Active`saat perekaman dihidupkan untuk semua sumber daya yang dievaluasi oleh kerangka kerja.
  - `Partially active`saat perekaman dimatikan untuk setidaknya satu sumber daya yang dievaluasi oleh kerangka kerja.
  - `Inactive`saat perekaman dimatikan untuk semua sumber daya yang dievaluasi oleh kerangka kerja.
  - `Unavailable`ketika AWS Backup Audit Manager tidak dapat memvalidasi status rekaman saat ini.

Untuk memperbaiki **`Inactive`** status **`Partially active`** atau

1. Pilih Frameworks dari panel navigasi kiri.
2. Pilih Kelola pelacakan sumber daya.
3. Ikuti petunjuk di pop-up untuk mengaktifkan perekaman yang sebelumnya tidak diaktifkan untuk jenis sumber daya Anda.

Untuk informasi selengkapnya tentang jenis sumber daya yang memerlukan pelacakan sumber daya berdasarkan kontrol yang disertakan dalam kerangka kerja, lihat komponen sumber daya kontrol dan remediasi AWS Backup Audit Manager.

- Status penerapan mengacu pada status penerapan kerangka kerja Anda. Status ini harus paling seringCompleted, tetapi bisa jugaCreate in progress,Update in progress,Delete in progress, danFailed.
  - Status Failed berarti kerangka kerja tidak diterapkan dengan benar. Hapus kerangka kerja, lalu buat ulang kerangka kerja melalui AWS Backup konsol atau melalui AWS Backup API.
- Kontrol yang sesuai menunjukkan jumlah kontrol kerangka kerja dengan semua evaluasi berlalu.
- Kontrol yang tidak sesuai menunjukkan jumlah kontrol kerangka kerja dengan setidaknya satu evaluasi tidak lulus.

Bagian Kontrol menunjukkan kepada Anda informasi berikut:

- Status kontrol mengacu pada status kepatuhan masing-masing kontrol. Kontrol dapat berupaCompliant, yang berarti semua sumber daya lulus evaluasi itu;Non-compliant, yang berarti bahwa setidaknya satu sumber daya tidak lulus evaluasi itu, ataуInsufficient data, yang berarti kontrol tidak menemukan sumber daya dalam ruang lingkup evaluasi untuk dievaluasi.
- Cakupan evaluasi dapat membatasi setiap kontrol ke satu atau beberapa jenis Sumber Daya, satu ID Sumber Daya, atau satu kunci Tag dan nilai Tag, berdasarkan cara Anda menyesuaikan kontrol saat membuat kerangka kerja audit. Jika semua bidang kosong (seperti yang ditunjukkan oleh tanda hubung, “-”), maka kontrol mengevaluasi semua sumber daya yang berlaku.

Menemukan sumber daya yang tidak sesuai

AWS Backup Audit Manager membantu Anda menemukan sumber daya mana yang tidak sesuai dengan dua cara.

- Saat Melihat status kepatuhan kerangka kerja, pilih nama kontrol di bagian Detail. Melakukan hal itu membawa Anda ke AWS Config konsol, di mana Anda dapat melihat daftar `Non-Compliant` sumber daya Anda.
- Setelah Anda membuat rencana laporan dengan templat kepatuhan sumber daya yang menyertakan kerangka kerja Anda, Anda dapat Melihat laporan untuk mengidentifikasi semua `Non-Compliant` sumber daya di semua kontrol Anda.

  Selanjutnya, Anda `Resource compliance report` menunjukkan terakhir kali AWS Backup Audit Manager mengevaluasi setiap kontrol Anda terakhir kali.

Memperbarui kerangka kerja audit

Anda dapat memperbarui deskripsi, kontrol, dan parameter kerangka kerja audit yang ada.

Untuk memperbarui kerangka kerja yang ada

1. Di panel navigasi kiri AWS Backup konsol, pilih Frameworks.
2. Pilih kerangka kerja yang ingin Anda edit dengan nama Framework nya.
3. Pilih Edit.

Menghapus kerangka kerja audit

Untuk menghapus kerangka kerja yang ada

1. Di panel navigasi kiri AWS Backup konsol, pilih Frameworks.
2. Pilih kerangka kerja yang ingin Anda hapus dengan nama Framework nya.
3. Pilih Hapus.
4. Ketik nama kerangka kerja Anda dan pilih Hapus kerangka kerja.

Bekerja dengan laporan audit

AWS Backup Laporan Audit Manager secara otomatis menghasilkan bukti AWS Backup aktivitas Anda, seperti:

- Pekerjaan cadangan mana yang selesai dan kapan
- Sumber daya apa yang Anda dukung

Ada dua jenis laporan. Saat membuat laporan, Anda memilih jenis yang dibuat.

Salah satu jenisnya adalah laporan pekerjaan, yang menunjukkan pekerjaan selesai dalam 24 jam terakhir dan semua pekerjaan aktif. Laporan pekerjaan tidak menampilkan status`completed with issues`. Untuk menemukan status ini, Anda dapat memfilter `Completed` pekerjaan dengan satu atau beberapa pesan status. AWS Backup Hanya akan menyertakan pesan status sebagai bagian dari status `Completed` pekerjaan jika pesan tersebut memerlukan perhatian atau tindakan.

Jenis laporan kedua adalah laporan kepatuhan. Laporan kepatuhan dapat memantau tingkat sumber daya atau berbagai kontrol yang berlaku.

AWS Backup Audit Manager mengirimkan laporan harian ke bucket Amazon S3 Anda. Jika laporan untuk wilayah saat ini dan akun saat ini, Anda dapat memilih untuk menerima laporan dalam format CSV atau JSON. Jika tidak, laporan tersedia dalam format CSV. Waktu laporan harian mungkin berfluktuasi selama beberapa jam karena AWS Backup Audit Manager melakukan pengacakan untuk mempertahankan kinerjanya. Anda juga dapat menjalankan laporan sesuai permintaan kapan saja.

Semua pemegang akun dapat membuat laporan lintas wilayah; manajemen dan pemegang akun administrator yang didelegasikan juga dapat membuat laporan lintas akun.

Anda dapat memiliki maksimal 20 rencana laporan per Akun AWS.

> **Note**
>
> Sumber daya seperti RDS yang tidak memiliki kemampuan untuk menunjukkan byte tambahan data dari cadangan tertentu akan menampilkan nilai `backupSizeInBytes` sebagai 0.

Untuk memungkinkan AWS Backup Audit Manager membuat laporan harian atau sesuai permintaan, Anda harus terlebih dahulu membuat rencana laporan dari templat laporan.

Topik

- Memilih template laporan Anda
- Membuat rencana laporan menggunakan AWS Backup konsol
- Membuat rencana laporan menggunakan AWS Backup API
- Membuat laporan sesuai permintaan
- Melihat laporan audit
- Memperbarui rencana laporan

- Menghapus rencana laporan

Memilih template laporan Anda

Template laporan mendefinisikan informasi yang disertakan dalam rencana laporan Anda dalam laporan Anda. Saat Anda mengotomatiskan laporan menggunakan rencana laporan, AWS Backup Audit Manager memberi Anda laporan selama 24 jam sebelumnya. AWS Backup Audit Manager membuat laporan ini antara jam 1 dan 5 pagi UTC. Ini menawarkan template laporan berikut.

Templat laporan cadangan

Templat laporan cadangan. Template ini memberi Anda pembaruan harian tentang pencadangan, pemulihan, atau penyalinan pekerjaan Anda. Anda dapat menggunakan laporan ini untuk memantau postur operasional Anda dan mengidentifikasi kegagalan yang mungkin memerlukan tindakan lebih lanjut. Tabel berikut mencantumkan setiap nama template laporan cadangan dan keluaran sampelnya.

Templat laporan cadangan	Contoh laporan dalam format 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",

Templat laporan cadangan	Contoh laporan dalam format 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"
    }
  ]
}
```

Templat laporan cadangan	Contoh laporan dalam format 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"
	    }

Templat laporan cadangan	Contoh laporan dalam format 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>

Templat laporan kepatuhan

Templat laporan kepatuhan memberi Anda laporan harian tentang kepatuhan aktivitas pencadangan dan sumber daya terhadap kontrol yang Anda tetapkan dalam satu atau beberapa kerangka kerja. Jika status kepatuhan salah satu kerangka kerja Anda adalah`Non-compliant`, tinjau laporan kepatuhan untuk mengidentifikasi sumber daya yang tidak sesuai.

Jenis templat laporan kepatuhan

- `Control compliance report`membantu Anda melacak status kepatuhan kontrol yang telah Anda tetapkan dalam kerangka kerja Anda.
- `Resource compliance report`membantu Anda melacak status kepatuhan sumber daya Anda terhadap kontrol yang Anda tetapkan dalam kerangka kerja Anda. Laporan ini mencakup hasil evaluasi terperinci, termasuk mengidentifikasi informasi tentang sumber daya yang tidak sesuai yang dapat Anda gunakan untuk mengidentifikasi dan memperbaiki sumber daya tersebut.

Tabel berikut menunjukkan contoh keluaran dari laporan kepatuhan.

Templat laporan kepatuhan	Contoh laporan dalam format JSON

CONTROL_COMPLIANCE_REPORT	{
	  "reportItems": [
	    {
	      "accountId": "112233445566",
	      "region": "me-south-1",
	      "frameworkName": "TestFram
	ework7",
	      "frameworkDescription": "A test
	 framework",
	      "controlName": "BACKUP_R
	ESOURCES_PROTECTED_BY_BACKUP_PLAN",
	      "controlComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-08-
	17T03:21:56.002Z",
	      "numResourcesCompliant": 91,
	      "numResourcesNonCompliant":
	 205,
	      "controlFrequency": "Twelve_H
	ours",
	      "controlScope": "",
	      "controlParameters": ""
	    },
	    {
	      "accountId": "112233445566",
	      "region": "me-south-1",
	      "frameworkName": "TestFram
	ework7",

Templat laporan kepatuhan	Contoh laporan dalam format 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
\"}"
    }
  ]
}
```

Templat laporan kepatuhan	Contoh laporan dalam format 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"
	    }
	  ]
	}

Membuat rencana laporan menggunakan AWS Backup konsol

Ada dua jenis laporan. Salah satu jenisnya adalah laporan pekerjaan, yang menunjukkan pekerjaan selesai dalam 24 jam terakhir dan semua pekerjaan aktif. Jenis laporan kedua adalah laporan kepatuhan. Laporan kepatuhan dapat memantau tingkat sumber daya atau berbagai kontrol yang berlaku. Saat membuat laporan, Anda memilih jenis laporan yang akan dibuat.

CATATAN: Tergantung pada jenis akun Anda, tampilan konsol dapat bervariasi. Hanya akun manajemen yang akan melihat fungsionalitas multi-akun.

Mirip dengan paket cadangan, Anda membuat rencana laporan untuk mengotomatiskan pembuatan laporan Anda dan menentukan bucket Amazon S3 tujuan mereka. Rencana laporan mengharuskan Anda memiliki bucket S3 untuk menerima laporan Anda. Untuk petunjuk cara menyiapkan bucket S3 baru, lihat Langkah 1: Membuat bucket S3 pertama Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk membuat rencana laporan Anda di AWS Backup konsol

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Laporan.
3. Pilih Buat rencana laporan.
4. Pilih salah satu template laporan dari daftar dropdown.
5. Masukkan nama paket Laporan yang unik. Nama harus antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).
6. (Opsional) Masukkan deskripsi rencana Laporan.
7. Template laporan kepatuhan hanya untuk satu akun. Pilih satu atau beberapa kerangka kerja yang akan dilaporkan. Anda dapat menambahkan maksimum 1.000 kerangka kerja ke rencana laporan.

    1. Pilih AWS Wilayah Anda menggunakan dropdown.
    2. Pilih kerangka kerja dari Wilayah itu menggunakan dropdown.
    3. Pilih Tambahkan kerangka kerja.
8. (Opsional) Untuk menambahkan tag ke rencana laporan Anda, pilih Tambahkan tag ke rencana laporan.
9. Jika Anda menggunakan akun manajemen, Anda dapat menentukan akun mana yang ingin Anda sertakan dalam rencana laporan ini. Anda dapat memilih Hanya akun saya, yang akan menghasilkan laporan hanya pada akun yang saat ini Anda masuki. Atau, Anda dapat memilih

Satu atau beberapa akun di organisasi saya (tersedia untuk manajemen dan akun administrator yang didelegasikan).

10. (Jika Anda membuat laporan kepatuhan hanya untuk satu Wilayah, lewati langkah ini). Anda dapat memilih Wilayah mana yang akan disertakan dalam laporan Anda. Klik menu tarik-turun untuk menampilkan Wilayah yang tersedia untuk Anda. Pilih Semua Wilayah yang tersedia atau Wilayah yang Anda inginkan.

    - Kotak centang Sertakan Wilayah baru saat dimasukkan ke dalam Backup Audit Manager akan memicu Wilayah baru untuk disertakan dalam laporan Anda saat tersedia.

11. Pilih format File laporan Anda. Semua laporan dapat diekspor dalam format CSV. Selain itu, laporan untuk satu wilayah dan satu Wilayah dapat diekspor dalam format JSON.
12. Pilih nama bucket S3 Anda menggunakan daftar dropdown.
13. (Opsional) Masukkan awalan bucket.

    AWS Backup mengirimkan akun Anda saat ini, laporan Wilayah saat ini kes3://*your-bucket-name*/prefix/Backup/*accountID*/*Region*/year/month/day/report-name.

    AWS Backup mengirimkan laporan lintas akun Anda ke `s3://`*`your-bucket-name`*`/prefix/Backup/crossaccount/`*`Region`*`/year/month/day/report-name`

    AWS Backup mengirimkan laporan Lintas wilayah Anda ke `s3://`*`your-bucket-name`*`/prefix/Backup/`*`accountID`*`/crossregion/year/month/day/report-name`
14. Pilih Buat rencana laporan.

Selanjutnya, Anda harus mengizinkan bucket S3 Anda untuk menerima laporan dari AWS Backup. Setelah Anda membuat rencana laporan, AWS Backup Audit Manager secara otomatis membuat kebijakan akses bucket S3 untuk Anda terapkan.

Jika Anda mengenkripsi bucket menggunakan kunci KMS kustom, kebijakan kunci KMS harus memenuhi persyaratan berikut:

- `Principal`Atribut harus menyertakan `AWSServiceRolePolicyForBackupReports`ARN peran terkait layanan Backup Audit Manager.

- `Action`Atribut harus menyertakan `kms:GenerateDataKey` dan `kms:Decrypt` minimal.

Kebijakan ini AWSServiceRolePolicyForBackupReportsmemiliki izin ini.

Untuk melihat dan menerapkan kebijakan akses ini ke bucket S3 Anda

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Laporan.
3. Di bawah nama rencana laporan, pilih rencana laporan dengan memilih namanya.
4. Pilih Edit.
5. Pilih Lihat kebijakan akses untuk bucket S3. Anda juga dapat menggunakan kebijakan di akhir prosedur ini.
6. Pilih Salin izin.
7. Pilih Edit kebijakan bucket. Perhatikan bahwa hingga laporan cadangan dibuat pertama kali, peran terkait layanan yang dirujuk dalam kebijakan bucket S3 belum akan ada, yang mengakibatkan kesalahan “Prinsipal tidak valid”.
8. Salin izin ke Kebijakan.

Contoh kebijakan bucket

```
{
  "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"
        }
      }
    }
  ]
}
```

Jika Anda menggunakan kustom AWS Key Management Service untuk mengenkripsi bucket S3 target yang menyimpan laporan, sertakan tindakan berikut dalam kebijakan Anda:

```
"Action":[
  "kms:GenerateDataKey",
  "kms:Encrypt"
],
"Resource":[
  "*"
],
```

Membuat rencana laporan menggunakan AWS Backup API

Anda juga dapat bekerja dengan rencana laporan secara terprogram.

Ada dua jenis laporan. Salah satu jenisnya adalah laporan pekerjaan, yang menunjukkan pekerjaan selesai dalam 24 jam terakhir dan semua pekerjaan aktif. Jenis laporan kedua adalah laporan kepatuhan. Laporan kepatuhan dapat memantau tingkat sumber daya atau berbagai kontrol yang berlaku. Saat membuat laporan, Anda memilih jenis laporan yang akan dibuat.

Mirip dengan paket cadangan, Anda membuat rencana laporan untuk mengotomatiskan pembuatan laporan Anda dan menentukan bucket Amazon S3 tujuan mereka. Rencana laporan mengharuskan Anda memiliki bucket S3 untuk menerima laporan Anda. Untuk petunjuk cara menyiapkan bucket S3 baru, lihat Langkah 1: Membuat bucket S3 pertama Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Jika Anda mengenkripsi bucket menggunakan kunci KMS kustom, kebijakan kunci KMS harus memenuhi persyaratan berikut:

- `Principal`Atribut harus menyertakan `AWSServiceRolePolicyForBackupReports`ARN peran terkait layanan Backup Audit Manager.

- `Action`Atribut harus menyertakan `kms:GenerateDataKey` dan `kms:Decrypt` minimal.

Kebijakan ini AWSServiceRolePolicyForBackupReportsmemiliki izin ini.

Untuk laporan single-account, Single-region, gunakan sintaks berikut untuk memanggil. 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"
}
```

Saat Anda menelepon DescribeReportPlan dengan nama unik rencana laporan, AWS Backup API merespons dengan informasi berikut.

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

Untuk laporan multi-akun, Multi-wilayah, gunakan sintaks berikut untuk menelepon. 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"
   }
}
```

Saat Anda menelepon DescribeReportPlan dengan nama unik paket laporan, AWS Backup API merespons dengan informasi berikut untuk paket multi-akun dan Multi-wilayah:

```
{
   "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"
         }
      }
}
```

Membuat laporan sesuai permintaan

Anda dapat membuat laporan baru sesuai keinginan Anda dengan membuat laporan sesuai permintaan dengan langkah-langkah berikut. AWS Backup Audit Manager mengirimkan laporan sesuai permintaan Anda ke bucket Amazon S3 yang Anda tentukan dalam paket laporan.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Laporan.
3. Di bawah nama rencana laporan, pilih rencana laporan dengan memilih namanya.
4. Pilih Buat laporan sesuai permintaan.

Anda dapat membuat laporan sesuai permintaan untuk rencana laporan yang ada.

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Laporan.
3. Di bawah Laporan rencana, pilih rencana laporan dengan mengklik tombol radio di sebelah nama rencana laporan.
4. Klik Tindakan, lalu klik Buat laporan sesuai permintaan.

Anda dapat melakukan ini untuk beberapa laporan, bahkan saat laporan sedang dibuat.

Melihat laporan audit

Anda dapat membuka, melihat, dan menganalisis laporan AWS Backup Audit Manager menggunakan program yang biasa Anda gunakan untuk bekerja dengan file CSV atau JSON. Perhatikan bahwa laporan untuk beberapa wilayah atau beberapa akun hanya tersedia dalam format CSV.

File besar dipecah menjadi beberapa laporan jika ukuran file total melebihi 50 MB. Jika file yang dihasilkan lebih dari 50 MB, AWS Backup Audit Manager akan membuat file CSV tambahan dengan sisa laporan.

Untuk melihat laporan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Laporan.
3. Di bawah nama rencana laporan, pilih rencana laporan dengan memilih namanya.
4. Di bawah Laporkan pekerjaan, klik tautan laporan untuk melihat laporan.
5. Jika status Laporan laporan Anda memiliki garis bawah bertitik, pilih untuk informasi tentang laporan Anda.
6. Pilih laporan mana yang akan dilihat berdasarkan waktu Penyelesaiannya.
7. Pilih tautan S3. Ini membuka bucket S3 tujuan Anda.
8. Di bawah Nama, pilih nama laporan yang ingin Anda lihat.
9. Untuk menyimpan laporan ke komputer Anda, pilih Unduh.

Memperbarui rencana laporan

Anda dapat memperbarui deskripsi rencana laporan yang ada, tujuan pengirimannya, dan formatnya. Jika berlaku, Anda juga dapat menambahkan atau menghapus kerangka kerja dari rencana laporan.

Untuk memperbarui rencana laporan yang ada

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Laporan.
3. Di bawah nama rencana laporan, pilih rencana laporan dengan memilih namanya.
4. Pilih Edit.
5. Anda dapat mengedit detail rencana laporan, termasuk nama dan deskripsi laporan, serta akun dan Wilayah mana yang disertakan dalam laporan.

Menghapus rencana laporan

Anda dapat menghapus rencana laporan yang ada. Saat Anda menghapus paket laporan, laporan apa pun yang sudah dibuat oleh rencana laporan tersebut akan tetap berada di bucket Amazon S3 tujuan mereka.

Untuk menghapus rencana laporan yang ada

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi kiri, pilih Laporan.
3. Di bawah nama rencana laporan, pilih rencana laporan dengan memilih namanya.
4. Pilih Hapus.
5. Masukkan nama rencana laporan Anda, lalu pilih Hapus rencana laporan.

Menggunakan AWS Backup Audit Manager dengan AWS CloudFormation

Kami menyediakan contoh AWS CloudFormation template berikut untuk referensi Anda:

Topik

- Aktifkan pelacakan sumber daya
- Menyebarkan kontrol default
- Bebaskan peran IAM dari evaluasi kontrol
- Buat rencana laporan

Aktifkan pelacakan sumber daya

Template berikut mengaktifkan pelacakan sumber daya seperti yang dijelaskan dalam Menghidupkan pelacakan sumber daya.

```
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
```

Menyebarkan kontrol default

Template berikut membuat kerangka kerja dengan kontrol default yang dijelaskan dalam kontrol dan remediasi 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
```

Bebaskan peran IAM dari evaluasi kontrol

Kontrol BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED memungkinkan Anda untuk mengecualikan hingga lima peran IAM yang masih dapat menghapus titik pemulihan secara manual. Template berikut menerapkan kontrol ini dan juga mengecualikan dua peran 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
```

Buat rencana laporan

Template berikut membuat rencana laporan.

```
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
```

Menggunakan AWS Backup Audit Manager dengan AWS Audit Manager

AWS Backup Audit Manager mengontrol peta ke kontrol standar bawaan AWS Audit Manager, memungkinkan Anda mengimpor temuan kepatuhan AWS Backup Audit Manager ke AWS Audit Manager laporan Anda. Anda mungkin ingin melakukannya untuk membantu petugas kepatuhan, manajer audit, atau kolega lain yang melaporkan aktivitas cadangan sebagai bagian dari postur kepatuhan organisasi Anda secara keseluruhan.

Anda dapat mengimpor hasil kepatuhan kontrol AWS Backup Audit Manager ke AWS Audit Manager kerangka kerja Anda. AWS Audit Manager Agar dapat mengumpulkan data secara otomatis dari kontrol AWS Backup Audit Manager Anda, buat kontrol khusus AWS Audit Manager menggunakan petunjuk untuk Menyesuaikan kontrol yang ada di Panduan AWS Audit Manager Pengguna. Saat Anda mengikuti instruksi tersebut, perhatikan bahwa sumber data untuk AWS Backup kontrol adalah AWS Config.

Untuk daftar AWS Backup kontrol, lihat Memilih kontrol Anda.

Kontrol dan remediasi

Halaman ini mencantumkan kontrol yang tersedia untuk AWS Backup Audit Manager. Anda dapat memilih panel info yang tepat untuk melihat daftar kontrol dan melompat ke kontrol tertentu. Untuk membandingkan kontrol dengan cepat, lihat tabel di Memilih kontrol Anda. Untuk mendefinisikan kontrol secara terprogram, lihat cuplikan kode di Membuat kerangka kerja menggunakan API. AWS Backup

Anda dapat menggunakan hingga 50 kontrol per akun per Wilayah. Menggunakan kontrol yang sama dalam dua kerangka kerja yang berbeda dihitung sebagai menggunakan dua kontrol dari batas kontrol 50.

Halaman ini mencantumkan setiap kontrol dengan informasi berikut:

- Deskripsi. Nilai dalam tanda kurung (“[]”) adalah nilai parameter default.
- Sumber daya yang dievaluasi oleh kontrol.
- Parameter kontrol.

- Kesempatan ketika menjalankan kontrol terjadi.
- Ruang lingkup kontrol, sebagai berikut:
  - Anda dapat menentukan Sumber Daya berdasarkan jenis dengan memilih satu atau beberapa layanan yang AWS Backup didukung.
  - Anda menentukan cakupan sumber daya Tagged dengan kunci tag tunggal dan nilai opsional.
  - Anda dapat menentukan sumber daya tunggal menggunakan daftar dropdown sumber daya tunggal.
- Langkah-langkah remediasi untuk membawa sumber daya yang berlaku ke dalam kepatuhan.

Perhatikan bahwa hanya sumber daya aktif yang akan disertakan saat kontrol mengevaluasi sumber daya untuk kepatuhan. Misalnya, instans Amazon EC2 dalam status berjalan akan dievaluasi oleh kontrol Titik pemulihan terakhir dibuat. Instans EC2 dalam keadaan berhenti tidak akan dimasukkan dalam evaluasi kepatuhan.

Sumber daya cadangan dilindungi oleh rencana cadangan

Deskripsi: Mengevaluasi jika sumber daya dilindungi oleh rencana cadangan.

Sumber daya: `AWS Backup: backup selection`

Parameter: Tidak ada

Terjadi: Secara otomatis setiap 24 jam

Cakupan:

- Sumber daya yang ditandai
- Sumber daya berdasarkan jenis (default)
- Sumber daya tunggal

Remediasi: Tetapkan sumber daya ke rencana cadangan. AWS Backup secara otomatis melindungi sumber daya Anda setelah Anda menetapkannya ke paket cadangan. Untuk informasi selengkapnya, lihat Menetapkan sumber daya ke paket cadangan.

Paket Backup frekuensi minimum dan retensi minimum

Deskripsi: Mengevaluasi jika rencana cadangan berisi setidaknya satu aturan cadangan yang frekuensi cadangannya setidaknya [1 hari] dan periode retensi setidaknya [35 hari].

Sumber daya: `AWS Backup: backup plans`

Parameter:

- Frekuensi cadangan yang diperlukan dalam jumlah jam atau hari.
- Periode retensi yang diperlukan dalam jumlah hari, minggu, bulan, atau tahun. Kami merekomendasikan retensi penyimpanan hangat setidaknya satu minggu untuk memungkinkan AWS Backup untuk mengambil cadangan tambahan jika memungkinkan, menghindari biaya tambahan.

Terjadi: Perubahan konfigurasi

Cakupan:

- Sumber daya yang ditandai
- Sumber daya tunggal

Remediasi: Perbarui rencana cadangan untuk mengubah frekuensi cadangan, periode retensi, atau keduanya. Memperbarui paket cadangan Anda mengubah periode retensi untuk titik pemulihan yang dibuat paket setelah pembaruan Anda.

Vaults mencegah penghapusan manual titik pemulihan

Deskripsi: Mengevaluasi jika brankas cadangan tidak mengizinkan penghapusan titik pemulihan secara manual kecuali oleh peran IAM tertentu.

Sumber daya: `AWS Backup: backup vaults`

Parameter: Nama Sumber Daya Amazon (ARN) hingga lima peran IAM diizinkan untuk menghapus titik pemulihan secara manual.

Terjadi: Perubahan konfigurasi

Cakupan:

- Sumber daya yang ditandai
- Sumber daya tunggal

Remediasi: Membuat atau mengubah kebijakan akses berbasis sumber daya pada brankas cadangan. Untuk contoh kebijakan dan petunjuk tentang cara menyetel kebijakan akses vault cadangan, lihat Menolak akses untuk menghapus titik pemulihan di brankas cadangan.

Poin pemulihan dienkripsi

Deskripsi: Mengevaluasi jika titik pemulihan dienkripsi.

Sumber daya: `AWS Backup: recovery points`

Parameter: Tidak ada

Terjadi: Perubahan konfigurasi

Cakupan:

- Sumber daya yang ditandai

Remediasi: Konfigurasikan enkripsi untuk titik pemulihan. Cara Anda mengkonfigurasi enkripsi untuk titik AWS Backup pemulihan berbeda tergantung pada jenis sumber daya.

Anda dapat mengonfigurasi enkripsi untuk jenis sumber daya yang mendukung AWS Backup pengelolaan penuh dalam penggunaan AWS Backup. Jika jenis sumber daya tidak mendukung AWS Backup pengelolaan penuh, Anda harus mengonfigurasi enkripsi cadangannya dengan mengikuti petunjuk layanan tersebut, seperti enkripsi Amazon EBS di Panduan Pengguna Amazon Elastic Compute Cloud. Untuk melihat daftar jenis sumber daya yang mendukung AWS Backup manajemen penuh, lihat bagian “ AWS Backup Manajemen penuh” pada Ketersediaan fitur berdasarkan sumber daya tabel.

Retensi minimum ditetapkan untuk titik pemulihan

Deskripsi: Mengevaluasi jika periode retensi titik pemulihan setidaknya [35 hari].

Sumber daya: `AWS Backup: recovery points`

Parameter: Diperlukan periode retensi titik pemulihan dalam jumlah hari, minggu, bulan, atau tahun. Kami merekomendasikan retensi penyimpanan hangat setidaknya satu minggu untuk memungkinkan AWS Backup untuk mengambil cadangan tambahan jika memungkinkan, menghindari biaya tambahan.

Terjadi: Perubahan konfigurasi

Cakupan:

- Sumber daya yang ditandai

Remediasi: Ubah periode retensi titik pemulihan Anda. Untuk informasi selengkapnya, lihat Mengedit cadangan.

Salinan cadangan Lintas Wilayah dijadwalkan

Deskripsi: Mengevaluasi jika sumber daya dikonfigurasi untuk membuat salinan cadangannya ke Wilayah lain. AWS

Sumber daya: `AWS Backup: backup selection`

Parameter:

- Pilih Wilayah AWS(s) di mana salinan cadangan harus ada (Opsional)
- Wilayah

Terjadi: Secara otomatis setiap 24 jam

Cakupan:

- Sumber daya yang ditandai
- Sumber daya berdasarkan jenis
- Sumber daya tunggal

Remediasi: Perbarui rencana cadangan untuk mengubah Wilayah AWS tempat salinan cadangan seharusnya ada.

Salinan cadangan lintas akun dijadwalkan

Deskripsi: Mengevaluasi jika sumber daya dikonfigurasi untuk membuat salinan cadangannya ke akun lain. Anda dapat menambahkan hingga 5 akun untuk dievaluasi oleh kontrol. Akun tujuan harus berada di organisasi yang sama dengan akun sumber di AWS Organizations.

Sumber daya: `AWS Backup: backup selection`

Parameter:

- Pilih ID AWS akun tempat salinan cadangan harus ada (Opsional)
- account-id

Terjadi: Secara otomatis setiap 24 jam

Cakupan:

- Sumber daya yang ditandai
- Sumber daya berdasarkan jenis
- Sumber daya tunggal

Remediasi: Perbarui rencana cadangan untuk mengubah atau menambahkan ID AWS akun di mana salinan seharusnya ada.

Cadangan dilindungi oleh AWS Backup Vault Lock

Deskripsi: Mengevaluasi jika sumber daya memiliki cadangan yang tidak dapat diubah yang disimpan di brankas cadangan yang terkunci.

Sumber daya: `AWS Backup: backup selection`

Parameter:

- Masukkan hari retensi minimum dan maksimum untuk AWS Backup Vault Lock (opsional)
- Hari retensi minimum
- Hari retensi maksimum

Terjadi: Secara otomatis setiap 24 jam

Cakupan:

- Sumber daya yang ditandai
- Sumber daya berdasarkan jenis
- Sumber daya tunggal

Remediasi: Kunci brankas cadangan untuk menyetel namanya, ubah hari retensi minimum, hari retensi maksimum, atau keduanya. Dapat juga menyertakan `ChangeableForDays` kunci brankas dalam mode kepatuhan.

Titik pemulihan terakhir dibuat

Deskripsi: Kontrol ini mengevaluasi apakah titik pemulihan telah dibuat dalam jangka waktu yang ditentukan (dalam hari atau jam).

Kontrol sesuai jika sumber daya memiliki titik pemulihan yang dibuat dalam jangka waktu yang ditentukan. Kontrol tidak sesuai jika titik pemulihan tidak dibuat dalam jumlah hari atau jam yang ditentukan.

Sumber daya: `AWS Backup: recovery points`

Parameter:

- Masukkan kerangka waktu yang ditentukan dalam bilangan bulat, baik dalam jam atau hari.
- Nilai `hours` dapat berkisar dari 1 hingga`744`.
- Nilai `days` dapat berkisar dari 1 ke`31`.

Terjadi: Secara otomatis setiap 24 jam

Cakupan:

- Sumber daya yang ditandai
- Sumber daya berdasarkan jenis
- Sumber daya tunggal

Remediasi:

- Perbarui rencana cadangan untuk mengubah kerangka waktu pembuatan titik pemulihan yang ditentukan.
- Selain itu, Anda dapat membuat cadangan sesuai permintaan.

Mengembalikan waktu untuk sumber daya memenuhi target

Deskripsi: Mengevaluasi jika memulihkan sumber daya yang dilindungi selesai dalam waktu pemulihan target.

Kontrol ini memeriksa apakah waktu pemulihan sumber daya tertentu memenuhi durasi target. Aturannya adalah NON_COMPLIANT jika `LatestRestoreExecutionTimeMinutes` jenis sumber daya lebih besar dari `maxRestoreTime` dalam hitungan menit.

Parameter:

- `maxRestoreTime`(dalam hitungan menit)

Terjadi: Secara otomatis setiap 24 jam

Cakupan:

- Sumber daya yang ditandai
- Sumber daya berdasarkan jenis
- Sumber daya tunggal

> **Note**
>
> AWS Backup tidak menyediakan perjanjian tingkat layanan (SLA) apa pun untuk waktu pemulihan. Waktu pemulihan dapat bervariasi berdasarkan beban dan kapasitas sistem, bahkan untuk pemulihan yang mengandung sumber daya yang sama.

Mengelola AWS Backup sumber daya di beberapa Akun AWS

> **Note**
>
> Sebelum Anda mengelola sumber daya Akun AWS di beberapa akun AWS Backup, akun Anda harus milik organisasi yang sama dalam AWS Organizations layanan.

Anda dapat menggunakan fitur manajemen lintas akun AWS Backup untuk mengelola dan memantau pencadangan, pemulihan, dan penyalinan pekerjaan Akun AWS yang Anda konfigurasikan AWS Organizations. AWS Organizationsadalah layanan yang menawarkan manajemen berbasis kebijakan untuk beberapa Akun AWS dari satu akun manajemen. Ini memungkinkan Anda untuk membakukan cara Anda menerapkan kebijakan cadangan, meminimalkan kesalahan manual dan upaya secara bersamaan. Dari tampilan pusat, Anda dapat dengan mudah mengidentifikasi sumber daya di semua akun yang memenuhi kriteria yang Anda minati.

Jika Anda mengatur AWS Organizations, Anda dapat mengonfigurasi AWS Backup untuk memantau aktivitas di semua akun Anda di satu tempat. Anda juga dapat membuat kebijakan cadangan dan menerapkannya ke akun terpilih yang merupakan bagian dari organisasi Anda dan melihat aktivitas pekerjaan pencadangan agregat langsung dari AWS Backup konsol. Fungsi ini memungkinkan administrator cadangan untuk secara efektif memantau status pekerjaan cadangan di ratusan akun di seluruh perusahaan mereka dari satu akun manajemen. AWS Organizations kuota berlaku.

Misalnya, Anda menentukan kebijakan cadangan A yang mengambil cadangan harian sumber daya tertentu dan menyimpannya selama 7 hari. Anda memilih untuk menerapkan kebijakan cadangan A ke seluruh organisasi. (Ini berarti bahwa setiap akun dalam organisasi mendapatkan kebijakan cadangan itu, yang membuat rencana cadangan terkait yang terlihat di akun itu.) Kemudian, Anda membuat OU bernama Finance, dan Anda memutuskan untuk menyimpan cadangannya hanya selama 30 hari. Dalam hal ini, Anda menentukan kebijakan cadangan B, yang mengesampingkan nilai siklus hidup, dan melampirkannya ke OU Keuangan tersebut. Ini berarti bahwa semua akun di bawah Finance OU mendapatkan rencana cadangan efektif baru yang mengambil cadangan harian dari semua sumber daya yang ditentukan dan menyimpannya selama 30 hari.

Dalam contoh ini, kebijakan cadangan A dan kebijakan cadangan B digabungkan menjadi kebijakan cadangan tunggal, yang mendefinisikan strategi perlindungan untuk semua akun di bawah OU bernama Finance. Semua akun lain dalam organisasi tetap dilindungi oleh kebijakan cadangan A.

Penggabungan dilakukan hanya untuk kebijakan cadangan yang berbagi nama paket cadangan yang sama. Anda juga dapat memiliki kebijakan A dan kebijakan B yang hidup berdampingan di akun itu tanpa penggabungan apa pun. Anda dapat menggunakan operator penggabungan lanjutan di tampilan JSON konsol saja. Untuk detail tentang penggabungan kebijakan, lihat Mendefinisikan kebijakan, sintaks kebijakan, dan pewarisan kebijakan di Panduan AWS Organizations Pengguna. Untuk referensi tambahan dan kasus penggunaan, lihat blog Mengelola cadangan dalam skala besar dalam AWS Organizations penggunaan Anda AWS Backup dan tutorial video Mengelola cadangan dalam skala yang Anda gunakan. AWS Organizations AWS Backup

Silakan lihat Ketersediaan fitur menurut AWS Wilayah untuk melihat di mana fitur manajemen lintas akun tersedia.

Untuk menggunakan manajemen lintas akun, Anda harus mengikuti langkah-langkah ini:

1. Buat akun manajemen AWS Organizations dan tambahkan akun di bawah akun manajemen.
2. Aktifkan fitur manajemen lintas akun di AWS Backup.
3. Buat kebijakan cadangan untuk diterapkan ke semua yang ada Akun AWS di akun manajemen Anda.

   > **Note**
   >
   > Untuk paket cadangan yang dikelola oleh Organizations, pengaturan keikutsertaan sumber daya di akun manajemen akan mengganti pengaturan di akun anggota, meskipun satu atau beberapa akun administrator yang didelegasikan dikonfigurasi. Akun administrator yang didelegasikan adalah akun anggota dengan fitur yang disempurnakan dan tidak dapat mengganti pengaturan seperti akun manajemen.

4. Kelola pencadangan, pemulihan, dan salin pekerjaan di semua pekerjaan Anda Akun AWS.

Topik

- Membuat akun manajemen di Organizations
- Mengaktifkan manajemen lintas akun
- Administrator yang didelegasikan
- Membuat kebijakan backup
- Memantau aktivitas dalam berbagai Akun AWS

- Aturan keikutsertaan sumber daya
- Mendefinisikan kebijakan, sintaks kebijakan, dan pewarisan kebijakan

Membuat akun manajemen di Organizations

Pertama, Anda harus membuat organisasi Anda dan mengonfigurasinya dengan akun AWS anggota di AWS Organizations.

Untuk membuat akun manajemen AWS Organizations dan menambahkan akun

- Untuk petunjuk, lihat Tutorial: Membuat dan mengonfigurasi organisasi di Panduan AWS Organizations Pengguna.

Mengaktifkan manajemen lintas akun

Sebelum Anda dapat menggunakan manajemen lintas akun AWS Backup, Anda harus mengaktifkan fitur (yaitu, ikut serta). Setelah fitur diaktifkan, Anda dapat membuat kebijakan cadangan yang memungkinkan Anda mengotomatiskan pengelolaan beberapa akun secara simultan.

Untuk mengaktifkan manajemen lintas akun

1. Buka Konsol AWS Backup di https://console.aws.amazon.com/backup/. Anda harus masuk menggunakan kredensi akun manajemen Anda.
2. Di panel navigasi kiri, pilih Pengaturan untuk membuka halaman manajemen lintas akun.
3. Di bagian Kebijakan cadangan, pilih Aktifkan.

   Ini memberi Anda akses ke semua akun dan memungkinkan Anda membuat kebijakan yang mengotomatiskan pengelolaan beberapa akun di organisasi Anda secara bersamaan.
4. Di bagian Pemantauan lintas akun, pilih Aktifkan.

   Ini memungkinkan Anda untuk memantau aktivitas pencadangan, penyalinan, dan pemulihan semua akun di organisasi Anda dari akun manajemen Anda.

Administrator yang didelegasikan

Administrasi yang didelegasikan menyediakan cara yang nyaman bagi pengguna yang ditugaskan di akun anggota terdaftar untuk melakukan sebagian besar tugas AWS Backup administratif. Anda dapat memilih untuk mendelegasikan administrasi AWS Backup ke akun anggota AWS Organizations, sehingga memperluas kemampuan untuk mengelola AWS Backup dari luar akun manajemen dan di seluruh organisasi.

Akun manajemen, secara default, adalah akun yang digunakan untuk mengedit dan mengelola kebijakan. Dengan menggunakan fitur administrator yang didelegasikan, Anda dapat mendelegasikan fungsi manajemen ini ke akun anggota yang Anda tentukan. Pada gilirannya, akun tersebut dapat mengelola kebijakan, selain akun manajemen.

Setelah akun anggota berhasil didaftarkan untuk administrasi yang didelegasikan, itu adalah akun administrator yang didelegasikan. Perhatikan bahwa akun, bukan pengguna, ditetapkan sebagai administrator yang didelegasikan.

Mengaktifkan akun administrator yang didelegasikan memungkinkan opsi untuk mengelola kebijakan cadangan, meminimalkan jumlah pengguna dengan akses ke akun manajemen, dan memungkinkan pemantauan lintas akun pekerjaan.

Di bawah ini adalah tabel yang menunjukkan fungsi akun manajemen, akun yang didelegasikan sebagai administrator Cadangan, dan akun yang menjadi anggota dalam Organisasi. AWS

> **Note**
>
> Akun administrator yang didelegasikan adalah akun anggota dengan fitur yang disempurnakan tetapi tidak dapat mengganti pengaturan keikutsertaan layanan dari akun anggota lain seperti akun manajemen.

HAK ISTIMEWA	AKUN MANAJEMEN	ADMINISTRATOR TERDELEGASIKAN	AKUN ANGGOTA
Daftarkan/batalkan pendaftaran akun administrator yang didelegasikan	Ya	Tidak	Tidak

HAK ISTIMEWA	AKUN MANAJEMEN	ADMINISTRATOR TERDELEGASIKAN	AKUN ANGGOTA
Mengelola kebijakan pencadangan di seluruh akun di AWS Organizations	Ya	Ya	Tidak
Pantau pekerjaan lintas akun	Ya	Ya	Tidak

Prasyarat

Sebelum Anda dapat mendelegasikan administrasi cadangan, Anda harus terlebih dahulu mendaftarkan setidaknya satu akun anggota di AWS organisasi Anda sebagai administrator yang didelegasikan. Sebelum Anda dapat mendaftarkan akun sebagai administrator yang didelegasikan, Anda harus terlebih dahulu mengkonfigurasi yang berikut:

- AWS Organizations harus diaktifkan dan dikonfigurasi dengan setidaknya satu akun anggota selain akun manajemen default Anda.
- Di AWS Backup konsol, pastikan kebijakan pencadangan, pemantauan lintas akun, dan fitur pencadangan lintas akun diaktifkan. Ini berada di bawah panel Administrator yang didelegasikan di konsol. AWS Backup
  - Pemantauan lintas akun memungkinkan Anda memantau aktivitas pencadangan di semua akun di organisasi Anda dari akun manajemen, serta dari akun administrator yang didelegasikan.
  - Opsional: Pencadangan lintas akun, yang memungkinkan akun di organisasi Anda menyalin cadangan ke akun lain (untuk sumber daya lintas akun yang didukung cadangan).
  - Aktifkan akses layanan dengan AWS Backup.

Ada dua langkah yang terlibat dalam mendirikan administrasi yang didelegasikan. Langkah pertama adalah mendelegasikan pemantauan pekerjaan lintas akun. Langkah kedua adalah mendelegasikan manajemen kebijakan cadangan.

Daftarkan akun anggota sebagai akun administrator yang didelegasikan

Ini adalah bagian pertama: Menggunakan AWS Backup konsol untuk mendaftarkan akun administrator yang didelegasikan untuk memantau pekerjaan lintas akun. Untuk mendelegasikan AWS Backup kebijakan, Anda akan menggunakan konsol Organizations di bagian berikutnya.

Untuk mendaftarkan akun anggota menggunakan AWS Backup Konsol:

1. Buka Konsol AWS Backup di https://console.aws.amazon.com/backup/. Anda harus masuk menggunakan kredensi akun manajemen Anda.
2. Di bawah Akun Saya di navigasi sebelah kiri konsol, pilih Pengaturan.
3. Di panel Administrator yang didelegasikan, klik Daftarkan administrator yang didelegasikan atau Tambahkan administrator yang didelegasikan.
4. Pada halaman Daftarkan administrator yang didelegasikan, pilih akun yang ingin Anda daftarkan, lalu pilih Daftar akun.

Akun yang ditunjuk ini sekarang akan terdaftar sebagai administrator yang didelegasikan, dengan hak administratif untuk memantau pekerjaan di seluruh akun dalam organisasi dan dapat melihat dan mengedit kebijakan (delegasi kebijakan). Akun anggota ini tidak dapat mendaftarkan atau membatalkan pendaftaran akun administrator lain yang didelegasikan. Anda dapat menggunakan konsol untuk mendaftarkan hingga 5 akun sebagai administrator yang didelegasikan.

Untuk mendaftarkan akun anggota menggunakan pemrograman:

Gunakan perintah CLI `register-delegated-administrator`. Anda dapat menentukan parameter berikut dalam permintaan CLI Anda:

- `service-principal`
- `account-id`

Di bawah ini adalah contoh permintaan CLI untuk mendaftarkan akun anggota secara terprogram:

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Membatalkan pendaftaran akun anggota

Gunakan prosedur berikut untuk menghapus akses administratif AWS Backup dengan membatalkan pendaftaran akun anggota di AWS organisasi Anda yang sebelumnya telah ditetapkan sebagai administrator yang didelegasikan.

Untuk membatalkan pendaftaran akun anggota menggunakan Konsol

1. Buka Konsol AWS Backup di https://console.aws.amazon.com/backup/. Anda harus masuk menggunakan kredensi akun manajemen Anda.
2. Di bawah Akun Saya di navigasi sebelah kiri konsol, pilih Pengaturan.
3. Di bagian Administrator yang didelegasikan, klik Deregister account.
4. Pilih akun yang ingin Anda deregister.
5. Di kotak dialog Deregister account, tinjau implikasi keamanan, lalu ketik `confirm` untuk menyelesaikan deregistrasi.
6. Pilih `Deregister account`.

Untuk membatalkan pendaftaran akun anggota menggunakan pemrograman:

Gunakan perintah CLI `deregister-delegated-administrator` untuk membatalkan pendaftaran akun administrator yang didelegasikan. Anda dapat menentukan parameter berikut dalam permintaan API Anda:

- `service-principal`
- `account-id`

Di bawah ini adalah contoh permintaan CLI untuk membatalkan pendaftaran akun anggota secara terprogram:

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Delegasikan AWS Backup kebijakan melalui AWS Organizations

Di dalam AWS Organizations konsol, Anda dapat mendelegasikan administrasi beberapa kebijakan, termasuk kebijakan Backup.

Dari akun manajemen yang masuk ke AWS Organizations konsol, Anda dapat membuat, melihat, atau menghapus kebijakan delegasi berbasis sumber daya untuk organisasi Anda. Untuk langkah-langkah mendelegasikan kebijakan, lihat Membuat kebijakan delegasi berbasis sumber daya di Panduan Pengguna.AWS Organizations

Membuat kebijakan backup

Setelah Anda mengaktifkan manajemen lintas akun, buat kebijakan pencadangan lintas akun dari akun manajemen Anda.

> **Warning**
>
> Saat Anda membuat kebijakan dengan JSON, nama kunci duplikat akan ditolak. Nama setiap kunci harus unik jika beberapa rencana, aturan, atau pilihan disertakan dalam satu kebijakan.

Buat kebijakan pencadangan melalui AWS Backup konsol

1. Di panel navigasi kiri, pilih Kebijakan cadangan. Pada halaman Kebijakan cadangan, pilih Buat kebijakan cadangan.
2. Di bagian Detail, masukkan nama kebijakan cadangan dan berikan deskripsi.
3. Di bagian Rincian rencana cadangan, pilih tab editor visual dan lakukan hal berikut:
   a. Untuk nama paket Backup, masukkan nama.
   b. Untuk Wilayah, pilih Wilayah dari daftar.
4. Di bagian Konfigurasi aturan Backup, pilih Tambahkan aturan cadangan.

   Jumlah maksimum aturan per paket cadangan adalah 10. Jika rencana berisi lebih dari 10 aturan, rencana cadangan akan diabaikan dan tidak ada cadangan yang akan dibuat darinya.

   a. Untuk nama Aturan, masukkan nama untuk aturan. Nama aturan peka huruf besar/kecil dan hanya dapat berisi karakter alfanumerik atau tanda hubung.
   b. Untuk Jadwal, pilih frekuensi cadangan dalam daftar Frekuensi, dan pilih salah satu opsi jendela Backup. Kami menyarankan Anda memilih Gunakan default jendela cadangan — direkomendasikan.
5. Untuk Siklus Hidup, pilih pengaturan siklus hidup yang Anda inginkan.

6. Untuk nama brankas Backup, masukkan nama. Ini adalah brankas cadangan tempat titik pemulihan yang dibuat oleh cadangan Anda akan disimpan.

   Pastikan brankas cadangan ada di semua akun Anda. AWS Backup tidak memeriksa ini.

7. (opsional) Pilih Wilayah tujuan dari daftar jika Anda ingin cadangan Anda disalin ke yang lain Wilayah AWS, dan tambahkan tag. Anda dapat memilih tag untuk titik pemulihan yang dibuat, terlepas dari pengaturan salinan lintas wilayah. Anda juga dapat menambahkan lebih banyak aturan.

8. Di bagian Penugasan sumber daya, berikan nama peran AWS Identity and Access Management (IAM). Untuk menggunakan peran AWS Backup layanan, berikan`service-role/AWSBackupDefaultServiceRole`.

   AWS Backup mengasumsikan peran ini di setiap akun untuk mendapatkan izin untuk melakukan pekerjaan pencadangan dan penyalinan, termasuk izin kunci enkripsi bila berlaku. AWS Backup juga menggunakan peran ini untuk melakukan penghapusan siklus hidup.

   > **Note**
   >
   > AWS Backup tidak memvalidasi bahwa peran itu ada atau jika peran dapat diasumsikan. Untuk rencana cadangan yang dibuat oleh manajemen lintas akun, AWS Backup akan menggunakan pengaturan opt-in dari akun manajemen dan mengganti pengaturan akun tertentu.
   > Untuk setiap akun yang ingin Anda tambahkan kebijakan pencadangan, Anda harus membuat vault dan peran IAM sendiri.

9. Tambahkan tag untuk memilih sumber daya yang ingin Anda cadangkan. Jumlah maksimum tag yang diizinkan adalah 30.

   AWS Organizations policy memungkinkan penetapan maksimum 30 tag jika rencana cadangan dibuat melalui kebijakan Organizations. Tag tambahan dapat disertakan dengan memanfaatkan beberapa tugas sumber daya atau melibatkan beberapa rencana pencadangan.

   Jika jumlah tag melebihi 30 dalam pilihan cadangan yang sama, baik melalui memodifikasi pilihan yang ada atau menggunakan`@@append`, rencana cadangan akan menjadi tidak valid dan akan dihapus dari akun lokal.

10. Di bagian Pengaturan lanjutan, pilih Windows VSS jika sumber daya yang Anda cadangkan menjalankan Microsoft Windows pada instans Amazon EC2. Ini memungkinkan Anda untuk mengambil cadangan Windows VSS yang konsisten dengan aplikasi.

> **Note**
>
> AWS Backup saat ini mendukung pencadangan sumber daya yang konsisten aplikasi yang berjalan di Amazon EC2 saja. Tidak semua jenis instans atau aplikasi didukung untuk cadangan Windows VSS. Untuk informasi selengkapnya, lihat Membuat cadangan Windows VSS.

11. Pilih Tambahkan paket cadangan untuk menambahkannya ke kebijakan, lalu pilih Buat kebijakan cadangan.

    Membuat kebijakan cadangan tidak melindungi sumber daya Anda sampai Anda melampirkannya ke akun. Anda dapat memilih nama kebijakan Anda dan melihat detailnya.

    Berikut ini adalah contoh AWS Organizations kebijakan yang membuat rencana cadangan. Jika Anda mengaktifkan cadangan Windows VSS, Anda harus menambahkan izin yang memungkinkan Anda mengambil cadangan yang konsisten dengan aplikasi seperti yang ditunjukkan di bagian kebijakan. `advanced_backup_settings`

```
{
  "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. Di bagian Target, pilih unit organisasi atau akun yang ingin dilampirkan kebijakan, lalu pilih Lampirkan. Kebijakan ini juga dapat ditambahkan ke unit atau akun organisasi individu.

> **Note**
>
> Pastikan untuk memvalidasi kebijakan Anda dan bahwa Anda menyertakan semua bidang yang diperlukan dalam kebijakan. Jika bagian dari kebijakan tidak valid, AWS Backup abaikan bagian-bagian tersebut, tetapi bagian kebijakan yang valid akan berfungsi seperti yang diharapkan. Saat ini, AWS Backup tidak memvalidasi AWS Organizations kebijakan untuk kebenaran.
> Jika Anda menerapkan satu kebijakan ke akun manajemen dan kebijakan yang berbeda ke akun anggota, dan kebijakan tersebut bertentangan (misalnya, memiliki periode penyimpanan cadangan yang berbeda), kedua kebijakan akan berjalan tanpa masalah (yaitu, kebijakan akan dijalankan secara independen untuk setiap akun). Misalnya, jika kebijakan akun manajemen mencadangkan volume Amazon EBS sekali sehari, dan

kebijakan lokal mencadangkan volume EBS seminggu sekali, kedua kebijakan akan berjalan.
Jika kolom wajib tidak ada dalam kebijakan efektif yang akan diterapkan ke akun (mungkin karena penggabungan antar kebijakan yang berbeda), kebijakan tersebut AWS Backup tidak berlaku sama sekali. Jika beberapa pengaturan tidak valid, AWS Backup sesuaikan.

Terlepas dari pengaturan keikutsertaan di akun anggota dalam rencana cadangan yang dibuat dari kebijakan cadangan, AWS Backup akan menggunakan pengaturan keikutsertaan yang ditentukan dalam akun manajemen organisasi.

Ketika Anda melampirkan kebijakan ke unit organisasi, setiap akun yang bergabung dengan unit organisasi ini mendapatkan kebijakan ini secara otomatis, dan setiap akun yang dihapus dari unit organisasi akan kehilangan kebijakan ini. Paket cadangan yang sesuai dihapus secara otomatis dari akun itu.

Memantau aktivitas dalam berbagai Akun AWS

Untuk memantau pencadangan, menyalin, dan memulihkan pekerjaan di seluruh akun, Anda harus mengaktifkan pemantauan lintas akun. Ini memungkinkan Anda memantau aktivitas pencadangan di semua akun dari akun manajemen organisasi Anda. Setelah Anda ikut serta, semua pekerjaan di seluruh organisasi Anda yang dibuat setelah keikutsertaan akan terlihat. Saat Anda memilih keluar, AWS Backup simpan pekerjaan dalam tampilan agregat selama 30 hari (dari mencapai status terminus). Pekerjaan yang dibuat setelah opt-out tidak terlihat dan tidak menampilkan pekerjaan cadangan yang baru dibuat. Untuk petunjuk keikutsertaan, lihatMengaktifkan manajemen lintas akun.

Untuk memantau beberapa akun

1. Buka Konsol AWS Backup di https://console.aws.amazon.com/backup/. Anda harus masuk menggunakan kredensi akun manajemen Anda.
2. Di panel navigasi kiri, pilih Pengaturan untuk membuka halaman manajemen lintas akun.
3. Di bagian Pemantauan lintas akun, pilih Aktifkan.

   Ini memungkinkan Anda untuk memantau aktivitas pencadangan dan pemulihan semua akun di organisasi Anda dari akun manajemen Anda.
4. Di panel navigasi kiri, pilih Pemantauan lintas akun.

5. Pada halaman pemantauan lintas akun, pilih tab Backup jobs, Restore jobs, atau Copy jobs untuk melihat semua lowongan yang dibuat di semua akun Anda. Anda dapat melihat masing-masing pekerjaan ini dengan Akun AWS ID, dan Anda dapat melihat semua pekerjaan di akun tertentu.
6. Di kotak pencarian, Anda dapat memfilter pekerjaan berdasarkan ID Akun, Status, atau ID Pekerjaan.

   Misalnya, Anda dapat memilih tab Backup jobs dan melihat semua pekerjaan cadangan yang dibuat di semua akun Anda. Anda dapat memfilter daftar berdasarkan ID Akun dan melihat semua pekerjaan cadangan yang dibuat di akun itu.

Aturan keikutsertaan sumber daya

Jika rencana cadangan akun anggota dibuat oleh kebijakan pencadangan tingkat Organisasi, pengaturan AWS Backup keikutsertaan untuk akun manajemen Organizations akan mengganti pengaturan keikutsertaan di akun anggota tersebut, tetapi hanya untuk paket cadangan tersebut.

Jika akun anggota juga memiliki paket cadangan tingkat lokal yang dibuat oleh pengguna, paket cadangan tersebut akan mengikuti pengaturan keikutsertaan di akun anggota, tanpa mengacu pada pengaturan keikutsertaan akun manajemen Organisasi.

Mendefinisikan kebijakan, sintaks kebijakan, dan pewarisan kebijakan

Topik-topik berikut didokumentasikan dalam Panduan AWS Organizations Pengguna.

- Kebijakan Backup — Lihat Kebijakan Backup.
- Sintaks kebijakan — Lihat sintaks kebijakan Backup dan contoh.
- Warisan untuk jenis kebijakan manajemen — Lihat Warisan untuk jenis kebijakan manajemen.

AWS Backup dan AWS CloudFormation

Secara umum

Dengan AWS CloudFormation itu, Anda dapat menyediakan dan mengelola AWS sumber daya Anda dengan cara yang aman dan berulang menggunakan template yang Anda buat. Anda dapat menggunakan AWS CloudFormation template dan StackSets untuk mengelola rencana cadangan, pilihan sumber daya cadangan, dan vault cadangan. Untuk selengkapnya tentang penggunaanAWS CloudFormation, lihat Bagaimana Cara AWS CloudFormation Kerjanya? dalam AWS CloudFormationUser Guide.

Sebelum Anda membuat AWS CloudFormation template Anda atauStackSet, pertimbangkan hal berikut:

- Buat template terpisah untuk paket cadangan dan brankas cadangan Anda. Anda hanya dapat menghapus brankas cadangan yang kosong. Anda tidak dapat menghapus tumpukan yang menyertakan vault cadangan jika berisi titik pemulihan.
- Pastikan Anda memiliki peran layanan yang tersedia sebelum membuat tumpukan Anda. Peran layanan AWS Backup default dibuat untuk Anda saat pertama kali Anda menetapkan sumber daya ke paket pencadangan. Jika Anda belum menetapkan sumber daya ke paket cadangan, lakukan sebelum membuat tumpukan. Anda juga dapat menentukan peran khusus yang Anda buat. Untuk informasi lebih lanjut tentang peran, lihat Peran layanan IAM.

Menerapkan vault cadangan, rencana cadangan, dan penetapan sumber daya menggunakan AWS CloudFormation

Untuk contoh AWS CloudFormation template yang menyebarkan vault cadangan, rencana cadangan, dan penetapan sumber daya, lihat. Menetapkan sumber daya menggunakan AWS CloudFormation

Menyebarkan rencana cadangan menggunakan AWS CloudFormation

Untuk contoh AWS CloudFormation template yang menyebarkan paket cadangan, lihat AWS CloudFormationtemplate untuk paket cadangan.

Menerapkan kerangka kerja AWS Backup Audit Manager dan rencana laporan menggunakan AWS CloudFormation

Untuk contoh AWS CloudFormation template yang menerapkan kerangka kerja AWS Backup Audit Manager dan rencana laporan, lihat AWS CloudFormationtemplate untuk rencana cadangan.

Menerapkan paket cadangan di seluruh akun menggunakan AWS CloudFormation

Anda dapat menggunakan AWS CloudFormation StackSets di beberapa akun di AWS Organisasi. Contoh template tersedia di Panduan AWS CloudFormation Pengguna.

Titik awal dan referensi yang sangat baik adalah publikasi Otomatiskan cadangan terpusat pada skala di seluruh AWS layanan menggunakan AWS Backup. Bersama Ibukun Oyewumi dan Sabith Venkitachalapathy (Juli 2021).

Pelajari lebih lanjut lanjut tentang AWS CloudFormation

Untuk informasi tentang menggunakan AWS CloudFormation denganAWS Backup, lihat Referensi Jenis AWS Backup Sumber Daya di Panduan AWS CloudFormation Pengguna.

Untuk informasi tentang mengontrol akses ke sumber daya AWS layanan saat menggunakanAWS CloudFormation, lihat Mengontrol Akses dengan AWS Identity and Access Management dalam Panduan AWS CloudFormation Pengguna.

Keamanan di AWS Backup

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku AWS Backup, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda untuk AWS Backup mencakup, tetapi tidak terbatas pada, hal-hal berikut. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data, persyaratan perusahaan, serta hukum dan peraturan yang berlaku.
  - Menanggapi komunikasi yang Anda terima dari AWS.
  - Mengelola kredensyal yang Anda dan tim Anda gunakan. Untuk informasi selengkapnya, lihat Identitas dan manajemen akses di AWS Backup.
  - Mengonfigurasi rencana cadangan dan penetapan sumber daya untuk mencerminkan kebijakan perlindungan data organisasi Anda. Untuk informasi selengkapnya, lihat Mengelola paket cadangan.
  - Secara teratur menguji kemampuan Anda untuk menemukan titik pemulihan tertentu dan mengembalikannya. Untuk informasi selengkapnya, lihat Menggunakan cadangan.
  - Memasukkan AWS Backup prosedur dalam pemulihan bencana organisasi Anda dan prosedur tertulis kelangsungan bisnis. Untuk titik awal, lihat Memulai dengan AWS Backup.
  - Memastikan bahwa karyawan Anda terbiasa dan telah AWS Backup berlatih menggunakan prosedur organisasi Anda jika terjadi keadaan darurat. Untuk informasi lebih lanjut, lihat Kerangka AWS Well-Architected.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Backup. Topik berikut menunjukkan cara mengonfigurasi AWS Backup untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan AWS Backup sumber daya Anda.

Topik

Validasi kepatuhan untuk AWS Backup

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Perlindungan data di AWS Backup

AWS Backup sesuai dengan model tanggung jawab AWS bersama, yang mencakup peraturan dan pedoman untuk perlindungan data. AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS layanan. AWS mempertahankan kontrol atas data yang dihosting pada infrastruktur ini, termasuk kontrol konfigurasi keamanan untuk menangani konten pelanggan dan data pribadi. AWS pelanggan dan AWS mitra Jaringan Mitra (APN), yang bertindak baik sebagai pengontrol data atau pengolah data, bertanggung jawab atas data pribadi apa pun yang mereka masukkan ke dalam. AWS Cloud

Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi Akun AWS kredensyal dan menyiapkan akun pengguna individu dengan AWS Identity and Access Management (IAM).

Ini membantu memastikan bahwa setiap pengguna hanya diberikan izin yang diperlukan untuk memenuhi tugas pekerjaan mereka. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan Secure Sockets Layer (SSL) /Transport Layer Security (TLS) untuk berkomunikasi dengan sumber daya. AWS
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default dalam AWS layanan.

Sebaiknya jangan pernah memasukkan informasi identitas yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Backup atau AWS layanan lain menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke AWS Backup atau layanan lain mungkin akan diambil untuk dimasukkan dalam log diagnostik. Saat Anda memberikan URL ke server eksternal, jangan menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Untuk informasi selengkapnya tentang perlindungan data, lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS .

Enkripsi untuk backup di AWS Backup

> **Note**
>
> AWS Backup Audit Manager membantu Anda mendeteksi backup yang tidak terenkripsi secara otomatis.

Anda dapat mengonfigurasi enkripsi untuk jenis sumber daya yang mendukung AWS Backup pengelolaan penuh dalam penggunaan AWS Backup. Jika jenis sumber daya tidak mendukung AWS Backup pengelolaan penuh, Anda harus mengonfigurasi enkripsi cadangannya dengan mengikuti petunjuk layanan tersebut, seperti enkripsi Amazon EBS di Panduan Pengguna Amazon Elastic Compute Cloud. Untuk melihat daftar jenis sumber daya yang mendukung AWS Backup manajemen penuh, lihat bagian “ AWS Backup Manajemen penuh” pada Ketersediaan fitur berdasarkan sumber daya tabel.

Tabel berikut mencantumkan setiap jenis sumber daya yang didukung, cara enkripsi dikonfigurasi untuk backup, dan apakah enkripsi independen untuk backup didukung. Ketika AWS Backup secara independen mengenkripsi cadangan, ia menggunakan algoritma enkripsi AES-256 standar industri.

Jenis sumber daya	Cara mengkonfigurasi enkripsi	AWS Backup Enkripsi independen
Amazon Simple Storage Service (Amazon S3)	Cadangan Amazon S3 dienkripsi menggunakan kunci AWS KMS (AWS Key Management Service) yang terkait dengan brankas cadangan. Kunci AWS KMS dapat berupa CMK yang dikelola pelanggan atau CMK yang dikelola yang AWS terkait dengan layanan. AWS Backup AWS Backup mengenkripsi semua cadangan bahkan jika bucket Amazon S3 sumber tidak dienkripsi.	Didukung
Mesin virtual VMware	Cadangan VM selalu dienkripsi. Kunci AWS KMS enkripsi untuk pencadangan mesin virtual dikonfigurasi di AWS Backup brankas tempat cadangan mesin virtual disimpan.	Didukung
Amazon DynamoDB setelah mengaktifkan Cadangan DynamoDB tingkat lanjut	Pencadangan DynamoDB selalu dienkripsi. Kunci AWS KMS enkripsi untuk backup DynamoDB dikonfigurasi di AWS Backup vault	Didukung

Jenis sumber daya	Cara mengkonfigurasi enkripsi	AWS Backup Enkripsi independen
	tempat cadangan DynamoDB disimpan.	
Amazon DynamoDB tanpa mengaktifkan Cadangan DynamoDB tingkat lanjut	Pencadangan DynamoDB secara otomatis dienkripsi dengan kunci enkripsi yang sama yang digunakan untuk mengenkripsi tabel DynamoDB sumber. Snapshot dari tabel DynamoDB yang tidak terenkripsi juga tidak terenkripsi. **Note** AWS Backup Untuk membuat cadangan tabel DynamoDB terenkripsi, Anda harus menambahkan izin `kms:Decrypt` dan peran IAM yang digunakan `kms:GenerateDataKey` untuk cadangan. Sebagai alternatif, Anda dapat menggunakan peran layanan AWS Backup default.	Tidak didukung

Jenis sumber daya	Cara mengkonfigurasi enkripsi	AWS Backup Enkripsi independen
Amazon Elastic File System (Amazon EFS)	Cadangan Amazon EFS selalu dienkripsi. Kunci AWS KMS enkripsi untuk cadangan Amazon EFS dikonfigurasi di AWS Backup brankas tempat cadangan Amazon EFS disimpan.	Didukung
Amazon Elastic Block Store (Amazon EBS)	Secara default, cadangan Amazon EBS dienkripsi menggunakan kunci yang digunakan untuk mengenkripsi volume sumber, atau tidak dienkripsi. Selama pemulihan, Anda dapat memilih untuk mengganti metode enkripsi default dengan menentukan kunci KMS.	Tidak didukung
AMI Amazon Elastic Compute Cloud (Amazon EC2)	AMI tidak terenkripsi. Snapshot EBS dienkripsi oleh aturan enkripsi default untuk cadangan EBS (lihat entri untuk EBS). Snapshot EBS data dan volume root dapat dienkripsi dan dilampirkan ke AMI.	Tidak didukung

Jenis sumber daya	Cara mengkonfigurasi enkripsi	AWS Backup Enkripsi independen
Amazon Relational Database Service (Amazon RDS)	Snapshot Amazon RDS secara otomatis dienkripsi dengan kunci enkripsi yang sama yang digunakan untuk mengenkripsi basis data Amazon RDS sumber. Cuplikan database Amazon RDS yang tidak terenkripsi juga tidak terenkripsi. **Note** AWS Backup Saat ini mendukung semua mesin database Amazon RDS, termasuk Amazon Aurora.	Tidak didukung
Amazon Aurora	Snapshot cluster Aurora secara otomatis dienkripsi dengan kunci enkripsi yang sama yang digunakan untuk mengenkripsi sumber cluster Amazon Aurora. Cuplikan cluster Aurora yang tidak terenkripsi juga tidak terenkripsi.	Tidak didukung

Jenis sumber daya	Cara mengkonfigurasi enkripsi	AWS Backup Enkripsi independen
AWS Storage Gateway	Snapshot Storage Gateway secara otomatis dienkripsi dengan kunci enkripsi yang sama yang digunakan untuk mengenkripsi volume Storage Gateway sumber. Snapshot dari volume Storage Gateway yang tidak terenkripsi juga tidak terenkripsi. **Note** Anda tidak perlu menggunakan kunci yang dikelola pelanggan di semua layanan untuk mengaktifkan Storage Gateway. Anda hanya perlu menyalin cadangan Storage Gateway ke vault yang mengonfigurasi kunci KMS. Ini karena Storage Gateway tidak memiliki kunci AWS KMS terkelola khusus layanan.	Tidak didukung

Jenis sumber daya	Cara mengkonfigurasi enkripsi	AWS Backup Enkripsi independen
Amazon FSx	Fitur enkripsi untuk sistem file Amazon FSx berbeda berdasarkan sistem file yang mendasarinya. Untuk mempelajari selengkapnya tentang sistem file Amazon FSx khusus Anda, lihat Panduan Pengguna FSx yang sesuai.	Tidak didukung
Amazon DocumentDB	Snapshot cluster Amazon DocumentDB secara otomatis dienkripsi dengan kunci enkripsi yang sama yang digunakan untuk mengenkripsi cluster Amazon DocumentDB sumber. Cuplikan cluster Amazon DocumentDB yang tidak terenkripsi juga tidak terenkripsi.	Tidak didukung
Amazon Neptune	Snapshot cluster Neptunus secara otomatis dienkripsi dengan kunci enkripsi yang sama yang digunakan untuk mengenkripsi cluster Neptunus sumber. Cuplikan cluster Neptunus yang tidak terenkripsi juga tidak terenkripsi.	Tidak didukung

Jenis sumber daya	Cara mengkonfigurasi enkripsi	AWS Backup Enkripsi independen
Amazon Timestream	Pencadangan snapshot tabel timestream selalu dienkripsi. Kunci AWS KMS enkripsi untuk cadangan Timestream dikonfigurasi di brankas cadangan tempat cadangan Timestream disimpan.	Didukung
Amazon Redshift	Cluster Amazon Redshift secara otomatis dienkripsi dengan kunci enkripsi yang sama yang digunakan untuk mengenkripsi cluster Amazon Redshift sumber. Cuplikan cluster Amazon Redshift yang tidak terenkripsi juga tidak terenkripsi.	Tidak didukung
AWS CloudFormation	CloudFormation backup selalu dienkripsi. Kunci CloudFormation enkripsi untuk CloudFormation cadangan dikonfigurasi di CloudFormation brankas tempat CloudFormation cadangan disimpan.	Didukung
Database SAP HANA pada instans Amazon EC2	Backup database SAP HANA selalu dienkripsi. Kunci AWS KMS enkripsi untuk backup database SAP HANA dikonfigurasi di AWS Backup brankas tempat backup database disimpan.	Didukung

Enkripsi untuk salinan cadangan

Saat Anda menggunakannya AWS Backup untuk menyalin cadangan di seluruh akun atau Wilayah, AWS Backup secara otomatis mengenkripsi salinan tersebut untuk sebagian besar jenis sumber daya, meskipun cadangan asli tidak dienkripsi. AWS Backup mengenkripsi salinan Anda menggunakan kunci KMS vault target. Namun, snapshot dari cluster Aurora, Amazon DocumentDB, dan Neptunus yang tidak terenkripsi juga tidak terenkripsi.

Enkripsi dan salinan cadangan

Salinan lintas akun dengan kunci KMS AWS terkelola tidak didukung untuk sumber daya yang tidak dikelola sepenuhnya oleh. AWS Backup Lihat AWS Backup Manajemen penuh untuk menentukan sumber daya mana yang sepenuhnya dikelola.

Untuk sumber daya yang dikelola sepenuhnya oleh AWS Backup, cadangan dienkripsi dengan kunci enkripsi brankas cadangan. Untuk sumber daya yang tidak sepenuhnya dikelola oleh AWS Backup, salinan lintas akun menggunakan kunci KMS yang sama dengan sumber daya sumber. Untuk informasi selengkapnya, lihat Kunci enkripsi dan salinan lintas akun

Enkripsi kredensi hypervisor mesin virtual

Mesin virtual yang dikelola oleh hypervisor menggunakan AWS Backup Gateway untuk menghubungkan sistem lokal. AWS Backup Adalah penting bahwa hypervisor memiliki keamanan yang kuat dan andal yang sama. Keamanan ini dapat dicapai dengan mengenkripsi hypervisor, baik dengan kunci yang AWS dimiliki atau dengan kunci yang dikelola pelanggan.

AWS kunci yang dimiliki dan dikelola pelanggan

AWS Backup menyediakan enkripsi untuk kredensyal hypervisor untuk melindungi informasi login pelanggan yang sensitif menggunakan AWS kunci enkripsi yang dimiliki. Anda memiliki opsi untuk menggunakan kunci yang dikelola pelanggan sebagai gantinya.

Secara default, kunci yang digunakan untuk mengenkripsi kredensyal di hypervisor Anda adalah kunci yang dimiliki.AWS AWS Backup menggunakan kunci ini untuk mengenkripsi kredensyal hypervisor secara otomatis. Anda tidak dapat melihat, mengelola, atau menggunakan kunci yang AWS dimiliki, Anda juga tidak dapat mengaudit penggunaannya. Namun, Anda tidak perlu mengambil tindakan apa pun atau mengubah program apa pun untuk melindungi kunci yang mengenkripsi data Anda. Untuk informasi selengkapnya, lihat kunci yang AWS dimiliki di Panduan AWS KMS Pengembang.

Atau, kredensyal dapat dienkripsi menggunakan kunci yang dikelola Pelanggan. AWS Backup mendukung penggunaan kunci yang dikelola pelanggan simetris yang Anda buat, miliki, dan kelola untuk melakukan enkripsi Anda. Karena Anda memiliki kendali penuh atas enkripsi ini, Anda dapat melakukan tugas-tugas seperti:

- Menetapkan dan memelihara kebijakan utama
- Menetapkan dan memelihara kebijakan dan hibah IAM
- Mengaktifkan dan menonaktifkan kebijakan utama
- Memutar bahan kriptografi kunci
- Menambahkan tanda
- Membuat alias kunci
- Kunci penjadwalan untuk penghapusan

Saat Anda menggunakan kunci yang dikelola pelanggan, AWS Backup validasi apakah peran Anda memiliki izin untuk mendekripsi menggunakan kunci ini (sebelum pekerjaan pencadangan atau pemulihan dijalankan). Anda harus menambahkan `kms:Decrypt` tindakan ke peran yang digunakan untuk memulai pekerjaan pencadangan atau pemulihan.

Karena `kms:Decrypt` tindakan tidak dapat ditambahkan ke peran cadangan default, Anda harus menggunakan peran selain peran cadangan default untuk menggunakan kunci yang dikelola pelanggan.

Untuk informasi selengkapnya, lihat kunci terkelola pelanggan di Panduan AWS Key Management Service Pengembang.

Hibah diperlukan saat menggunakan kunci yang dikelola pelanggan

AWS KMS membutuhkan hibah untuk menggunakan kunci yang dikelola pelanggan Anda. Saat Anda mengimpor konfigurasi hypervisor yang dienkripsi dengan kunci yang dikelola pelanggan, AWS Backup buat hibah atas nama Anda dengan mengirimkan permintaan ke. `CreateGrant` AWS KMS AWS Backup menggunakan hibah untuk mengakses kunci KMS di akun pelanggan.

Anda dapat mencabut akses ke hibah, atau menghapus AWS Backup akses ke kunci yang dikelola pelanggan kapan saja. Jika Anda melakukannya, semua gateway Anda yang terkait dengan hypervisor Anda tidak dapat lagi mengakses nama pengguna dan kata sandi hypervisor yang dienkripsi oleh kunci yang dikelola pelanggan, yang akan memengaruhi pencadangan dan pemulihan

pekerjaan Anda. Secara khusus, pencadangan dan pemulihan pekerjaan yang Anda lakukan pada mesin virtual di hypervisor ini akan gagal.

Backup gateway menggunakan `RetireGrant` operasi untuk menghapus hibah saat Anda menghapus hypervisor.

Memantau kunci enkripsi

Saat Anda menggunakan kunci yang dikelola AWS KMS pelanggan dengan AWS Backup sumber daya Anda, Anda dapat menggunakan AWS CloudTrailatau Amazon CloudWatch Logs untuk melacak permintaan yang AWS Backup dikirim AWS KMS.

Cari AWS CloudTrail peristiwa dengan `"eventName"` bidang berikut untuk memantau AWS KMS operasi yang dipanggil oleh AWS Backup untuk mengakses data yang dienkripsi oleh kunci terkelola pelanggan Anda:

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

Manajemen identitas dan akses di AWS Backup

Akses ke AWS Backup membutuhkan kredensyal. Kredensyal tersebut harus memiliki izin untuk mengakses AWS sumber daya, seperti database Amazon DynamoDB atau sistem file Amazon EFS. Selain itu, titik pemulihan yang dibuat oleh AWS Backup untuk beberapa layanan yang AWS Backup didukung tidak dapat dihapus menggunakan layanan sumber (seperti Amazon EFS). Anda dapat menghapus titik pemulihan tersebut menggunakan AWS Backup.

Bagian berikut memberikan rincian tentang bagaimana Anda dapat menggunakan AWS Identity and Access Management (IAM) dan AWS Backup untuk membantu mengamankan akses ke sumber daya Anda.

> **Warning**
>
> AWS Backup menggunakan peran IAM yang sama dengan yang Anda pilih saat menetapkan sumber daya untuk mengelola siklus hidup titik pemulihan Anda. Jika Anda menghapus atau mengubah peran itu, AWS Backup tidak dapat mengelola siklus hidup titik pemulihan

Anda. Ketika ini terjadi, ia akan mencoba menggunakan peran terkait layanan untuk mengelola siklus hidup Anda. Dalam sebagian kecil kasus, ini mungkin juga tidak berfungsi, meninggalkan titik `EXPIRED` pemulihan pada penyimpanan Anda, yang mungkin menimbulkan biaya yang tidak diinginkan. Untuk menghapus titik `EXPIRED` pemulihan, hapus secara manual menggunakan prosedur di Menghapus cadangan.

Topik

Autentikasi

Akses ke AWS Backup atau AWS layanan yang Anda cadangkan memerlukan kredensyal yang AWS dapat digunakan untuk mengautentikasi permintaan Anda. Anda dapat mengakses AWS sebagai salah satu jenis identitas berikut:

- Akun AWS pengguna root — Saat Anda mendaftar AWS, Anda memberikan alamat email dan kata sandi yang terkait dengan AWS akun Anda. Ini adalah pengguna Akun AWS root Anda. Kredensialnya menyediakan akses lengkap ke semua sumber daya Anda AWS .

  > **Important**
  >
  > Untuk alasan keamanan, kami sarankan Anda menggunakan pengguna root hanya untuk membuat administrator. Administrator adalah pengguna IAM dengan izin penuh untuk Anda. Akun AWS Anda kemudian dapat menggunakan pengguna admin ini untuk membuat pengguna dan peran IAM lainnya dengan izin terbatas. Untuk informasi selengkapnya, lihat Praktik Terbaik IAM dan Membuat Pengguna Admin IAM dan Grup Pertama Anda dalam Panduan Pengguna IAM.

- Pengguna IAM — Pengguna IAM adalah identitas di dalam Anda Akun AWS yang memiliki izin khusus khusus (misalnya, izin untuk membuat brankas cadangan untuk menyimpan cadangan

Anda). Anda dapat menggunakan nama pengguna dan kata sandi IAM untuk masuk untuk mengamankan AWS halaman web seperti, Forum AWS Diskusi AWS Management Console, atau Pusat.AWS Support

Selain nama pengguna dan kata sandi, Anda juga dapat membuat access key untuk setiap pengguna. Anda dapat menggunakan kunci ini ketika Anda mengakses AWS layanan secara terprogram, baik melalui salah satu dari beberapa SDK atau dengan menggunakan (AWS Command Line Interface CLI AWS). Alat SDK dan AWS CLI menggunakan kunci akses untuk menandatangani permintaan Anda secara kriptografis. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang melakukan autentikasi permintaan, lihat Proses Penandatanganan Tanda Tangan Versi 4 dalam Referensi Umum AWS.

- IAM role – IAM role adalah identitas IAM yang dapat Anda buat di akun Anda yang memiliki izin spesifik. Peran ini mirip dengan Pengguna IAM, tetapi tidak terkait dengan orang tertentu. Peran IAM memungkinkan Anda memperoleh kunci akses sementara yang dapat digunakan untuk mengakses AWS layanan dan sumber daya. Peran IAM dengan kredensial sementara berguna dalam situasi berikut:
  - Akses pengguna federasi — Alih-alih membuat pengguna IAM, Anda dapat menggunakan identitas pengguna yang sudah ada sebelumnya dari AWS Directory Service, direktori pengguna perusahaan Anda, atau penyedia identitas web. Ini dikenal sebagai pengguna gabungan. AWS menugaskan peran kepada pengguna gabungan saat akses diminta melalui penyedia identitas. Untuk informasi lebih lanjut tentang pengguna gabungan, lihat Pengguna Gabungan dan Peran di Panduan Pengguna IAM.
  - Administrasi lintas akun — Anda dapat menggunakan peran IAM di akun Anda untuk memberikan Akun AWS izin lain untuk mengelola sumber daya akun Anda. Sebagai contoh, lihat Tutorial: Mendelegasikan Akses di Seluruh Akun AWS Menggunakan Peran IAM dalam Panduan Pengguna IAM.
  - AWS akses layanan — Anda dapat menggunakan peran IAM di akun Anda untuk memberikan izin AWS layanan untuk mengakses sumber daya akun Anda. Untuk informasi selengkapnya, lihat Membuat Peran untuk Mendelegasikan Izin ke AWS Layanan di Panduan Pengguna IAM.
  - Aplikasi yang berjalan di Amazon Elastic Compute Cloud (Amazon EC2) - Anda dapat menggunakan peran IAM untuk mengelola kredensyal sementara untuk aplikasi yang berjalan pada instans Amazon EC2 dan membuat permintaan API. AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans memuat peran dan memungkinkan program yang berjalan

di instans EC2 untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM role untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan pengguna IAM.

Pengendalian akses

Anda dapat memiliki kredensyal yang valid untuk mengautentikasi permintaan Anda, tetapi kecuali Anda memiliki izin yang sesuai, Anda tidak dapat mengakses AWS Backup sumber daya seperti brankas cadangan. Anda juga tidak dapat mencadangkan AWS sumber daya seperti volume Amazon Elastic Block Store (Amazon EBS).

Setiap AWS sumber daya dimiliki oleh Akun AWS, dan izin untuk membuat atau mengakses sumber daya diatur oleh kebijakan izin. Administrator akun dapat melampirkan kebijakan izin ke identitas AWS Identity and Access Management (IAM) (yaitu, pengguna, grup, dan peran). Dan beberapa layanan juga mendukung melampirkan kebijakan izin ke sumber daya.

> **Note**
>
> Administrator akun (atau pengguna administrator) adalah pengguna dengan izin administrator. Untuk informasi selengkapnya, lihat Praktik Terbaik IAM dalam Panduan Pengguna IAM.

Ketika memberikan izin, Anda memutuskan siap yang mendapatkan izin, sumber daya yang mereka dapatkan izinnya, dan tindakan khusus yang ingin Anda izinkan di sumber daya tersebut.

Bagian berikut mencakup cara kerja kebijakan akses dan cara Anda menggunakannya untuk melindungi cadangan Anda.

Topik

- Sumber daya dan operasi
- Kepemilikan sumber daya
- Menentukan elemen kebijakan: tindakan, efek, dan prinsip
- Menentukan kondisi dalam kebijakan
- Izin API: referensi tindakan, sumber daya, dan kondisi
- Izin menyalin tag

- Kebijakan akses

Sumber daya dan operasi

Sumber daya adalah objek yang ada dalam layanan. AWS Backup sumber daya termasuk rencana cadangan, brankas cadangan, dan cadangan. Backup adalah istilah umum yang mengacu pada berbagai jenis sumber daya cadangan yang ada di dalamnya AWS. Misalnya, snapshot Amazon EBS, snapshot Amazon Relational Database Service (Amazon RDS), dan backup Amazon DynamoDB adalah semua jenis sumber daya cadangan.

Pada tahun AWS Backup, cadangan juga disebut sebagai titik pemulihan. Saat menggunakan AWS Backup, Anda juga bekerja dengan sumber daya dari AWS layanan lain yang Anda coba lindungi, seperti volume Amazon EBS atau tabel DynamoDB. Sumber daya ini memiliki Nama Sumber Daya Amazon (ARN) unik yang terkait dengannya. ARN secara unik mengidentifikasi sumber daya. AWS Anda harus memiliki ARN ketika Anda perlu menentukan sumber daya secara jelas di semua AWS, seperti dalam kebijakan IAM atau panggilan API.

Tabel berikut mencantumkan sumber daya, subresource, format ARN, dan contoh ID unik.

AWS Backup ARN sumber daya

Jenis sumber daya	Format ARN	Contoh ID unik
Paket Backup	`arn:aws:backup:`*`region`*`:`*`account-id`*`:backup-plan:*`	
Brankas cadangan	`arn:aws:backup:`*`region`*`:`*`account-id`*`:backup-vault:*`	
Titik pemulihan untuk Amazon EBS	`arn:aws:ec2:`*`region`*`::snapshot/*`	`snapshot/snap-05f426fd8kdjb4224`
Titik pemulihan untuk gambar Amazon EC2	`arn:aws:ec2:`*`region`*`::image/ami-*`	`image/ami-1a2b3e4f5e6f7g890`

Jenis sumber daya	Format ARN	Contoh ID unik
Titik pemulihan untuk Amazon RDS	`arn:aws:rds:region:account-id:snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Titik pemulihan untuk Aurora	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Titik pemulihan untuk Storage Gateway	`arn:aws:ec2:region::snapshot/*`	`snapshot/snap-0d40e49137e31d9e0`
Titik pemulihan untuk DynamoDB tanpa Cadangan DynamoDB tingkat lanjut	`arn:aws:dynamodb:region:account-id:table/*/backup/*`	`table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3`
Titik pemulihan untuk DynamoDB dengan diaktifkan Cadangan DynamoDB tingkat lanjut	`arn:aws:backup:region:account-id:recovery-point:*`	`12a34a56-7bb8-901c-cd23-4567d8e9ef01`
Titik pemulihan untuk Amazon EFS	`arn:aws:backup:region:account-id:recovery-point:*`	`d99699e7-e183-477e-bfcd-ccb1c6e5455e`
Titik pemulihan untuk Amazon FSx	`arn:aws:fsx:region:account-id:backup/backup-*`	`backup/backup-1a20e49137e31d9e0`
Titik pemulihan untuk mesin virtual	`arn:aws:backup:region:account-id:recovery-point:*`	`1801234a-5b6b-7dc8-8032-836f7ffc623b`

Jenis sumber daya	Format ARN	Contoh ID unik
Titik pemulihan untuk pencadangan berkelanjutan Amazon S3	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -5ec207d0
Titik pemulihan untuk cadangan berkala S3	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -20211231900000-5ec207d0
Titik pemulihan untuk Amazon DocumentDB	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Titik pemulihan untuk Neptunus	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Titik pemulihan untuk Amazon Redshift	arn:aws:redshift: *region*:*account-id* :snapshot: *resource*/awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Titik pemulihan untuk Amazon Timestream	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta
Titik pemulihan untuk AWS CloudFormation template	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012
Titik pemulihan untuk database SAP HANA pada instans Amazon EC2	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012

Sumber daya yang mendukung AWS Backup manajemen penuh semuanya memiliki titik pemulihan dalam format`arn:aws:backup:region:account-id::recovery-point:*`. Memudahkan Anda menerapkan kebijakan izin untuk melindungi titik pemulihan tersebut. Untuk melihat sumber daya mana yang mendukung AWS Backup manajemen penuh, lihat bagian Ketersediaan fitur berdasarkan sumber daya tabel tersebut.

AWS Backup menyediakan satu set operasi untuk bekerja dengan AWS Backup sumber daya. Untuk daftar operasi yang tersedia, lihat AWS Backup Tindakan.

Kepemilikan sumber daya

Akun AWS Memiliki sumber daya yang dibuat di akun, terlepas dari siapa yang menciptakan sumber daya. Secara khusus, pemilik sumber daya adalah entitas utama (yaitu, pengguna Akun AWS root, pengguna IAM, atau peran IAM) yang mengautentikasi permintaan pembuatan sumber daya. Akun AWS Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredensyal pengguna Akun AWS root Anda Akun AWS untuk membuat brankas cadangan, Anda Akun AWS adalah pemilik brankas.
- Jika Anda membuat pengguna IAM di Akun AWS dan memberikan izin untuk membuat brankas cadangan kepada pengguna tersebut, pengguna dapat membuat brankas cadangan. Namun, AWS akun Anda, tempat pengguna berada, memiliki sumber daya brankas cadangan.
- Jika Anda membuat peran IAM Akun AWS dengan izin untuk membuat brankas cadangan, siapa pun yang dapat mengambil peran tersebut dapat membuat vault. Anda Akun AWS, yang menjadi milik peran tersebut, memiliki sumber daya brankas cadangan.

Menentukan elemen kebijakan: tindakan, efek, dan prinsip

Untuk setiap AWS Backup sumber daya (lihatSumber daya dan operasi), layanan mendefinisikan satu set operasi API (lihatTindakan). Untuk memberikan izin untuk operasi API ini, AWS Backup tentukan serangkaian tindakan yang dapat Anda tentukan dalam kebijakan. Operasi API dapat memerlukan izin untuk lebih dari satu tindakan.

Berikut adalah elemen-elemen kebijakan yang paling dasar:

- Sumber daya – Dalam kebijakan, Anda menggunakan Amazon Resource Name (ARN) untuk mengidentifikasi sumber daya yang diatur kebijakan. Untuk informasi selengkapnya, lihat Sumber daya dan operasi.

- Tindakan – Anda menggunakan kata kunci tindakan untuk mengidentifikasi operasi sumber daya yang ingin Anda izinkan atau tolak.
- Efek – Anda menentukan efek ketika pengguna meminta tindakan tertentu—efek ini dapat berupa pemberian izin atau penolakan. Jika Anda tidak secara eksplisit memberikan akses ke (mengizinkan) sumber daya, akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat mengaksesnya, meskipun kebijakan yang berbeda memberikan akses.
- Principal – Dalam kebijakan berbasis identitas (Kebijakan IAM), pengguna yang kebijakannya terlampir adalah principal yang implisit. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang diinginkan untuk menerima izin (berlaku hanya untuk kebijakan berbasis sumber daya).

Untuk mem-pelajari selengkapnya tentang sintaksis dan penjelasan kebijakan IAM, lihat Referensi Kebijakan JSON IAM dalam Panduan Pengguna IAM.

Untuk tabel yang menampilkan semua tindakan AWS Backup API, lihatIzin API: referensi tindakan, sumber daya, dan kondisi.

Menentukan kondisi dalam kebijakan

Ketika Anda memberikan izin, Anda dapat menggunakan bahasa kebijakan IAM untuk menentukan kondisi ketika kebijakan harus berlaku. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu. Untuk informasi selengkapnya tentang menentukan kondisi dalam bahasa kebijakan, lihat Kondisi dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

AWS Backup mendefinisikan set sendiri dari kunci kondisi. Untuk melihat daftar kunci AWS Backup kondisi, lihat Kunci kondisi untuk AWS Backup dalam Referensi Otorisasi Layanan.

Izin API: referensi tindakan, sumber daya, dan kondisi

Saat Anda mengatur Pengendalian akses dan menulis kebijakan izin yang dapat Anda lampirkan ke identitas IAM (kebijakan berbasis identitas), Anda dapat menggunakan daftar sebagai referensi. Daftar mencakup setiap operasi AWS Backup API, tindakan terkait yang dapat Anda berikan izin untuk melakukan tindakan, dan AWS sumber daya yang dapat Anda berikan izin. Anda menentukan tindakan dalam bidang `Action` kebijakan, dan Anda menentukan nilai sumber daya pada bidang

`Resource` kebijakan. Jika `Resource` bidang kosong, Anda dapat menggunakan wildcard (`*`) untuk menyertakan semua sumber daya.

Anda dapat menggunakan kunci kondisi AWS-wide dalam AWS Backup kebijakan Anda untuk menyatakan kondisi. Untuk daftar lengkap tombol AWS-wide, lihat Kunci yang Tersedia di Panduan Pengguna IAM.

[1] Menggunakan kebijakan akses vault yang ada.

[2] Lihat AWS Backup ARN sumber daya untuk ARN titik pemulihan khusus sumber daya.

[3] `StartRestoreJob` harus memiliki pasangan kunci-nilai dalam metadata untuk sumber daya. Untuk mendapatkan metadata sumber daya, panggil API. `GetRecoveryPointRestoreMetadata`

[4] Jenis sumber daya tertentu memerlukan peran yang melakukan pencadangan untuk memiliki izin penandaan tertentu `backup:TagResource` jika Anda berencana untuk menyertakan tag sumber daya asli dalam cadangan Anda atau menambahkan tag tambahan ke cadangan. Pencadangan apa pun dengan ARN yang dimulai dengan `arn:aws:backup:`*`region`*`:`*`account-id`*`:recovery-point:` atau cadangan yang berkelanjutan memerlukan izin ini. `backup:TagResource`Izin harus diterapkan untuk `"`*`resourcetype`*`": "arn:aws:backup:`*`region`*`:`*`account-id:`*`recovery-point:*"`

Untuk informasi selengkapnya, lihat Kunci tindakan, sumber daya, dan kondisi AWS Backup di Referensi Otorisasi Layanan.

Izin menyalin tag

Saat AWS Backup melakukan pekerjaan pencadangan atau penyalinan, ia mencoba menyalin tag dari sumber daya sumber Anda (atau titik pemulihan dalam kasus penyalinan) ke titik pemulihan Anda.

> **Note**
>
> AWS Backup tidak menyalin tag secara asli selama pekerjaan pemulihan. Untuk arsitektur berbasis peristiwa yang akan menyalin tag selama pekerjaan pemulihan, lihat Cara menyimpan tag sumber daya dalam AWS Backup memulihkan pekerjaan.

Selama pekerjaan pencadangan atau penyalinan, AWS Backup agregat tag yang Anda tentukan dalam paket cadangan (atau salin paket, atau cadangan sesuai permintaan) dengan tag dari sumber daya sumber Anda. Namun, AWS memberlakukan batas 50 tag per sumber daya, yang AWS Backup

tidak dapat melebihi. Ketika pencadangan atau salinan pekerjaan mengumpulkan tag dari paket dan sumber daya, mungkin menemukan lebih dari 50 tag total, itu tidak akan dapat menyelesaikan pekerjaan, dan akan gagal dalam pekerjaan. Ini konsisten dengan praktik terbaik penandaan AWS-wide. Untuk mempelajari selengkapnya, lihat Batas tag di Panduan Referensi AWS Umum.

- Sumber daya Anda memiliki lebih dari 50 tag setelah menggabungkan tag pekerjaan cadangan Anda dengan tag sumber daya sumber Anda. AWS mendukung hingga 50 tag per sumber daya. Untuk informasi selengkapnya, lihat Batas tag.
- Peran IAM yang Anda berikan AWS Backup tidak memiliki izin untuk membaca tag sumber atau menyetel tag tujuan. Untuk informasi selengkapnya dan contoh kebijakan peran IAM, lihat Kebijakan Terkelola.

Anda dapat menggunakan paket cadangan untuk membuat tag yang bertentangan dengan tag sumber daya sumber Anda. Ketika kedua konflik, tag dari rencana cadangan Anda diutamakan. Gunakan teknik ini jika Anda memilih untuk tidak menyalin nilai tag dari sumber daya sumber Anda. Tentukan kunci tag yang sama, tetapi nilainya berbeda atau kosong, menggunakan paket cadangan Anda.

Izin Diperlukan untuk menetapkan tag ke cadangan

Jenis sumber daya	Izin yang diperlukan
Sistem file Amazon EFS	`elasticfilesystem:DescribeTags`
Sistem file Amazon FSx	`fsx:ListTagsForResource`
Basis data Amazon RDS dan cluster Amazon Aurora	`rds:AddTagsToResource` `rds:ListTagsForResource`
Volume Storage Gateway	`storagegateway:ListTagsForResource`
Instans Amazon EC2 dan volume Amazon EBS	`EC2:CreateTags` `EC2:DescribeTags`

DynamoDB tidak mendukung penetapan tag ke cadangan kecuali Anda mengaktifkan terlebih dahulu. Cadangan DynamoDB tingkat lanjut

Saat cadangan Amazon EC2 membuat Titik Pemulihan Gambar dan sekumpulan snapshot, AWS Backup menyalin tag ke AMI yang dihasilkan. AWS Backup juga menyalin tag dari volume yang terkait dengan instans Amazon EC2 ke snapshot yang dihasilkan.

Kebijakan akses

Kebijakan izin menjelaskan siapa yang memiliki akses ke suatu objek. Kebijakan yang terlampir pada identitas IAM disebut sebagai kebijakan berbasis identitas (kebijakan IAM). Kebijakan yang melekat pada sumber daya disebut sebagai kebijakan berbasis sumber daya. AWS Backup mendukung kebijakan berbasis identitas dan kebijakan berbasis sumber daya.

> **Note**
>
> Bagian ini membahas penggunaan IAM dalam konteks. AWS Backup Bagian ini tidak memberikan informasi yang mendetail tentang layanan IAM. Untuk dokumentasi IAM lengkap, lihat Apa yang Dimaksud dengan IAM? dalam Panduan Pengguna IAM. Untuk informasi tentang sintaksis dan penjelasan kebijakan IAM, lihat Referensi Kebijakan IAM JSON dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas (kebijakan IAM)

Kebijakan berbasis identitas adalah kebijakan yang dapat Anda lampirkan ke identitas IAM, seperti pengguna atau peran. Misalnya, Anda dapat menentukan kebijakan yang memungkinkan pengguna untuk melihat dan mencadangkan AWS sumber daya, tetapi mencegahnya memulihkan cadangan.

Untuk informasi lebih lanjut tentang pengguna, grup, peran, dan izin, lihat Identitas (Pengguna, Grup, dan Peran) dalam Panduan Pengguna IAM.

Untuk informasi tentang cara menggunakan kebijakan IAM untuk mengontrol akses ke cadangan, lihat. Kebijakan terkelola untuk AWS Backup

Kebijakan berbasis sumber daya

AWS Backup mendukung kebijakan akses berbasis sumber daya untuk brankas cadangan. Ini memungkinkan Anda menentukan kebijakan akses yang dapat mengontrol pengguna mana yang memiliki jenis akses apa pun ke cadangan apa pun yang diatur dalam brankas cadangan. Kebijakan akses berbasis sumber daya untuk brankas cadangan menyediakan cara mudah untuk mengontrol akses ke cadangan Anda.

Kebijakan akses vault cadangan mengontrol akses pengguna saat Anda menggunakan AWS Backup API. Beberapa jenis cadangan, seperti snapshot Amazon Elastic Block Store (Amazon EBS) dan Amazon Relational Database Service (Amazon RDS), juga dapat diakses menggunakan API layanan tersebut. Anda dapat membuat kebijakan akses terpisah di IAM yang mengontrol akses ke API tersebut untuk sepenuhnya mengontrol akses ke cadangan.

Untuk mempelajari cara membuat kebijakan akses untuk brankas cadangan, lihat. Tetapkan kebijakan akses pada brankas cadangan

Peran layanan IAM

Peran AWS Identity and Access Management (IAM) mirip dengan pengguna, karena itu adalah AWS identitas dengan kebijakan izin yang menentukan apa yang dapat dan tidak dapat dilakukan identitas. AWS Namun, alih-alih secara unik terkait dengan satu orang, peran dimaksudkan untuk menjadi dapat diambil oleh siapa pun yang membutuhkannya. Peran layanan adalah peran yang diasumsikan AWS layanan untuk melakukan tindakan atas nama Anda. Sebagai layanan yang melakukan operasi pencadangan atas nama Anda, AWS Backup mengharuskan Anda meneruskannya peran untuk diasumsikan saat melakukan operasi pencadangan atas nama Anda. Untuk informasi selengkapnya tentang peran IAM, lihat Peran IAM dalam Panduan Pengguna IAM.

Peran yang Anda berikan AWS Backup harus memiliki kebijakan IAM dengan izin yang memungkinkan AWS Backup untuk melakukan tindakan yang terkait dengan operasi pencadangan, seperti membuat, memulihkan, atau kedaluwarsa pencadangan. Izin yang berbeda diperlukan untuk setiap AWS layanan yang AWS Backup mendukung. Peran juga harus AWS Backup terdaftar sebagai entitas tepercaya, yang memungkinkan AWS Backup untuk mengambil peran.

Saat Anda menetapkan sumber daya ke paket cadangan, atau jika Anda melakukan pencadangan, penyalinan, atau pemulihan sesuai permintaan, Anda harus meneruskan peran layanan yang memiliki akses untuk melakukan operasi dasar pada sumber daya yang ditentukan. AWS Backup menggunakan peran ini untuk membuat, menandai, dan menghapus sumber daya di akun Anda.

Menggunakan AWS peran untuk mengontrol akses ke cadangan

Anda dapat menggunakan peran untuk mengontrol akses ke cadangan Anda dengan mendefinisikan peran dengan cakupan sempit dan dengan menentukan siapa yang dapat meneruskan peran itu. AWS Backup Misalnya, Anda dapat membuat peran yang hanya memberikan izin untuk mencadangkan database Amazon Relational Database Service (Amazon RDS) dan hanya memberikan izin kepada pemilik database Amazon RDS untuk meneruskan peran tersebut. AWS Backup AWS Backup menyediakan beberapa kebijakan terkelola yang telah ditetapkan untuk setiap

layanan yang didukung. Anda dapat melampirkan kebijakan terkelola ini ke peran yang Anda buat. Ini membuatnya lebih mudah untuk membuat peran khusus layanan yang memiliki izin yang benar yang diperlukan. AWS Backup

Untuk informasi selengkapnya tentang kebijakan AWS terkelola AWS Backup, lihatKebijakan terkelola untuk AWS Backup.

Peran layanan default untuk AWS Backup

Saat menggunakan AWS Backup konsol untuk pertama kalinya, Anda dapat memilih untuk AWS Backup membuat peran layanan default untuk Anda. Peran ini memiliki izin yang AWS Backup diperlukan untuk membuat dan memulihkan cadangan atas nama Anda.

> **Note**
>
> Peran default dibuat secara otomatis saat Anda menggunakan AWS Management Console. Anda dapat membuat peran default menggunakan AWS Command Line Interface (AWS CLI), tetapi harus dilakukan secara manual.

Jika Anda lebih suka menggunakan peran khusus, seperti peran terpisah untuk jenis sumber daya yang berbeda, Anda juga dapat melakukannya dan meneruskan peran kustom Anda AWS Backup. Untuk melihat contoh peran yang mengaktifkan pencadangan dan pemulihan untuk masing-masing jenis sumber daya, lihat Kebijakan yang dikelola pelanggan tabel.

Peran layanan default diberi nama`AWSBackupDefaultServiceRole`. Peran layanan ini berisi dua kebijakan terkelola, AWSBackupServiceRolePolicyForBackupdan AWSBackupServiceRolePolicyForRestores.

`AWSBackupServiceRolePolicyForBackup`mencakup kebijakan IAM yang memberikan AWS Backup izin untuk menggambarkan sumber daya yang dicadangkan, kemampuan untuk membuat, menghapus, mendeskripsikan, atau menambahkan tag ke cadangan terlepas dari AWS KMS kunci yang dienkripsi.

`AWSBackupServiceRolePolicyForRestores`menyertakan kebijakan IAM yang memberikan AWS Backup izin untuk membuat, menghapus, atau menjelaskan sumber daya baru yang dibuat dari cadangan, terlepas dari AWS KMS kunci yang dienkripsi. Ini juga mencakup izin untuk menandai sumber daya yang baru dibuat.

Untuk memulihkan instans Amazon EC2, Anda harus meluncurkan instans baru.

Membuat peran layanan default di konsol

Tindakan spesifik yang Anda lakukan di AWS Backup Konsol membuat peran layanan AWS Backup default.

Untuk membuat peran layanan AWS Backup default di AWS akun Anda

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Untuk membuat peran untuk akun Anda, tetapkan sumber daya ke paket cadangan atau buat cadangan sesuai permintaan.

   a. Buat rencana cadangan dan tetapkan sumber daya ke cadangan. Lihat Membuat cadangan terjadwal.

   b. Atau, buat cadangan sesuai permintaan. Lihat Membuat cadangan sesuai permintaan.
3. Verifikasi bahwa Anda telah membuat akun Anda dengan mengikuti langkah-langkah berikut: `AWSBackupDefaultServiceRole`

   a. Tunggu beberapa menit. Untuk informasi selengkapnya, lihat Perubahan yang saya buat tidak selalu langsung terlihat di Panduan Pengguna AWS Identity and Access Management.

   b. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.

   c. Di menu navigasi kiri, pilih Peran.

   d. Di bilah pencarian, ketik`AWSBackupDefaultServiceRole`. Jika pilihan ini ada, Anda telah membuat peran AWS Backup default dan menyelesaikan prosedur ini.

   e. Jika `AWSBackupDefaultServiceRole` masih tidak muncul, tambahkan izin berikut ke pengguna IAM atau peran IAM yang Anda gunakan untuk mengakses konsol.

```
{
  "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":"*"
    }
  ]
}
```

Untuk Wilayah China, ganti *aws* dengan *aws-cn*. Untuk AWS GovCloud (US) Wilayah, ganti *aws* dengan *aws-us-gov*.

f. Jika Anda tidak dapat menambahkan izin ke pengguna IAM atau peran IAM, minta administrator untuk membuat peran dengan nama selain secara manual `AWSBackupDefaultServiceRole` dan melampirkan peran tersebut ke kebijakan terkelola ini:

- `AWSBackupServiceRolePolicyForBackup`
- `AWSBackupServiceRolePolicyForRestores`

Kebijakan terkelola untuk AWS Backup

Kebijakan terkelola adalah kebijakan berbasis identitas mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Saat Anda melampirkan kebijakan pada entitas prinsipal, Anda memberikan entitas sebuah izin yang ditentukan dalam kebijakan.

AWS kebijakan yang dikelola dibuat dan dikelola oleh AWS. Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut.

Kebijakan terkelola pelanggan memberi Anda kontrol halus untuk mengatur akses ke cadangan. AWS Backup Misalnya, Anda dapat menggunakannya untuk memberikan akses administrator cadangan database Anda ke cadangan Amazon RDS tetapi bukan yang Amazon EFS.

Untuk informasi selengkapnya, lihat Kebijakan terkelola di Panduan Pengguna IAM.

AWS kebijakan terkelola

AWS Backup menyediakan kebijakan AWS terkelola berikut untuk kasus penggunaan umum. Kebijakan ini memudahkan Anda menentukan izin yang tepat dan mengontrol akses ke cadangan Anda. Ada dua jenis kebijakan yang dikelola. Satu jenis dirancang untuk ditugaskan kepada pengguna untuk mengontrol akses mereka AWS Backup. Jenis kebijakan terkelola lainnya dirancang untuk dilampirkan pada peran yang Anda berikan AWS Backup. Tabel berikut mencantumkan semua kebijakan terkelola yang AWS Backup menyediakan dan menjelaskan bagaimana kebijakan tersebut didefinisikan. Anda dapat menemukan kebijakan terkelola ini di bagian Kebijakan konsol IAM.

Kebijakan

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

Kebijakan ini memberikan izin bagi pengguna untuk membuat kontrol dan kerangka kerja yang menentukan harapan mereka terhadap AWS Backup sumber daya dan aktivitas, dan untuk mengaudit sumber AWS Backup daya dan aktivitas terhadap kontrol dan kerangka kerja yang ditentukan. Kebijakan ini memberikan izin AWS Config dan layanan serupa untuk menggambarkan harapan pengguna melakukan audit.

Kebijakan ini juga memberikan izin untuk mengirimkan laporan audit ke Amazon S3 dan layanan serupa, dan memungkinkan pengguna untuk menemukan dan membuka laporan audit mereka.

Untuk melihat izin kebijakan ini, lihat AWSBackupAuditAccessdi Referensi Kebijakan AWS Terkelola.

AWSBackupDataTransferAccess

Kebijakan ini memberikan izin untuk API transfer data bidang AWS Backup penyimpanan, yang memungkinkan agen AWS Backint menyelesaikan transfer data cadangan dengan bidang AWS Backup penyimpanan. Anda dapat melampirkan kebijakan ini ke peran yang diasumsikan oleh instans Amazon EC2 yang menjalankan SAP HANA dengan agen Backint.

Untuk melihat izin kebijakan ini, lihat AWSBackupDataTransferAccessdi Referensi Kebijakan AWS Terkelola.

AWSBackupFullAccess

Administrator cadangan memiliki akses penuh ke AWS Backup operasi, termasuk membuat atau mengedit rencana cadangan, menetapkan AWS sumber daya untuk rencana cadangan, dan memulihkan cadangan. Administrator Backup bertanggung jawab untuk menentukan dan menegakkan kepatuhan cadangan dengan mendefinisikan rencana cadangan yang memenuhi persyaratan bisnis dan peraturan organisasi mereka. Administrator cadangan juga memastikan bahwa AWS sumber daya organisasi mereka ditugaskan ke rencana yang sesuai.

Untuk melihat izin kebijakan ini, lihat AWSBackupFullAccessdi Referensi Kebijakan AWS Terkelola.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Untuk melihat izin kebijakan ini, lihat di Referensi Kebijakan AWS Terkelola.

AWSBackupOperatorAccess

Operator Backup adalah pengguna yang bertanggung jawab untuk memastikan sumber daya yang menjadi tanggung jawab mereka didukung dengan benar. Operator cadangan memiliki izin untuk menetapkan AWS sumber daya ke rencana cadangan yang dibuat oleh administrator cadangan. Mereka juga memiliki izin untuk membuat cadangan sesuai permintaan AWS sumber daya mereka dan untuk mengonfigurasi periode retensi cadangan sesuai permintaan. Operator cadangan tidak memiliki izin untuk membuat atau mengedit rencana cadangan atau menghapus cadangan terjadwal setelah dibuat. Operator Backup dapat memulihkan backup. Anda dapat membatasi jenis sumber daya yang dapat ditetapkan oleh operator cadangan ke paket cadangan atau memulihkan dari cadangan. Anda melakukan ini dengan mengizinkan hanya peran layanan tertentu yang akan diteruskan ke AWS Backup yang memiliki izin untuk jenis sumber daya tertentu.

Untuk melihat izin kebijakan ini, lihat AWSBackupOperatorAccessdi Referensi Kebijakan AWS Terkelola.

AWSBackupOrganizationAdminAccess

Administrator organisasi memiliki akses penuh ke AWS Organizations operasi, termasuk membuat, mengedit, atau menghapus kebijakan cadangan, menetapkan kebijakan cadangan ke akun dan unit organisasi, dan memantau aktivitas pencadangan dalam organisasi. Administrator organisasi bertanggung jawab untuk melindungi akun di organisasi mereka dengan mendefinisikan dan menetapkan kebijakan cadangan yang memenuhi persyaratan bisnis dan peraturan organisasi mereka.

Untuk melihat izin kebijakan ini, lihat AWSBackupOrganizationAdminAccessdi Referensi Kebijakan AWS Terkelola.

AWSBackupRestoreAccessForSAPHANA

Kebijakan ini memberikan AWS Backup izin untuk memulihkan cadangan SAP HANA di Amazon EC2.

Untuk melihat izin kebijakan ini, lihat AWSBackupRestoreAccessForSAPHANAdi Referensi Kebijakan AWS Terkelola.

AWSBackupServiceLinkedRolePolicyForBackup

Kebijakan ini dilampirkan pada peran terkait layanan yang diberi nama AWSServiceRoleforBackup AWS Backup untuk memungkinkan AWS layanan panggilan atas nama Anda untuk mengelola cadangan Anda. Untuk informasi selengkapnya, lihat the section called “Backup dan copy”.

Untuk melihat izin kebijakan ini, lihat AWSBackupServiceLinkedRolePolicyforBackupdi Referensi Kebijakan AWS Terkelola.

AWSBackupServiceLinkedRolePolicyForBackupTest

Untuk melihat izin kebijakan ini, lihat AWSBackupServiceLinkedRolePolicyForBackupTestdi Referensi Kebijakan AWS Terkelola.

AWSBackupServiceRolePolicyForBackup

Memberikan AWS Backup izin untuk membuat cadangan semua jenis sumber daya yang didukung atas nama Anda.

Untuk melihat izin kebijakan ini, lihat AWSBackupServiceRolePolicyForBackupdi Referensi Kebijakan AWS Terkelola.

AWSBackupServiceRolePolicyForRestores

Memberikan AWS Backup izin untuk memulihkan cadangan semua jenis sumber daya yang didukung atas nama Anda.

Untuk melihat izin kebijakan ini, lihat AWSBackupServiceRolePolicyForRestoresdi Referensi Kebijakan AWS Terkelola.

Untuk pemulihan instans EC2, Anda juga harus menyertakan izin berikut untuk meluncurkan instans EC2:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
    ]
}
```

AWSBackupServiceRolePolicyForS3Backup

Kebijakan ini berisi izin yang diperlukan AWS Backup untuk mencadangkan bucket S3 apa pun. Ini termasuk akses ke semua objek dalam ember dan AWS KMS kunci terkait.

Untuk melihat izin kebijakan ini, lihat AWSBackupServiceRolePolicyForS3Backupdi Referensi Kebijakan AWS Terkelola.

AWSBackupServiceRolePolicyForS3Restore

Kebijakan ini berisi izin yang diperlukan AWS Backup untuk memulihkan cadangan S3 ke bucket. Ini termasuk izin baca dan tulis ke bucket dan penggunaan AWS KMS kunci apa pun sehubungan dengan operasi S3.

Untuk melihat izin kebijakan ini, lihat AWSBackupServiceRolePolicyForS3Restoredi Referensi Kebijakan AWS Terkelola.

AWSServiceRolePolicyForBackupReports

AWS Backup menggunakan kebijakan ini untuk peran AWSServiceRoleForBackupReportsterkait layanan. Peran terkait layanan ini memberikan AWS Backup izin untuk memantau dan melaporkan kepatuhan pengaturan cadangan, pekerjaan, dan sumber daya Anda dengan kerangka kerja Anda.

Untuk melihat izin kebijakan ini, lihat AWSServiceRolePolicyForBackupReportsdi Referensi Kebijakan AWS Terkelola.

AWSServiceRolePolicyForBackupRestoreTesting

Untuk melihat izin kebijakan ini, lihat AWSServiceRolePolicyForBackupRestoreTestingdi Referensi Kebijakan AWS Terkelola.

Kebijakan yang dikelola pelanggan

Bagian berikut menjelaskan izin cadangan dan pemulihan yang disarankan untuk aplikasi Layanan AWS dan pihak ketiga yang didukung oleh AWS Backup. Anda dapat menggunakan kebijakan AWS terkelola yang ada sebagai model saat membuat dokumen kebijakan sendiri, lalu menyesuaikannya untuk membatasi akses ke AWS sumber daya.

Amazon Aurora

Cadangan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Memulihkan

Mulailah dengan `RDSPermissions` pernyataan dari AWSBackupServiceRolePolicyForRestores.

Amazon DynamoDB

Cadangan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForBackup:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Memulihkan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForRestores:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamoDBRestorePermissions`
- `KMSPermissions`

Amazon EBS

Cadangan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForBackup:

- `EBSResourcePermissions`
- `EBSTagAndDeletePermissions`
- `EBSCopyPermissions`
- `EBSSnapshotTierPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Memulihkan

Mulailah dengan `EBSPermissions` pernyataan dari AWSBackupServiceRolePolicyForRestores.

Tambahkan pernyataan berikut.

```
{
      "Effect":"Allow",
      "Action": [
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
},
```

Amazon EC2

Cadangan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForBackup:

- EBSCopyPermissions
- EC2CopyPermissions
- EC2Permissions
- EC2TagPermissions
- EC2ModifyPermissions
- EBSResourcePermissions
- GetResourcesPermissions
- BackupVaultPermissions

Memulihkan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForRestores:

- EBSPermissions
- EC2DescribePermissions
- EC2RunInstancesPermissions
- EC2TerminateInstancesPermissions
- EC2CreateTagsPermissions

Tambahkan pernyataan berikut.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
```

```
},
```

Amazon EFS

Cadangan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForBackup:

- `EFSPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Memulihkan

Mulailah dengan `EFSPermissions` pernyataan dari AWSBackupServiceRolePolicyForRestores.

Amazon FSx

Cadangan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForBackup:

- `FsxBackupPermissions`
- `FsxCreateBackupPermissions`
- `FsxPermissions`
- `FsxVolumePermissions`
- `FsxListTagsPermissions`
- `FsxDeletePermissions`
- `FsxResourcePermissions`
- `KMSPermissions`

Memulihkan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForRestores:

- `FsxPermissions`
- `FsxTagPermissions`
- `FsxBackupPermissions`

- `FsxDeletePermissions`
- `FsxDescribePermissions`
- `FsxVolumeTagPermissions`
- `FsxBackupTagPermissions`
- `FsxVolumePermissions`
- `DSPermissions`
- `KMSDescribePermissions`

Amazon RDS

Cadangan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Memulihkan

Mulailah dengan `RDSPermissions` pernyataan dari AWSBackupServiceRolePolicyForRestores.

Amazon S3

Cadangan

Mulailah dengan AWSBackupServiceRolePolicyForS3Backup.

Tambahkan `BackupVaultPermissions` dan `BackupVaultCopyPermissions` pernyataan jika Anda perlu menyalin cadangan ke akun lain.

Memulihkan

Mulailah dengan AWSBackupServiceRolePolicyForS3Restore.

AWS Storage Gateway

Cadangan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForBackup:

- `StorageGatewayPermissions`
- `EBSTagAndDeletePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Tambahkan pernyataan berikut.

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
},
```

Memulihkan

Mulailah dengan pernyataan berikut dari AWSBackupServiceRolePolicyForRestores:

- `StorageGatewayVolumePermissions`
- `StorageGatewayGatewayPermissions`
- `StorageGatewayListPermissions`

Mesin virtual

Cadangan

Mulailah dengan `BackupGatewayBackupPermissions` pernyataan dari AWSBackupServiceRolePolicyForBackup.

Memulihkan

Mulailah dengan `GatewayRestorePermissions` pernyataan dari AWSBackupServiceRolePolicyForRestores.

Cadangan terenkripsi

Untuk memulihkan cadangan terenkripsi, lakukan salah satu hal berikut

- Tambahkan peran Anda ke daftar yang diizinkan untuk kebijakan AWS KMS kunci
- Tambahkan pernyataan berikut dari peran IAM Anda AWSBackupServiceRolePolicyForRestoresuntuk pemulihan:
  - `KMSDescribePermissions`
  - `KMSPermissions`
  - `KMSCreateGrantPermissions`

Pembaruan kebijakan untuk AWS Backup

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Backup sejak layanan ini mulai melacak perubahan ini.

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForBackup — Permbaruan ke kebijakan yang sudah ada	AWS Backup menambahkan izin `backup:TagResource` untuk kebijakan ini. Izin diperlukan untuk mendapatkan izin penandaan selama pembuatan titik pemulihan.	17 Mei 2024
AWSBackupServiceRolePolicyForS3Backup – Pembaruan ke kebijakan yang ada	AWS Backup menambahkan izin `backup:TagResource` untuk kebijakan ini. Izin diperlukan untuk mendapatkan izin penandaan selama pembuatan titik pemulihan.	17 Mei 2024

Perubahan	Deskripsi	Tanggal
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	AWS Backup menambahkan izin `backup:TagResource` untuk kebijakan ini. Izin diperlukan untuk mendapatkan izin penandaan selama pembuatan titik pemulihan.	17 Mei 2024
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin`rds:DeleteDBInstanceAutomatedBackups` . Izin ini diperlukan AWS Backup untuk mendukung pencadangan berkelanjutan dan point-in-time-restore instans Amazon RDS.	1 Mei 2024
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	AWS Backup memperbarui Amazon Resource Name (ARN) dengan izin `storagegateway:ListVolumes` dari `arn:aws:storagegateway:*:*:gateway/*` to untuk mengakomodasi perubahan * dalam model Storage Gateway API.	1 Mei 2024

Perubahan	Deskripsi	Tanggal
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	AWS Backup memperbarui Amazon Resource Name (ARN) dengan izin `storagegateway:ListVolumes` dari `arn:aws:storagegateway:*:*:gateway/*` to untuk mengakomodasi perubahan * dalam model Storage Gateway API.	1 Mei 2024

Perubahan	Deskripsi	Tanggal
AWSServiceRolePolicyForBackupRestoreTesting – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk menjelaskan dan mencantumkan titik pemulihan dan sumber daya yang dilindungi untuk melakukan rencana pengujian pemulihan :`backup:DescribeRecoveryPoint` ,, `backup:DescribeProtectedResource` `backup:ListProtectedResources` , dan`backup:ListRecoveryPointsByResource` . Menambahkan izin `ec2:DescribeSnapshotTierStatus` untuk mendukung penyimpanan tingkat arsip Amazon EBS. Menambahkan izin `rds:DescribeDBClusterAutomatedBackups` untuk mendukung pencadangan berkelanjutan Amazon Aurora. Menambahkan izin berikut untuk mendukung pengujian pemulihan cadangan `redshift:DescribeClusters` Amazon Redshift: dan. `redshift:DeleteCluster`	Februari 14, 2024

Perubahan	Deskripsi	Tanggal
	Menambahkan izin `timestream:DeleteTable` untuk mendukung pengujian pemulihan cadangan Amazon Timestream.	
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan izin `ec2:DescribeSnapshotTierStatus` dan `ec2:RestoreSnapshotTier` . Izin ini diperlukan bagi pengguna untuk memiliki opsi untuk memulihkan sumber daya Amazon EBS yang disimpan AWS Backup dari penyimpanan arsip. Untuk pemulihan instans EC2, Anda juga harus menyertakan izin seperti yang ditunjukkan dalam pernyataan kebijakan berikut untuk meluncurkan instans EC2:	27 November 2023

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin `ec2:DescribeSnapshotTierStatus` dan `ec2:ModifySnapshotTier` untuk mendukung opsi penyimpanan tambahan untuk sumber daya Amazon EBS yang dicadangkan untuk dialihkan ke tingkat penyimpanan arsip. Izin ini diperlukan bagi pengguna untuk memiliki opsi untuk mentransisikan sumber daya Amazon EBS yang disimpan AWS Backup ke penyimpanan arsip.	27 November 2023

Perubahan	Deskripsi	Tanggal
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin `ec2:DescribeSnapshotTierStatus` dan `ec2:ModifySnapshotTier` untuk mendukung opsi penyimpanan tambahan untuk sumber daya Amazon EBS yang dicadangkan untuk dialihkan ke tingkat penyimpanan arsip. Izin ini diperlukan bagi pengguna untuk memiliki opsi untuk mentransisikan sumber daya Amazon EBS yang disimpan AWS Backup ke penyimpanan arsip. Menambahkan izin `rds:DescribeDBClusterSnapshots` dan`rds:RestoreDBClusterToPointInTime` , yang diperlukan untuk PITR (point-in-time mengembalikan) cluster Aurora.	

Perubahan	Deskripsi	Tanggal
AWSServiceRolePolicyForBackupRestoreTesting – Kebijakan baru	Memberikan izin yang diperlukan untuk melakukan pengujian pemulihan. Izin termasuk tindakan `list, read, and write` untuk layanan berikut yang akan disertakan dalam tes pemulihan: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx for Lustre, fsX untuk Windows File Server, fsX untuk ONTAP, FSx untuk OpenZx FS, Amazon Neptunus, Amazon RDS, dan Amazon S3.	27 November 2023
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan `restore-testing.backup.amazonaws.com` ke `IamPassRolePermissions` dan `IamCreateServiceLinkedRolePermissions` . Penambahan ini diperlukan AWS Backup untuk melakukan tes pemulihan atas nama pelanggan.	27 November 2023

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan izin `rds:DescribeDBClusterSnapshots` dan`rds:RestoreDBClusterToPointInTime` , yang diperlukan untuk PITR (point-in-time mengembalikan) cluster Aurora.	September 6, 2023
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin`rds:DescribeDBClusterAutomatedBackups` , yang diperlukan untuk pencadangan terus menerus dan point-in-time pemulihan cluster Aurora.	September 6, 2023
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin`rds:DescribeDBClusterAutomatedBackups` , yang diperlukan untuk pencadangan terus menerus dan point-in-time pemulihan cluster Aurora.	September 6, 2023

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin`rds:DescribeDBClusterAutomatedBackups` . Izin ini diperlukan untuk AWS Backup mendukung pencadangan berkelanjutan dan point-in-time pemulihan cluster Aurora. Menambahkan izin `rds:DeleteDBClusterAutomatedBackups` untuk mengizinkan AWS Backup siklus hidup menghapus dan memisahkan titik pemulihan berkelanjutan Amazon Aurora saat periode retensi selesai. Izin ini diperlukan untuk titik pemulihan Aurora untuk menghindari transisi ke suatu `EXIPIRED` keadaan. Menambahkan izin `rds:ModifyDBCluster` yang memungkinkan AWS Backup untuk berinteraksi dengan cluster Aurora. Penambahan ini memungkinkan pengguna kemampuan untuk mengaktifkan atau menonaktifkan pencadangan berkelanjutan berdasarkan konfigurasi yang diinginkan.	September 6, 2023

Perubahan	Deskripsi	Tanggal
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan tindakan `ram:GetResourceShareAssociations` untuk memberikan izin pengguna untuk mendapatkan asosiasi berbagi sumber daya untuk jenis vault baru.	8 Agustus 2023
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menambahkan tindakan `ram:GetResourceShareAssociations` untuk memberikan izin pengguna untuk mendapatkan asosiasi berbagi sumber daya untuk jenis vault baru.	8 Agustus 2023
AWSBackupServiceRolePolicyForS3Backup – Pembaruan ke kebijakan yang ada	Menambahkan izin `s3:PutInventoryConfiguration` untuk meningkatkan kecepatan kinerja pencadangan dengan menggunakan inventaris bucket.	1 Agustus 2023

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan tindakan berikut untuk memberikan izin pengguna untuk menambahkan tag untuk memulihkan sumber daya:`storagegateway:AddTagsToResource` ,`elasticfilesystem:TagResource` , `ec2:CreateTags` hanya `ec2:CreateAction` yang mencakup salah satu `RunInstances` atau`CreateVolume` ,`fsx:TagResource` , `dancloudformation:TagResource` .	22 Mei 2023
AWSBackupAuditAccess – Pembaruan ke kebijakan yang ada	Mengganti pemilihan sumber daya dalam API `config:DescribeComplianceByConfigRule` dengan sumber daya wildcard untuk memudahkan pengguna memilih sumber daya.	11 April 2023
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk memulihkan Amazon EFS menggunakan kunci terkelola pelanggan :`kms:GenerateDataKeyWithoutPlaintext` . Ini membantu memastikan pengguna memiliki izin yang diperlukan untuk memulihkan sumber daya Amazon EFS.	Maret 27, 2023

Perubahan	Deskripsi	Tanggal
AWSServiceRolePolicyForBackupReports – Pembaruan ke kebijakan yang ada	Memperbarui `config:DescribeConfigRules` dan `config:DescribeConfigRuleEvaluationStatus` tindakan untuk memungkinkan AWS Backup Audit Manager mengakses aturan yang dikelola Manajer AWS Backup AWS Config Audit.	9 Maret 2023
AWSBackupServiceRolePolicyForS3Restore – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut:`kms:Decrypt` ,`s3:PutBucketOwnershipControls` , dan `s3:GetBucketOwnershipControls` ke kebijakan `AWSBackupServiceRolePolicyForS3Restore` . Izin ini diperlukan untuk mendukung pemulihan objek saat enkripsi KMS digunakan dalam cadangan asli dan untuk memulihkan objek saat kepemilikan objek dikonfigurasi pada bucket asli, bukan ACL.	13 Februari 2023

Perubahan	Deskripsi	Tanggal
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk menjadwalkan pencadangan menggunakan tag VMware dari mesin virtual dan untuk mendukung pembatasan bandwidth berbasis jadwal:,,,,,, dan. `backup-gateway:GetHypervisorPropertyMappings backup-gateway:GetVirtualMachine backup-gateway:PutHypervisorPropertyMappings backup-gateway:GetHypervisor backup-gateway:StartVirtualMachinesMetadataSync backup-gateway:GetBandwidthRateLimitSchedule backup-gateway:PutBandwidthRateLimitSchedule`	Desember 15, 2022

Perubahan	Deskripsi	Tanggal
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk menjadwalkan pencadangan menggunakan tag VMware dari mesin virtual dan untuk mendukung pembatasan bandwidth berbasis jadwal:,,, dan. `backup-gateway:GetHypervisorPropertyMappings backup-gateway:GetVirtualMachine backup-gateway:GetHypervisor backup-gateway:GetBandwidthRateLimitSchedule`	Desember 15, 2022
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync – Kebijakan baru	Memberikan izin bagi AWS Backup Gateway untuk menyinkronkan metadata mesin virtual di jaringan on-premise dengan Backup Gateway.	Desember 15, 2022

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung pekerjaan cadangan Timestrea m:`timestream:StartAwsBackupJob` ,,`timestream:GetAwsBackupStatus` ,,`timestream:ListTables` ,`timestream:ListDatabases` , `timestream:ListTagsForResource` `timestream:DescribeTable` `timestream:DescribeDatabase` , dan. `timestream:DescribeEndpoints`	13 Desember 2022

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung pekerjaan pemulihan Timestream:`timestream:StartAwsRestoreJob` ,,`timestream:GetAwsRestoreStatus` ,`timestream:ListTables` ,`timestream:ListTagsForResource` ,`timestream:ListDatabases` , `timestream:DescribeTable` `timestream:DescribeDatabase` `s3:GetBucketAcl` , dan. `timestream:DescribeEndpoints`	13 Desember 2022
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung sumber daya Timestream:`timestream:ListTables` ,`timestream:ListDatabases` , `s3:ListAllMyBuckets` dan. `timestream:DescribeEndpoints`	13 Desember 2022

Perubahan	Deskripsi	Tanggal
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung sumber daya Timestream:`timestream:ListDatabases` ,, `timestream:ListTables` `s3:ListAllMyBuckets` , dan. `timestream:DescribeEndpoints`	13 Desember 2022
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung sumber daya Timestream:`timestream:ListDatabases` ,,`timestream:ListTables` ,`timestream:ListTagsForResource` ,`timestream:DescribeDatabase` ,, `timestream:DescribeTable` `timestream:GetAwsBackupStatus` `timestream:GetAwsRestoreStatus` , dan. `timestream:DescribeEndpoints`	13 Desember 2022

Perubahan	Deskripsi	Tanggal
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung sumber daya Amazon Redshift`redshift:DescribeClusters` :`redshift:DescribeClusterSubnetGroups` ,,,`redshift:DescribeNodeConfigurationOptions` ,`redshift:DescribeOrderableClusterOptions` , `redshift:DescribeClusterParameterGroups` `redshift:DescribeClusterTracks` `redshift:DescribeSnapshotSchedules` , dan. `ec2:DescribeAddresses`	27 November 2022

Perubahan	Deskripsi	Tanggal
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung sumber daya Amazon Redshiftredshift: DescribeC lusters :redshift: DescribeClusterSub netGroups ,,,, redshift:DescribeN odeConfigurationOp tions redshift: DescribeO rderableClusterOpt ions ,redshift: DescribeClusterPar ameterGroups, . redshift:DescribeC lusterTracks redshift:DescribeS napshotSchedules , danec2:DescribeAddres ses .	27 November 2022

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung pekerjaan pemulihan Amazon Redshift`redshift:RestoreFromClusterSnapshot`:`redshift:RestoreTableFromClusterSnapshot` ,,`redshift:DescribeClusters` , dan. `redshift:DescribeTableRestoreStatus`	27 November 2022
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung pekerjaan pencadangan Amazon Redshift`redshift:CreateClusterSnapshot` :`redshift:DescribeClusterSnapshots` ,,,, `redshift:DescribeTags` `redshift:DeleteClusterSnapshot` `redshift:DescribeClusters` , dan. `redshift:CreateTags`	27 November 2022
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung CloudFormation sumber daya:`cloudformation:ListStacks` .	27 November 2022

Perubahan	Deskripsi	Tanggal
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung CloudFormation sumber daya:`cloudformation:ListStacks` .	27 November 2022
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung CloudFormation sumber daya:`redshift:DescribeClusterSnapshots` ,, `redshift:DescribeTags` `redshift:DeleteClusterSnapshot` , dan`redshift:DescribeClusters` .	27 November 2022
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung pekerjaan cadangan tumpukan AWS CloudFormation aplikasi: `cloudformation:GetTemplate` ,`cloudformation:DescribeStacks` , dan`cloudformation:ListStackResources` .	16 November 2022

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung pekerjaan pencadangan tumpukan AWS CloudFormation aplikasi: `cloudformation:CreateChangeSet` dan `cloudformation:DescribeChangeSet`	16 November 2022
AWSBackupOrganizationAdminAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut ke kebijakan ini untuk mengizinkan administrator organisasi menggunakan fitur Administrator Delegasi:,, dan `organizations:ListDelegatedAdministrator organizations:RegisterDelegatedAdministrator organizations:DeregisterDelegatedAdministrator`	27 November 2022
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung SAP HANA di instans Amazon EC2`ssm-sap:GetOperation` :`ssm-sap:ListDatabases` ,,,,`ssm-sap:BackupDatabase` , `ssm-sap:UpdateHanaBackupSettings` dan. `ssm-sap:GetDatabase ssm-sap:ListTagsForResource`	November 20, 2022

Perubahan	Deskripsi	Tanggal
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung SAP HANA di instans Amazon EC2`ssm-sap:GetOperation` `:ssm-sap:ListDatabases` ,,, dan. `ssm-sap:GetDatabase` `ssm-sap:ListTagsForResource`	November 20, 2022
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung SAP HANA di instans Amazon EC2`ssm-sap:GetOperation` `:ssm-sap:ListDatabases` ,,, dan. `ssm-sap:GetDatabase` `ssm-sap:ListTagsForResource`	November 20, 2022
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung SAP HANA di instans Amazon EC2:. `ssm-sap:GetOperation`	November 20, 2022
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung pekerjaan pemulihan gateway Backup ke instans EC2:`ec2:CreateTags` .	November 20, 2022

Perubahan	Deskripsi	Tanggal
AWSBackupDataTransferAccess – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut untuk mendukung transfer data penyimpanan aman untuk sumber daya SAP HANA Di Amazon EC2`backup-storage:StartObject` :`backup-storage:PutChunk` ,,,, `backup-storage:GetChunk` `backup-storage:ListChunks` `backup-storage:ListObjects` , `backup-storage:GetObjectMetadata` dan. `backup-storage:NotifyObjectComplete`	November 20, 2022

Perubahan	Deskripsi	Tanggal
AWSBackupRestoreAccessForSAPHANA – Pembaruan ke kebijakan yang ada	Menambahkan izin berikut bagi pemilik sumber daya untuk melakukan pemulihan sumber daya SAP HANA Di Amazon EC2`backup:Get*` :`backup:List*` ,,,,,,,`backup:Describe*` ,`backup:StartBackupJob` ,`backup:StartRestoreJob` ,`ssm-sap:GetOperation` ,`ssm-sap:ListDatabases` ,, `ssm-sap:BackupDatabase` `ssm-sap:RestoreDatabase` `ssm-sap:UpdateHanaBackupSettings` , `ssm-sap:GetDatabase` dan. `ssm-sap:ListTagsForResource`	November 20, 2022
AWSBackupServiceRolePolicyForS3Backup – Pembaruan ke kebijakan yang ada	Menambahkan izin `s3:GetBucketAcl` untuk mendukung operasi pencadangan AWS Backup untuk Amazon S3.	Agustus 24, 2022

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan tindakan berikut untuk memberikan akses untuk membuat instance database untuk mendukung fungsionalitas Multi-availability Zone (Multi-AZ):. `rds:CreateDBInstance`	20 Juli 2022
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan `s3:GetBucketTagging` izin untuk memberikan izin kepada pengguna untuk memilih bucket yang akan dicadangkan dengan wildcard sumber daya. Tanpa izin ini, pengguna yang memilih bucket mana yang akan dicadangkan dengan wildcard sumber daya tidak berhasil.	6 Mei 2022
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan sumber daya volume dalam lingkup yang ada `fsx:CreateBackup` dan `fsx:ListTagsForResource` tindakan, dan menambahkan tindakan baru `fsx:DescribeVolumes` untuk mendukung fsX untuk cadangan tingkat volume ONTAP.	27 April 2022

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan tindakan berikut untuk memberikan izin pengguna untuk memulihkan fsX untuk `fsx:DescribeVolumes` volume ONTAP`fsx:CreateVolumeFromBackup` ,,, `fsx:DeleteVolume` dan. `fsx:UntagResource`	27 April 2022
AWSBackupServiceRolePolicyForS3Backup – Pembaruan ke kebijakan yang ada	Menambahkan tindakan berikut untuk memberikan izin pengguna untuk menerima pemberitahuan perubahan pada bucket Amazon S3 mereka selama operasi pencadangan: dan. `s3:GetBucketNotification` `s3:PutBucketNotification`	25 Februari 2022

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForS3Backup – Kebijakan baru	Menambahkan tindakan berikut untuk memberikan izin pengguna untuk mencadangkan bucket Amazon S3 merekas3:GetInventoryConfiguration :s3:PutInventoryConfiguration ,,,,,s3:ListBucketVersions ,s3:ListBucket , s3:GetBucketTagging s3:GetBucketVersioning , s3:GetBucketNotification dan s3:GetBucketLocation s3:ListAllMyBuckets Menambahkan tindakan berikut untuk memberikan izin pengguna untuk mencadangkan objek Amazon S3 merekas3:GetObject :s3GetObjectAcl ,,,, s3:GetObjectVersionTagging s3:GetObjectVersionAcl s3:GetObjectTagging , dan. s3:GetObjectVersion Menambahkan tindakan berikut untuk memberikan izin pengguna untuk mencadangkan data Amazon S3 terenkrip	Februari 17, 2022

Perubahan	Deskripsi	Tanggal
	si mereka: dan. `kms:Decrypt` `kms:DescribeKey` Menambahkan tindakan berikut untuk memberikan izin pengguna untuk mengambil cadangan tambahan data Amazon S3 mereka menggunakan EventBridge aturan Amazon:,, ,`events:DescribeRule` ,,,,,,,,`events:EnableRule` ,, `events:PutRule` `events:DeleteRule` `events:PutTargets` , `events:RemoveTargets` dan. `events:ListTargetsByRule` `events:DisableRule` `cloudwatch:GetMetricData` `events:ListRules`	

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForS3Restore – Kebijakan baru	Menambahkan tindakan berikut untuk memberikan izin pengguna untuk memulihkan bucket Amazon S3 merekas3:CreateBucket :s3:ListBucketVersions ,,,, s3:ListBucket s3:GetBucketVersioning , s3:GetBucketLocation dan. s3:PutBucketVersioning Menambahkan tindakan berikut untuk memberikan izin pengguna untuk memulihkan bucket Amazon S3 merekas3:GetObject :s3:GetObjectVersion ,,,,,s3:DeleteObject ,s3:PutObjectVersionAcl ,s3:GetObjectVersionAcl ,s3:GetObjectTagging , s3:PutObjectTagging s3:GetObjectAcl s3:PutObjectAcl , s3:PutObject dan. s3:ListMultipartUploadParts	Februari 17, 2022

Perubahan	Deskripsi	Tanggal
	Menambahkan tindakan berikut untuk memberikan izin pengguna untuk mengenkripsi data Amazon S3 yang dipulihkan`kms:Decrypt` :`kms:DescribeKey` ,, dan. `kms:GenerateDataKey`	
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Ditambahkan `s3:ListAllMyBuckets` untuk memberikan izin pengguna untuk melihat daftar bucket mereka dan memilih mana yang akan ditetapkan ke paket cadangan.	14 Februari 2022
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Ditambahkan `backup-gateway:ListVirtualMachines` untuk memberikan izin pengguna untuk melihat daftar mesin virtual mereka dan memilih mana yang akan ditetapkan ke paket cadangan. Ditambahkan `backup-gateway:ListTagsForResource` untuk memberikan izin pengguna untuk daftar tag untuk mesin virtual mereka.	30 November 2021

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Ditambahkan `backup-gateway:Backup` untuk memberikan izin pengguna mengembalikan cadangan mesin virtual mereka. AWS Backup juga ditambahkan `backup-gateway:ListTagsForResource` untuk memberikan izin pengguna untuk mencantumkan tag yang ditetapkan ke cadangan mesin virtual mereka.	30 November 2021
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Ditambahkan `backup-gateway:Restore` untuk memberikan izin pengguna mengembalikan cadangan mesin virtual mereka.	30 November 2021

Perubahan	Deskripsi	Tanggal
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Menambahkan tindakan berikut untuk memberikan izin kepada pengguna untuk menggunakan AWS Backup Gateway untuk membuat cadangan, memulihkan, dan mengelola mesin virtual mereka:,, ,,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:Tes	30 November 2021

Perubahan	Deskripsi	Tanggal
	`tHypervisorConfigu ration` ,`backup-ga teway:UntagResourc e` ,`backup-gateway:Upd ateGatewayInformat ion` , dan`backup-ga teway:UpdateHyperv isor` .	
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menambahkan tindakan berikut untuk memberika n izin pengguna untuk mencadangkan mesin virtual mereka:`backup-ga teway:ListGateways` ,, `backup-gateway:Lis tHypervisors` `backup-gateway:ListTagsForR esource` , dan`backup-ga teway:ListVirtualM achines` .	30 November 2021
AWSBackupServiceLi nkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Ditambahkan `dynamodb:ListTagsOfResource` untuk memberikan izin pengguna untuk mencantum kan tag tabel DynamoDB mereka untuk dicadangkan menggunakan fitur cadangan AWS Backup DynamoDB lanjutan.	23 November 2021

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Ditambahkan `dynamodb:StartAwsBackupJob` untuk memberikan izin pengguna untuk mencadangkan tabel DynamoDB mereka menggunakan fitur cadangan lanjutan. Ditambahkan `dynamodb:ListTagsOfResource` untuk memberikan pengguna izin untuk menyalin tag dari tabel DynamoDB sumber mereka ke backup mereka.	23 November 2021
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Ditambahkan `dynamodb:RestoreTableFromAwsBackup` untuk memberikan izin pengguna mengembalikan tabel DynamoDB mereka yang dicadangkan menggunakan fitur cadangan lanjutan AWS Backup DynamoDB lanjutan.	23 November 2021
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Ditambahkan `dynamodb:RestoreTableFromAwsBackup` untuk memberikan izin pengguna mengembalikan tabel DynamoDB mereka yang dicadangkan menggunakan fitur cadangan lanjutan AWS Backup DynamoDB lanjutan.	23 November 2021

Perubahan	Deskripsi	Tanggal
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menghapus tindakan `backup:GetRecoveryPointRestoreMetadata` dan `rds:DescribeDBSnapshots` karena mereka berlebihan. AWS Backup tidak membutuhkan keduanya `backup:GetRecoveryPointRestoreMetadata` dan `backup:Get*` sebagai bagian dari`AWSBackupOperatorAccess` . Juga, AWS Backup tidak membutuhkan keduanya `rds:DescribeDBSnapshots` dan `rds:describeDBSnapshots` sebagai bagian dari`AWSBackupOperatorAccess` .	23 November 2021

Perubahan	Deskripsi	Tanggal
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan tindakan `baruelasticfilesystem:DescribeFileSystems` ,`dynamodb:ListTables` ,`storagegateway:ListVolumes` ,`ec2:DescribeVolumes` ,`ec2:DescribeInstances` ,`rds:DescribeDBInstances` ,`rds:DescribeDBClusters` ,, dan `fsx:DescribeFileSystems` untuk memungkinkan pelanggan melihat dan memilih dari daftar sumber daya yang AWS Backup didukung saat memilih sumber daya mana yang akan ditetapkan ke rencana cadangan.	November 10, 2021
AWSBackupAuditAccess – Kebijakan baru	Ditambahkan `AWSBackupAuditAccess` untuk memberikan izin pengguna untuk menggunakan AWS Backup Audit Manager. Izin mencakup kemampuan untuk mengonfigurasi kerangka kerja kepatuhan dan menghasilkan laporan.	Agustus 24, 2021

Perubahan	Deskripsi	Tanggal
AWSServiceRolePolicyForBackupReports – Kebijakan baru	Ditambahkan `AWSServiceRolePolicyForBackupReports` untuk memberikan izin untuk peran terkait layanan untuk mengotomatiskan pemantauan pengaturan cadangan, pekerjaan, dan sumber daya untuk kepatuhan dengan kerangka kerja yang dikonfigurasi oleh pengguna.	Agustus 24, 2021
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Ditambahkan `iam:CreateServiceLinkedRole` untuk membuat peran terkait layanan (dengan upaya terbaik) untuk mengotomatiskan penghapusan titik pemulihan yang kedaluwarsa untuk Anda. Tanpa peran terkait layanan ini, AWS Backup tidak dapat menghapus titik pemulihan yang kedaluwarsa setelah pelanggan menghapus peran IAM asli yang mereka gunakan untuk membuat titik pemulihan mereka.	Juli 5, 2021

Perubahan	Deskripsi	Tanggal
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan tindakan baru `dynamodb:DeleteBackup` untuk memberikan `DeleteRecoveryPoint` izin untuk mengotomatiskan penghapusan titik pemulihan DynamoDB yang kedaluwarsa berdasarkan pengaturan siklus hidup rencana cadangan Anda.	Juli 5, 2021
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menghapus tindakan `backup:GetRecoveryPointRestoreMetadata` dan `rds:DescribeDBSnapshots` karena mereka berlebihan. AWS Backup tidak membutuhkan keduanya `backup:GetRecoveryPointRestoreMetadata` dan `backup:Get*` sebagai bagian dari `AWSBackupOperatorAccess` Juga, AWS Backup tidak membutuhkan keduanya `rds:DescribeDBSnapshots` dan `rds:describeDBSnapshots` sebagai bagian dari `AWSBackupOperatorAccess`	25 Mei 2021

Perubahan	Deskripsi	Tanggal
AWSBackupOperatorAccess – Pembaruan ke kebijakan yang ada	Menghapus tindakan `backup:GetRecoveryPointRestoreMetadata` dan `rds:DescribeDBSnapshots` karena mereka berlebihan. AWS Backup tidak membutuhkan keduanya `backup:GetRecoveryPointRestoreMetadata` dan `backup:Get*` sebagai bagian dari`AWSBackupOperatorAccess` . Juga, AWS Backup tidak membutuhkan keduanya `rds:DescribeDBSnapshots` dan `rds:describeDBSnapshots` sebagai bagian dari`AWSBackupOperatorAccess` .	25 Mei 2021
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan tindakan baru `fsx:TagResource` untuk memberikan `StartRestoreJob` izin agar Anda dapat menerapkan tag ke sistem file Amazon FSx selama proses pemulihan.	24 Mei 2021

Perubahan	Deskripsi	Tanggal
AWSBackupServiceRolePolicyForRestores – Pembaruan ke kebijakan yang ada	Menambahkan tindakan baru `ec2:DescribeImages` dan `ec2:DescribeInstances` memberikan `StartRestoreJob` izin untuk memungkinkan Anda memulihkan instans Amazon EC2 dari titik pemulihan.	24 Mei 2021
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan tindakan baru `fsx:CopyBackup` untuk memberikan `StartCopyJob` izin agar Anda dapat menyalin titik pemulihan Amazon FSx di seluruh Wilayah dan akun.	12 April 2021
AWSBackupServiceLinkedRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Menambahkan tindakan baru `fsx:CopyBackup` untuk memberikan `StartCopyJob` izin agar Anda dapat menyalin titik pemulihan Amazon FSx di seluruh Wilayah dan akun.	12 April 2021
AWSBackupServiceRolePolicyForBackup – Pembaruan ke kebijakan yang ada	Diperbarui untuk memenuhi persyaratan berikut: AWS Backup Untuk membuat cadangan tabel DynamoDB terenkripsi, Anda harus menambahkan izin `kms:Decrypt` dan peran IAM yang digunakan `kms:GenerateDataKey` untuk cadangan.	10 Maret 2021

Perubahan	Deskripsi	Tanggal
AWSBackupFullAccess – Pembaruan ke kebijakan yang ada	Diperbarui untuk memenuhi persyaratan berikut: Untuk digunakan AWS Backup untuk mengonfigurasi pencadangan berkelanjutan untuk database Amazon RDS Anda, verifikasi izin API yang `rds:ModifyDBInstance` ada dalam peran IAM yang ditentukan oleh konfigurasi paket Backup Anda. Untuk memulihkan backup berkelanjutan Amazon RDS, Anda harus menambahkan izin `rds:RestoreDBInstanceToPointInTime` ke peran IAM yang Anda kirimkan untuk pekerjaan pemulihan. Di AWS Backup konsol, untuk menjelaskan rentang waktu yang tersedia untuk point-in-time pemulihan, Anda harus menyertakan izin `rds:DescribeDBInstanceAutomatedBackups` API dalam kebijakan yang dikelola IAM.	10 Maret 2021
AWS Backup mulai melacak perubahan	AWS Backup mulai melacak perubahan untuk kebijakan AWS-managed nya.	10 Maret 2021

Menggunakan peran terkait layanan untuk AWS Backup

AWS Backup menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Backup Peran terkait layanan telah ditentukan sebelumnya oleh AWS Backup dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Topik

Menggunakan peran untuk membuat cadangan dan menyalin

AWS Backup menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Backup Peran terkait layanan telah ditentukan sebelumnya oleh AWS Backup dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Backup lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Backup mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Backup dapat mengambil perannya. Izin-izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini melindungi AWS Backup sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AWS Backup

AWS Backup menggunakan peran terkait layanan bernama AWSServiceRoleForBackup—Menyediakan AWS Backup izin untuk mencantumkan sumber daya yang dapat Anda cadangkan dan menyalin cadangan.

AWS Backup juga menggunakan peran untuk menghapus semua cadangan untuk semua jenis sumber daya kecuali untuk Amazon EC2.

Peran AWSServiceRoleForBackup terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `backup.amazonaws.com`

Untuk melihat izin kebijakan ini, lihat AWSBackupServiceLinkedRolePolicyforBackupdi Referensi Kebijakan AWS Terkelola.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Membuat peran yang terhubung dengan layanan untuk AWS Backup

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mencantumkan sumber daya untuk dicadangkan, menyiapkan cadangan lintas akun, atau melakukan pencadangan di, API AWS Management Console, atau AWS API AWS CLI, akan AWS Backup menciptakan peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran Baru yang Muncul di Akun IAM Saya.

Jika Anda menghapus peran yang terhubung dengan layanan ini, lalu ingin membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut di akun Anda. Saat Anda mencantumkan sumber daya untuk dicadangkan, menyiapkan cadangan lintas akun, atau melakukan pencadangan, AWS Backup buat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk AWS Backup

AWS Backup tidak memungkinkan Anda untuk mengedit peran AWSServiceRoleForBackup terkait layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit

penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Backup

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, kami menyarankan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan dan tidak dipantau atau dipelihara secara aktif. Namun, Anda harus membersihkan peran tertaut layanan terlebih dahulu sebelum dapat menghapusnya secara manual.

Membersihkan peran tertaut-layanan

Sebelum dapat menggunakan IAM untuk menghapus peran tertaut-layanan, Anda harus terlebih dahulu menghapus semua sumber daya yang digunakan oleh peran tersebut. Pertama, Anda harus menghapus semua titik pemulihan Anda. Kemudian, Anda harus menghapus semua brankas cadangan Anda.

> **Note**
>
> Jika AWS Backup layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika itu terjadi, tunggu beberapa menit, lalu coba operasi lagi.

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRoleForBackup (konsol)

1. Untuk menghapus semua titik pemulihan dan brankas cadangan (kecuali brankas default Anda), ikuti prosedur di Menghapus brankas cadangan.
2. Untuk menghapus vault default Anda, gunakan perintah berikut di AWS CLI:

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

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRoleForBackup (AWS CLI)

1. Untuk menghapus semua titik pemulihan Anda, gunakan delete-recovery-point.
2. Untuk menghapus semua brankas cadangan Anda, gunakan. `delete-backup-vault`

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRoleForBackup (API)

1. Untuk menghapus semua titik pemulihan Anda, gunakan`DeleteRecoveryPoint`.
2. Untuk menghapus semua brankas cadangan Anda, gunakan. `DeleteBackupVault`

Menghapus peran tertaut layanan secara manual

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForBackup terkait layanan. Untuk informasi lebih lanjut, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Wilayah yang didukung untuk peran yang terhubung dengan layanan AWS Backup

AWS Backup mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat fitur dan Wilayah yang AWS Backup didukung.

Menggunakan peran untuk AWS Backup Audit Manager

AWS Backup menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Backup Peran terkait layanan telah ditentukan sebelumnya oleh AWS Backup dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Backup lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Backup mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Backup dapat mengambil perannya. Izin-izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini melindungi AWS Backup sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AWS Backup

AWS Backup menggunakan peran terkait layanan bernama AWSServiceRoleForBackupReports—Menyediakan AWS Backup izin untuk membuat kontrol, kerangka kerja, dan laporan.

Peran AWSServiceRoleForBackupReports terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `backup.amazonaws.com`

Untuk melihat izin kebijakan ini, lihat AWSServiceRolePolicyForBackupReportsdi Referensi Kebijakan AWS Terkelola.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Membuat peran yang terhubung dengan layanan untuk AWS Backup

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat kerangka kerja atau rencana laporan di AWS Management Console, API AWS CLI, atau AWS API, akan AWS Backup membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran Baru yang Muncul di Akun IAM Saya.

Jika Anda menghapus peran yang terhubung dengan layanan ini, lalu ingin membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut di akun Anda. Saat Anda membuat kerangka kerja atau rencana laporan, AWS Backup buat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk AWS Backup

AWS Backup tidak memungkinkan Anda untuk mengedit peran AWSServiceRoleForBackupReports terkait layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat

mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Backup

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, kami menyarankan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan dan tidak dipantau atau dipelihara secara aktif. Namun, Anda harus membersihkan peran tertaut layanan terlebih dahulu sebelum dapat menghapusnya secara manual.

Membersihkan peran tertaut-layanan

Sebelum dapat menggunakan IAM untuk menghapus peran tertaut-layanan, Anda harus terlebih dahulu menghapus semua sumber daya yang digunakan oleh peran tersebut. Anda harus menghapus semua kerangka kerja dan rencana laporan.

> **Note**
>
> Jika AWS Backup layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika itu terjadi, tunggu beberapa menit, lalu coba operasi lagi.

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRoleForBackupReports (konsol)

1. Untuk menghapus semua kerangka kerja, lihat Menghapus kerangka kerja.
2. Untuk menghapus semua rencana laporan, lihat Menghapus rencana laporan.

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRoleForBackupReports (AWS CLI)

1. Untuk menghapus semua kerangka kerja, gunakan delete-framework.
2. Untuk menghapus semua rencana laporan, gunakan delete-report-plan.

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRoleForBackupReports (API)

1. Untuk menghapus semua kerangka kerja, gunakan DeleteFramework.

2. Untuk menghapus semua rencana laporan, gunakan DeleteReportPlan.

Menghapus peran tertaut layanan secara manual

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForBackupReports terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran yang terhubung dengan layanan AWS Backup

AWS Backup mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat fitur dan Wilayah yang AWS Backup didukung.

Menggunakan peran untuk memulihkan pengujian

AWS Backup menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Backup Peran terkait layanan telah ditentukan sebelumnya oleh AWS Backup dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Backup lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Backup mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Backup dapat mengambil perannya. Izin-izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini melindungi AWS Backup sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AWS Backup

AWS Backup menggunakan peran terkait layanan bernama AWSServiceRolePolicyForBackupRestoreTesting— Menyediakan izin cadangan untuk melakukan pengujian pemulihan.

Peran AWSServiceRolePolicyForBackupRestoreTesting terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `backup.amazonaws.com`

Untuk melihat izin kebijakan ini, lihat AWSServiceRolePolicyForBackupRestoreTestingdi Referensi Kebijakan AWS Terkelola.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Membuat peran yang terhubung dengan layanan untuk AWS Backup

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda melakukan pengujian pemulihan di AWS Management Console, the AWS CLI, atau AWS API, AWS Backup buat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran Baru yang Muncul di Akun IAM Saya.

Jika Anda menghapus peran yang terhubung dengan layanan ini, lalu ingin membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut di akun Anda. Saat Anda melakukan pengujian pemulihan, AWS Backup buat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk AWS Backup

AWS Backup tidak memungkinkan Anda untuk mengedit peran AWSServiceRolePolicyForBackupRestoreTesting terkait layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Backup

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, kami menyarankan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan dan tidak dipantau atau dipelihara secara aktif. Namun, Anda harus membersihkan peran tertaut layanan terlebih dahulu sebelum dapat menghapusnya secara manual.

Membersihkan peran tertaut-layanan

Sebelum dapat menggunakan IAM untuk menghapus peran tertaut-layanan, Anda harus terlebih dahulu menghapus semua sumber daya yang digunakan oleh peran tersebut. Anda harus menghapus semua rencana pengujian pemulihan.

> **Note**
>
> Jika AWS Backup layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika itu terjadi, tunggu beberapa menit, lalu coba operasi lagi.

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRolePolicyForBackupRestoreTesting (konsol)

- Untuk menghapus semua paket pengujian pemulihan, lihat Memulihkan pengujian.

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI)

- Untuk menghapus rencana pengujian pemulihan, gunakan`delete-restore-testing-plan`.

Untuk menghapus AWS Backup sumber daya yang digunakan oleh AWSServiceRolePolicyForBackupRestoreTesting (API)

- Untuk menghapus rencana pengujian pemulihan, gunakan`DeleteRestoreTestingPlan`.

Menghapus peran tertaut layanan secara manual

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRolePolicyForBackupRestoreTesting terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran yang terhubung dengan layanan AWS Backup

AWS Backup mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat fitur dan Wilayah yang AWS Backup didukung.

Pencegahan confused deputy lintas layanan

Masalah confused deputy adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang lebih berhak untuk melakukan tindakan tersebut. Pada tahunAWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan panggilan) memanggil layanan lain (layanan yang disebut). Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak atas sumber daya pelanggan lain dengan cara yang seharusnya tidak memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS sediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsip layanan yang telah diberikan akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan dalam kebijakan sumber daya untuk membatasi izin yang AWS Backup memberikan layanan lain ke sumber daya. Jika Anda menggunakan kedua kunci konteks kondisi global, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Nilai `aws:SourceArn` harus berupa AWS Backup brankas saat menggunakan AWS Backup untuk mempublikasikan topik Amazon SNS atas nama Anda.

Cara paling efektif untuk melindungi dari masalah wakil yang membingungkan adalah dengan menggunakan kunci konteks kondisi `aws:SourceArn` global dengan ARN penuh sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws::`*`servicename`*`::`*`123456789012`*`:*`.

Keamanan infrastruktur di AWS Backup

Sebagai layanan terkelola, AWS Backup dilindungi oleh keamanan jaringan AWS global. Untuk informasi selengkapnya tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan infrastruktur dalam Kerangka Kerja AWS Arsitektur Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Backup melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.2 atau versi yang lebih baru. Klien juga harus mendukung cipher suite dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Integritas Data di AWS Backup

AWS Backup tujuan integritas data

AWS Backup berusaha untuk menjaga integritas selama transmisi, penyimpanan, dan pemrosesan data Anda. AWS Backup memperlakukan data sumber daya yang tersimpan sebagai informasi penting konten-agnostik, karena kami menawarkan tingkat keamanan yang sama tinggi kepada pelanggan, terlepas dari jenis data yang Anda simpan. Kami waspada terhadap keamanan pelanggan kami dan telah menerapkan langkah-langkah teknis dan fisik yang canggih terhadap akses yang tidak sah. Anda memiliki kendali penuh atas bagaimana data Anda diklasifikasikan, Wilayah tempat Anda menyimpan data, dan cara Anda mengontrol, mengarsipkan, dan melindungi data Anda dari pengungkapan.

AWS Backup implementasi integritas data

AWS Backup bekerja bersama dengan layanan lain AWS dan Amazon untuk menjaga integritas data yang disimpannya dan berinteraksi dengannya. Alat yang digunakan dapat bervariasi dan dapat mencakup (tetapi tidak terbatas pada):

- Validasi objek berkelanjutan terhadap checksum mereka untuk mencegah kerusakan objek
- Checksum internal untuk mengonfirmasi integritas data saat transit dan saat istirahat
- Checksum dihitung pada data dalam backup yang dibuat dari toko utama
- Upaya otomatis untuk mengembalikan tingkat normal redundansi penyimpanan objek jika terjadi kerusakan disk atau deteksi kegagalan perangkat
- Penyimpanan data yang berlebihan di beberapa lokasi fisik
- Peningkatan daya tahan objek di beberapa zona ketersediaan selama penulisan awal, dikombinasikan dengan replikasi lebih lanjut jika perangkat tidak tersedia atau bit-rot yang terdeteksi
- Checksum pada semua lalu lintas jaringan untuk mendeteksi kerusakan paket data saat menyimpan atau mengambil data

AWS Backup menyimpan data asli untuk Amazon DynamoDB dengan fitur-fitur canggih, Amazon EFS, Amazon S3, Amazon Timestream, dan mesin virtual yang berjalan dengan VMware yang terhubung melalui gateway Backup. AWS Backup memfasilitasi pencadangan data yang disimpan dengan layanan lain, termasuk Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon FSX untuk Windows File Server, Amazon FSx for Lustre, Amazon FSx for Lustre, Amazon FSx untuk OpenZFS, Amazon FSx untuk OpenZFS, Amazon FSx FSX untuk ONTAP, Amazon Neptunus, Amazon RDS, dan Amazon Redshift. NetApp

Konfirmasi obyektif dan audit integritas AWS Backup data

Data yang disimpan langsung oleh AWS Backup dan data yang disimpan dalam kemitraan dengan sesama AWS layanan yang AWS Backup berinteraksi menjadi sasaran proses ketat Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang mendukung integritas data ini. Integritas ini dikonfirmasi oleh auditor pihak ketiga yang independen melalui laporan audit SOC tahunan yang tersedia melalui AWS Artifactlaporan audit SOC. AWS Management Console

Kepemilikan hukum dan AWS Backup

Penahanan hukum adalah alat administratif yang membantu mencegah cadangan dihapus saat berada di bawah penahanan. Saat penahanan dilakukan, pencadangan di bawah penahanan tidak dapat dihapus dan kebijakan siklus hidup yang akan mengubah status cadangan (seperti transisi ke `Deleted` negara bagian) ditunda hingga penahanan hukum dihapus. Cadangan dapat memiliki lebih dari satu pegangan hukum.

Penahanan hukum dapat diterapkan pada satu atau lebih cadangan (juga dikenal sebagai titik pemulihan) yang dibuat oleh AWS Backup jika siklus hidup mereka memungkinkan. Jenis cadangan yang disebut backup berkelanjutan memiliki siklus hidup maksimum 35 hari. Penahanan hukum tidak memperpanjang siklus hidup pencadangan berkelanjutan.

Ketika penahanan hukum dibuat, ia dapat mempertimbangkan kriteria penyaringan tertentu, seperti jenis sumber daya dan ID sumber daya. Selain itu, Anda dapat menentukan rentang tanggal pembuatan cadangan yang ingin Anda sertakan dalam penangguhan hukum. Penahanan dan pencadangan hukum memiliki banyak: banyak hubungan, yang berarti cadangan dapat memiliki lebih dari sekadar penahanan hukum dan penahanan hukum dapat mencakup lebih dari satu cadangan. Setiap akun dapat memiliki maksimal 50 penahanan hukum yang aktif pada satu waktu.

Penahanan hukum hanya berlaku untuk cadangan asli tempat mereka ditempatkan. Ketika cadangan disalin di seluruh Wilayah atau akun (jika sumber daya mendukungnya), cadangan tersebut tidak mempertahankan atau membawa pegangan hukumnya. Penangguhan hukum, seperti sumber daya lainnya, memiliki ARN (Nama Sumber Daya Amazon) unik yang terkait dengannya. Hanya poin pemulihan yang dibuat oleh yang AWS Backup dapat menjadi bagian dari pegangan hukum.

Perhatikan bahwa meskipun AWS Backup Vault Lock memberikan perlindungan tambahan dan kekekalan ke brankas, penangguhan hukum memberikan perlindungan tambahan terhadap penghapusan cadangan individu (titik pemulihan). Penahanan hukum tidak kedaluwarsa dan menyimpan data dalam cadangan tanpa batas waktu. Penahanan tetap aktif sampai dirilis oleh pengguna dengan izin yang memadai.

Buat pegangan hukum

Ketika penahanan hukum dibuat, itu hanya berisi poin pemulihan yang telah dibuat. Cadangan (poin pemulihan) dengan status `EXPIRED` atau tidak `DELETING` akan dimasukkan dalam penahanan hukum. Poin pemulihan (cadangan) dengan status `CREATING` mungkin tidak termasuk dalam penangguhan hukum, tergantung pada waktu penyelesaian.

Penahanan hukum dapat ditambahkan oleh pengguna yang memiliki izin IAM yang diperlukan.

Buat penahanan hukum menggunakan konsol

Untuk membuat pegangan hukum

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di dasbor di sebelah kiri konsol, temukan Akun Saya. Pilih pegangan Legal.

3. Pilih Tambahkan penahanan hukum.
4. Tiga panel ditampilkan: Detail penahanan hukum, Ruang lingkup penahanan hukum, dan tag penahanan hukum.

    a. Di bawah rincian penahanan hukum, masukkan judul penahanan hukum dan deskripsi untuk penahanan di kotak teks yang disediakan.
    b. Di panel Lingkup penahanan hukum, pilih bagaimana Anda ingin memilih sumber daya yang akan disertakan dalam penahanan. Saat Anda membuat penahanan, Anda memilih metode yang digunakan untuk memilih sumber daya yang berada dalam penahanan hukum. Anda dapat memilih untuk memasukkan salah satu dari berikut ini:

        - Jenis dan ID sumber daya tertentu
        - Pilih brankas cadangan
        - Semua jenis sumber daya atau semua brankas cadangan dalam akun Anda

    c. Tentukan rentang tanggal penangguhan hukum Anda. Masukkan tanggal dalam format YYYY:MM:DD (tanggal sudah termasuk).
    d. Secara opsional, Anda dapat menambahkan tag untuk penahanan di bawah tag penahanan hukum. Tag dapat membantu mengkategorikan penahanan untuk referensi dan organisasi masa depan. Anda dapat menambahkan hingga 50 tag total.
5. Ketika Anda puas dengan konfigurasi penahanan hukum baru Anda, klik tombol Tambahkan penahanan baru.

Buat pegangan hukum menggunakan AWS CLI

Anda dapat membuat penahanan hukum menggunakan create-legal-holdperintah.

```
aws backup create-legal-hold --title "my title" \
    --description "my description" \
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

Lihat pegangan hukum

Anda dapat melihat detail penahanan hukum di AWS Backup konsol atau secara terprogram.

Lihat penahanan hukum menggunakan konsol

Untuk melihat semua penahanan hukum dalam akun menggunakan konsol Backup,

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Menggunakan bagian kiri dasbor, di bawah Akun saya, klik Penahanan hukum.
3. Tabel penahanan hukum menampilkan judul, status, deskripsi, ID, dan tanggal pembuatan penahanan yang ada. Klik pada karat (panah bawah) di sebelah header tabel untuk memfilter tabel dengan kolom yang dipilih.

Lihat pegangan hukum secara terprogram

Untuk melihat semua penahanan hukum secara terprogram, Anda dapat menggunakan panggilan API berikut: ListLegalHoldsdan. GetLegalHold

Template JSON berikut dapat digunakan untuk`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
        }
   }
```

```
}
```

Template JSON berikut dapat digunakan untuk`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,
  ]

}
```

Berikut ini adalah nilai status yang mungkin.

Status	Deskripsi
CREATING	Poin pemulihan yang diminta sedang dalam proses ditahan, dan menghapus permintaan dari titik pemulihan tersebut mungkin berhasil karena penahanan belum selesai dibuat.
AKTIF	Penahanan hukum telah dibuat, Semua poin pemulihan yang tercantum dalam penangguhan hukum ini diadakan.
MEMBATALKAN	Penahanan hukum sedang dalam proses dihapus, dan menghapus permintaan poin pemulihan di bawah penahanan mungkin berhasil.
MEMBATALKAN	Penahanan hukum sepenuhnya dilepaskan dan tidak lagi berpengaruh. Poin pemulihan dapat dihapus.

Lepaskan pegangan hukum

Penahanan hukum tetap berlaku sampai dihapus oleh pengguna dengan izin yang memadai. Menghapus penahanan hukum juga dikenal sebagai membatalkan, menghapus, atau melepaskan penahanan hukum. Menghapus penahanan hukum menghilangkannya dari semua cadangan yang dilampirkan. Setiap cadangan yang kedaluwarsa selama penangguhan hukum akan dihapus dalam waktu 24 jam setelah penangguhan hukum dihapus.

Lepaskan penahanan hukum menggunakan konsol

Untuk melepaskan penahanan menggunakan konsol

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Masukkan deskripsi yang ingin Anda kaitkan dengan rilis.
3. Tinjau detailnya, lalu klik Rilis tahan.
4. Saat kotak dialog Release hold muncul, konfirmasikan maksud Anda untuk melepaskan penahanan dengan mengetikkan `confirm` ke dalam kotak teks.

- Centang kotak yang menyatakan bahwa Anda membatalkan penahanan.

Pada halaman penahanan hukum Anda dapat melihat semua pegangan Anda. Jika rilis berhasil, status penahanan itu akan ditampilkan sebagai`Released`.

Lepaskan penahanan hukum secara terprogram

Untuk menghapus penahanan secara terprogram, gunakan panggilan API. CancelLegalHold

Gunakan template JSON berikut.

```
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 memungkinkan Anda untuk membuat koneksi pribadi antara Virtual Private Cloud (“VPC”) dan titik akhir dengan membuat antarmuka VPC AWS Backup endpoint. Endpoint antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses AWS Backup API

secara pribadi dengan membatasi semua lalu lintas jaringan antara VPC Anda dan ke AWS Backup jaringan Amazon.

AWS PrivateLink memungkinkan Anda mengakses AWS Backup operasi secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau AWS Direct Connect koneksi. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi AWS Backup dengan titik akhir API Instans Anda juga tidak memerlukan alamat IP publik untuk menggunakan API yang tersedia dan operasi AWS Backup API gateway Backup. Lalu lintas antara VPC Anda dan AWS Backup tidak meninggalkan jaringan Amazon.

Untuk informasi selengkapnya tentang titik akhir VPC, lihat Titik akhir VPC Antarmuka () di AWS PrivateLink Panduan Pengguna Amazon VPC.

Pertimbangan untuk titik akhir Amazon VPC

Sebelum menyiapkan titik akhir VPC antarmuka untuk titik akhir, tinjau properti dan batasan AWS Backup titik akhir Antarmuka di Panduan Pengguna Amazon VPC.

Semua AWS Backup operasi yang relevan untuk mengelola sumber daya Amazon Backup tersedia dari VPC Anda menggunakan. AWS PrivateLink

Kebijakan titik akhir VPC didukung untuk titik akhir Backup. Secara default, akses penuh ke operasi Backup diizinkan melalui titik akhir. Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Membuat titik akhir AWS Backup VPC

Anda dapat membuat titik akhir VPC untuk AWS Backup menggunakan konsol VPC Amazon atau (CLI). AWS Command Line Interface AWS Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di Panduan Pengguna Amazon VPC.

Buat titik akhir VPC untuk AWS Backup menggunakan nama layanan.
`com.amazonaws.region.backup`

Di Wilayah China (Beijing) dan Wilayah China (Ningxia), nama layanannya
`haruscn.com.amazonaws.region.backup`.

Untuk titik akhir gateway Backup, gunakan`com.amazonaws.region.backup-gateway`.

Port TCP berikut harus diizinkan dalam grup keamanan saat membuat titik akhir VPC untuk Gateway cadangan:

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Protokol	Port	Arahan	Sumber	Tujuan	Penggunaan
TCP	443 (HTTPS)	Ke luar	Gerbang Cadangan	AWS	Untuk komunikasi dari Backup Gateway ke titik akhir AWS layanan

Menggunakan VPC endpoint

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API AWS Backup dengan titik akhir VPC menggunakan nama DNS default untuk Wilayah, misalnya. AWS `backup.us-east-1.amazonaws.com`

Namun, untuk Wilayah China (Beijing) dan Wilayah China (Ningxia) Wilayah AWS, permintaan API harus dibuat dengan titik akhir VPC `backup.cn-north-1.amazonaws.com.cn` menggunakan `backup.cn-northwest-1.amazonaws.com.cn` dan, masing-masing.

Untuk informasi selengkapnya, lihat Mengakses layanan melalui titik akhir antarmuka di Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC

Anda dapat melampirkan kebijakan titik akhir ke titik akhir VPC yang mengontrol akses ke Amazon Backup API. Kebijakan menentukan:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.

- Sumber daya yang menjadi target tindakan.

> **Important**
>
> Ketika kebijakan non-default diterapkan ke titik akhir VPC antarmuka AWS Backup untuk, permintaan API tertentu yang gagal, seperti yang gagal`RequestLimitExceeded`, mungkin tidak dicatat atau Amazon. AWS CloudTrail CloudWatch

Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Contoh: Kebijakan titik akhir VPC untuk tindakan AWS Backup

Berikut ini adalah contoh kebijakan endpoint untuk AWS Backup. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke AWS Backup tindakan yang tercantum untuk semua prinsip pada semua sumber daya.

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

Contoh: Kebijakan titik akhir VPC yang menolak semua akses dari akun tertentu AWS

Kebijakan titik akhir VPC berikut menolak `123456789012` semua akses AWS akun ke sumber daya menggunakan titik akhir. Kebijakan ini mengizinkan semua tindakan dari akun lainnya.

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"Stmt1645236612384",
```

```
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

Untuk detail lebih lanjut tentang respons API yang tersedia, silakan merujuk ke Panduan API.

Ketersediaan AWS Backup saat ini mendukung titik akhir VPC di Wilayah berikut: AWS

- Wilayah AS Timur (Ohio)
- Wilayah AS Timur (Virginia Utara)
- Wilayah AS Barat (Oregon)
- Wilayah AS Barat (California Utara)
- Wilayah Afrika (Cape Town)
- Wilayah Asia Pacific (Hong Kong)
- Wilayah Asia Pasifik (Mumbai)
- Wilayah Asia Pasifik (Osaka)
- Wilayah Asia Pacific (Seoul)
- Wilayah Asia Pasifik (Singapura)
- Wilayah Asia Pasifik (Sydney)
- Wilayah Asia Pasifik (Tokyo)
- Wilayah Kanada (Pusat)
- Wilayah Eropa (Frankfurt)
- Wilayah Eropa (Irlandia)
- Wilayah Eropa (London)
- Wilayah Eropa (Paris)
- Wilayah Eropa (Stockholm)

- Wilayah Eropa (Milan)
- Wilayah Middle East (Bahrain)
- Wilayah Amerika Selatan (Sao Paulo)
- Wilayah Asia Pasifik (Jakarta)
- Wilayah Asia Pasifik (Osaka)
- Wilayah Tiongkok (Beijing)
- Wilayah China (Ningxia)
- AWS GovCloud (AS-Timur)
- AWS GovCloud (AS-Barat)

> **Note**
>
> AWS Backup untuk VMware tidak tersedia di Wilayah China (China (Beijing) Region and China (Ningxia) Region) atau Asia Pacific (Jakarta) Region.

Ketahanan di AWS Backup

AWS Backup mengambil ketahanannya — dan keamanan data Anda — dengan sangat serius.

AWS Backup menyimpan cadangan Anda dengan setidaknya ketahanan dan daya tahan sebanyak AWS layanan asli sumber daya Anda akan memberi Anda, jika Anda mendukungnya di sana.

AWS Backup dirancang untuk menggunakan infrastruktur AWS global untuk mereplikasi cadangan Anda di beberapa Availability Zone untuk daya tahan 99,999999999% (11 sembilan) pada tahun tertentu, asalkan Anda mematuhi dokumentasi saat ini. AWS Backup

AWS Backup mengenkripsi paket cadangan Anda saat istirahat dan terus mencadangkannya. Anda juga dapat membatasi akses ke paket cadangan menggunakan kredensyal dan kebijakan AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat Autentikasi, Kontrol Akses, dan Praktik Terbaik Keamanan di IAM.

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. AWS Backup menyimpan cadangan Anda di seluruh Availability Zones. Zona Ketersediaan memiliki ketersediaan

dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data. Untuk informasi selengkapnya, lihat Perjanjian Tingkat AWS Backup Layanan (SLA).

Selain itu, AWS Backup memberdayakan Anda untuk menyalin cadangan Anda di seluruh Wilayah untuk ketahanan yang lebih besar. Untuk informasi selengkapnya tentang fitur Salin AWS Backup lintas wilayah, lihat Membuat Salinan Cadangan.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

AWS Backup kuota

Kuota berikut berlaku saat bekerja dengan AWS Backup. Banyak AWS Backup kuota dapat disesuaikan jika diizinkan oleh layanan jenis sumber daya. Untuk meminta penyesuaian kuota, jelaskan kasus penggunaan Anda ke AWS Support.

AWS Backup kuota

Sumber Daya	Kuota	Catatan
Jumlah brankas cadangan per Wilayah per akun	300	Anda dapat meminta penyesuaian.
Jumlah titik pemulihan per brankas cadangan	1.000.000	Anda dapat meminta penyesuaian.
Jumlah paket cadangan per Wilayah per akun	300	Anda dapat meminta penyesuaian.
Jumlah versi per paket cadangan	2.000	Anda dapat meminta penyesuaian.
Jumlah penugasan sumber daya per rencana cadangan	100	Tidak dapat disesuaikan
Jumlah pekerjaan pencadangan aktif per akun	Tidak terbatas.	
Jumlah salinan cadangan bersamaan per akun yang keluar ke Wilayah tujuan	100	Anda dapat meminta penyesuaian untuk sumber daya tertentu (saat ini mesin virtual, Advanced DynamoDB, Timestream, Amazon EFS, dan database SAP HANA di instans Amazon EC2)
Jumlah salinan bersamaan per vault cadangan tujuan di akun	5	Tidak dapat disesuaikan

Sumber Daya	Kuota	Catatan
setelah batas (entri di atas) tercapai		
Jumlah salinan lintas akun bersamaan yang dapat dibuat dari sumber daya yang sama ke Wilayah tujuan yang sama	30	Tidak dapat disesuaikan.
Jumlah pekerjaan pencadangan dan penyalinan bersamaan per sumber daya	1	Tidak dapat disesuaikan. Kuota ini membantu Anda mempertahankan kinerja beban kerja Anda.
Jumlah tag metadata per cadangan	50	Anda tidak dapat meminta penyesuaian. AWS memberlakukan kuota ini di semua sumber daya. Lihat Batas dan persyaratan penamaan tag di Referensi AWS Umum.
Jumlah tag per pemilihan sumber daya dalam kebijakan pencadangan lintas akun	30	Tidak dapat disesuaikan. Tag tambahan dapat disertakan dengan memanfaatkan beberapa tugas sumber daya atau rencana cadangan.
Jumlah hypervisor	10	Tidak dapat disesuaikan
Jumlah pegangan hukum	50 per akun	Tidak dapat disesuaikan
Jumlah maksimum lapisan cadangan bersarang dari tumpukan aplikasi	10	Tidak dapat disesuaikan

AWS Backup kuota sumber daya Amazon Timestream

Sumber Daya	Kuota	Catatan
Jumlah pekerjaan pencadangan Timestream bersamaan per akun	4	Anda dapat meminta penyesuaian.
Jumlah pekerjaan pemulihan Timestream bersamaan per akun	1	Anda dapat meminta penyesuaian.

Ada kuota pada penugasan sumber daya tunggal dalam satu aturan cadangan. Anda dapat membuat rencana cadangan dengan beberapa aturan cadangan.

AWS Backup Kuota Audit Manager

Sumber Daya	Kuota	Catatan
Jumlah kerangka kerja per akun per Wilayah	15	Anda dapat meminta penyesuaian.
Jumlah kontrol per akun per Wilayah	50	Anda dapat meminta penyesuaian.
Jumlah rencana laporan per akun	20	Anda dapat meminta penyesuaian.
Jumlah kerangka kerja per rencana laporan	1.000	Tidak dapat disesuaikan
Jumlah maksimum akun dikalikan dengan Wilayah dalam rencana laporan	300	Tidak dapat disesuaikan

Kembalikan kuota rencana pengujian

Sumber Daya	Kuota	Catatan
Kembalikan rencana pengujian	100	Tidak dapat disesuaikan
Jumlah tag di setiap paket	50	Tidak dapat disesuaikan
Pilihan per paket	30	Tidak dapat disesuaikan
ARN per pilihan pengujian pemulihan	30	Tidak dapat disesuaikan
Kondisi per seleksi	30	Termasuk yang terkandung dalam keduanya `StringEquals` dan`StringNotEquals` .
Penyeleksi vault per pilihan pengujian pemulihan	30	Tidak dapat disesuaikan
Nilai maksimum (dalam hari) jendela seleksi	365 hari	
Batas jam jendela mulai	Minimal: 1 jam; Maksimal: 168 jam	
Panjang karakter maksimum dari nama rencana pengujian pemulihan	50 karakter	Alfanumerik dan garis bawah, tidak ada spasi putih
Panjang karakter maksimum dari nama pemilihan pengujian pemulihan	50 karakter	Alfanumerik dan garis bawah, tidak ada spasi putih

AWS Backup gateway kuota

Sumber Daya	Kuota	Catatan
Cadangkan atau pulihkan pekerjaan per gateway	4	Anda tidak dapat meminta penyesuaian. Alih-alih, buat lebih banyak gateway dan hubungkan ke hypervisor Anda.

Ketika Anda mengelola backup di beberapa akun menggunakan AWS Organizations, Anda mungkin menemukan kuota yang dikenakan. AWS Organizations Untuk kuota ini, lihat Kuota untuk AWS Organizations di AWS Organizations Panduan Pengguna.

Anda mungkin juga menemukan kuota yang diberlakukan oleh layanan yang AWS Backup didukung, termasuk:

- Amazon Elastic File System
- Toko Blok Elastis Amazon
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon DynamoDB
- Amazon FSx for Lustre
- Amazon FSx for Windows File Server
- Amazon DocumentDB
- Amazon Neptunus
- Layanan Penyimpanan Sederhana Amazon
- Amazon Timestream

Pemantauan

AWS Backup bekerja dengan AWS alat lain untuk memberdayakan Anda memantau beban kerjanya. Alat-alat ini meliputi:

- AWS Backup dasbor konsol
  - Dasbor pekerjaan menghadirkan pemantauan kesehatan pekerjaan, tempat Anda dapat melihat metrik yang menunjukkan keberhasilan dan kegagalan pekerjaan, disaring berdasarkan alasan, akun, Wilayah, dan jenis sumber daya.
  - Dasbor pekerjaan tersedia di Wilayah di mana AWS Backup Audit Manager didukung. Lihat Ketersediaan fitur oleh Wilayah AWS untuk Wilayah tersebut. Semua Wilayah lain akan dapat mengaksesCloudWatch Dasbor.
- Amazon CloudWatch dan Amazon EventBridge untuk memantau AWS Backup proses.
  - Anda dapat menggunakan CloudWatch untuk melacak metrik, membuat alarm, dan melihat dasbor.
  - Anda dapat menggunakan EventBridge untuk melihat dan memantau AWS Backup acara.

  Untuk informasi selengkapnya, lihat Memantau AWS Backup peristiwa menggunakan Amazon EventBridge dan .
- AWS CloudTrailuntuk memantau panggilan AWS Backup API. Anda dapat mengidentifikasi waktu, sumber IP, pengguna, dan akun yang melakukan panggilan tersebut. Untuk informasi selengkapnya, lihat Logging panggilan AWS Backup API dengan CloudTrail.
- Amazon Simple Notification Service (Amazon SNS) untuk berlangganan topik AWS Backup terkait seperti backup, restore, dan copy event. Untuk informasi selengkapnya, lihat Opsi pemberitahuan dengan AWS Backup.

AWS Backup dasbor konsol

> **Note**
>
> Dasbor pekerjaan tersedia di semua Wilayah di mana AWS Backup Audit Manager didukung. Lihat Ketersediaan fitur oleh Wilayah AWS untuk Wilayah tersebut. Semua Wilayah lain akan dapat mengaksesCloudWatch Dasbor.

Topik

Ikhtisar dasbor cadangan

AWS Backup menyediakan dasbor Pekerjaan di konsol untuk membantu Anda memantau kesehatan pencadangan, menyalin, dan memulihkan pekerjaan Anda. Data yang sama yang ditampilkan secara visual di konsol dapat diambil di baris perintah melalui AWS CLI.

Dasbor pekerjaan dapat digunakan untuk mengidentifikasi masalah dengan pencadangan, menyalin, dan memulihkan pekerjaan melalui pemantauan tingkat organisasi atau akun anggota. Dengan informasi ini, Anda dapat mengidentifikasi dan mendiagnosis peristiwa dan kemungkinan masalah untuk membantu memastikan kesetiaan dalam aktivitas Anda.

Dasbor pekerjaan dapat menampilkan dua kerangka waktu. Secara default, data dari 14 hari terakhir ditampilkan, tetapi Anda dapat mengubah tampilan untuk menampilkan 7 hari terakhir. Jika Anda mengubah jangka waktu, data akan diperbarui untuk mencerminkan interval waktu baru.

Perhatikan dasbor menampilkan data hingga pukul 0:00 UTC terbaru; artinya, data hari ini tidak disertakan. Dasbor diperbarui setiap hari selama sekitar 1:30 - 2:30 UTC.

Melihat dasbor pekerjaan

Untuk melihat dasbor pekerjaan, masuk ke AWS Backup konsol dan pilih dasbor Pekerjaan di bilah navigasi kiri.

Pada halaman dasbor pekerjaan, Anda dapat memilih dari tab backup, copy, atau restore jobs.

Ikhtisar dasbor pekerjaan menampilkan tampilan agregat selama jangka waktu yang ditentukan untuk aktivitas pekerjaan, termasuk pekerjaan yang diselesaikan, diselesaikan dengan masalah, kedaluwarsa, dan gagal. Secara default, data dari 14 hari terakhir ditampilkan, tetapi Anda dapat mengubah tampilan untuk menampilkan 7 hari.

> **Note**
>
> `Completed with issues`adalah status pekerjaan yang ditampilkan di konsol yang menunjukkan pekerjaan yang diselesaikan dengan pesan status.

Kesehatan Job

Bagan garis menampilkan garis tingkat pekerjaan yang berhasil dan tidak berhasil dari waktu ke waktu. Garis tingkat keberhasilan menunjukkan agregasi pekerjaan yang diselesaikan dan diselesaikan dengan masalah. Garis tarif yang tidak berhasil menunjukkan jumlah pekerjaan yang gagal dan kedaluwarsa sesuai dengan rentang waktu yang ditentukan.

Pekerjaan dalam keadaan tidak selesai atau tidak gagal (pekerjaan dengan status dibuat, tertunda, berjalan, dibatalkan, dibatalkan, atau sebagian) tidak termasuk; persentase total mungkin tidak sama dengan 100%.

Status pekerjaan dari waktu ke waktu

Dengan diagram batang, Anda dapat membuat bagan batang kustom yang menunjukkan jumlah pekerjaan di setiap kategori (Selesai, Lengkap dengan masalah, Gagal, dan Kedaluwarsa), didistribusikan berdasarkan hari.

Dengan menu tarik-turun, pilih status, jenis sumber daya, dan AWS Wilayah yang ingin Anda lihat di bagan. Jika Anda ingin menjelajahi pilihan Anda lebih lanjut, pilih Lihat pekerjaan untuk melihat bagian yang telah difilter sebelumnya dari halaman pemantauan pekerjaan/lintas akun.

Anda dapat mengarahkan mouse ke bar untuk menampilkan popover yang menunjukkan data pekerjaan terperinci untuk tanggal yang dipilih.

Pekerjaan bermasalah

Pekerjaan bermasalah adalah pekerjaan yang memiliki status Gagal, Kedaluwarsa, atau Selesai dengan masalah. Setiap bagan menampilkan metrik terkait yang berisi akun, jenis sumber daya, atau alasan utama yang berisi jumlah pekerjaan bermasalah tertinggi.

Tampilan default mengurutkan widget dasbor berdasarkan metrik yang ditentukan dalam urutan menurun, dimulai dengan metrik dengan jumlah pekerjaan bermasalah tertinggi yang termasuk dalam metrik.

Tampilan akun bermasalah teratas hanya akan terlihat di akun yang memiliki akses melalui Organizations, seperti akun administratif dan akun administrator yang didelegasikan. Jika terlihat, Anda dapat mengarahkan kursor ke akun untuk menampilkan jumlah pekerjaan bermasalah yang termasuk dalam akun yang dipilih.

Anda dapat memilih bilah di dalam grafik untuk membuka jendela popup. Di jendela ini, Anda dapat memilih status pekerjaan untuk membuka tabel pemantauan pekerjaan/lintas akun yang disaring berdasarkan status yang dipilih.

Alasan pekerjaan bermasalah

Widget Alasan bermasalah teratas menunjukkan kategori kode pesan yang menjadi milik pesan kesalahan. Namun, kategori tersebut mungkin tidak menjelaskan masalah yang dialami pekerjaan. Perluas kategori kode pesan di bawah ini untuk melihat detail selengkapnya tentang pesan atau kesalahan tertentu yang mungkin dihadapi pekerjaan Anda.

“VSS_ERROR”

- “Upaya Pencadangan Windows VSS gagal karena Instance atau Agen SSM memiliki status tidak valid atau hak istimewa yang tidak memadai.”
- “Upaya Pencadangan Windows VSS gagal karena hak istimewa yang tidak memadai untuk melakukan operasi ini”
- “Upaya Pencadangan Windows VSS gagal karena ec2-vss-agent.exe tidak diinstal dalam Instance”
- “Windows VSS Backup Job Error ditemui, mencoba untuk backup reguler”
- “Upaya Pencadangan Windows VSS gagal karena batas waktu pada pembuatan snapshot yang diaktifkan VSS”
- Upaya Pencadangan Windows VSS gagal karena versi Windows Server yang tidak didukung. Versi yang didukung adalah Windows Server 2012 atau yang lebih baru.
- “Upaya Pencadangan Windows VSS gagal karena batas waktu pada pembuatan snapshot yang diaktifkan VSS”

“LIMIT_TERLAMPAUI”

- “Batas pelanggan terlampaui: Anda telah mencapai jumlah cadangan bersamaan maksimum, yaitu 300. Tunggu sampai pekerjaan lain selesai, dan coba lagi. Anda juga dapat menghubungi AWS Support untuk meminta peningkatan kuota.”

- “Snapshot dalam proses maksimum yang diizinkan untuk satu volume terlampaui.”
- “Batas snapshot aktif maksimum yang diizinkan terlampaui.”
- “Tidak dapat membuat lebih dari 20 snapshot pengguna”
- “Set tag yang dihasilkan tidak boleh memiliki lebih dari 50 tag pengguna.”
- “Anda telah mencapai backup maksimum yang didukung untuk akun/database Anda. Lihat Kuota di panduan pengembang Timestream untuk informasi tambahan.”
- “Anda telah mencapai kuota 50.000 untuk jumlah gambar publik dan pribadi yang diizinkan di Wilayah ini. Deregister gambar yang tidak digunakan, atau minta peningkatan kuota AMI Anda.
- “Cadangan Anda berhasil, tetapi kami tidak dapat mempertahankan NetworkInterfaces metadata karena ukurannya melebihi batas internal kami.”
- “Batas REGEX #subscriber terlampaui”
- “REGEX #More dari 50 tag yang ditentukan”
- “REGEX #can memiliki paling banyak”

“ACCESS_DENIED”

- “Anda tidak berwenang untuk melakukan operasi ini.”
- “Akses Ditolak mencoba menelepon AWS Backup layanan”
- “Gambar dari AWS Marketplace tidak dapat disalin ke AWS akun lain.”
- “Salin pekerjaan gagal karena brankas Cadangan tujuan dienkripsi dengan kunci terkelola layanan Backup default. Isi brankas ini tidak dapat disalin. Hanya konten brankas Cadangan yang dienkripsi oleh AWS KMS kunci yang dapat disalin.
- Snapshot yang dienkripsi dengan tidak Kunci yang dikelola AWS dapat dibagikan. Tentukan snapshot lain.
- “Snapshot terenkripsi dengan kunci default Amazon EBS tidak dapat dibagikan
- “Copy job gagal. Akun sumber dan tujuan harus menjadi anggota dari organisasi yang sama.
- “REGEX #access ditolak”
- “REGEX #not diizinkan untuk”
- “REGEX #cannot diasumsikan oleh AWS Backup
- “REGEX #does tidak memiliki izin”
- “Izin REGEX #missing”

“CONCURRENT_JOB”

- “Pekerjaan cadangan gagal karena ada pekerjaan yang berjalan untuk sumber daya yang sama.”

“FEATURE_NOT_ENABLED”

- “Copy job gagal. Fitur salinan lintas akun tidak diaktifkan untuk organisasi saat ini.

“JOB_KEDALUWARSA”

- “Pekerjaan cadangan berakhir sebelum selesai.”

“INVALID_LIFECYCLE”

- “Copy job gagal. Retensi yang ditentukan dalam pekerjaan tidak berada dalam rentang yang ditentukan untuk Brankas Cadangan target.”
- “REGEX #could tidak dimulai karena berada di dalam atau terlalu dekat dengan jendela pemeliharaan mingguan yang dikonfigurasi”
- “REGEX #could tidak dimulai karena berada di dalam atau terlalu dekat dengan jendela cadangan otomatis yang dikonfigurasi”

“INVALID_STATE”

- “REGEX #Instance tidak dalam keadaan”
- “REGEX #not dalam status tersedia”
- “REGEX #not dalam keadaan tersedia”
- “Volume snapshot REGEX #Cannot”

“KMS_KEY_ERROR”

- “Kunci KMS dinonaktifkan atau penghapusan tertunda atau akses ke kunci KMS ditolak”
- “ID kunci yang diberikan tidak dapat diakses”
- “Salinan snapshot AMI gagal dengan kesalahan: ID kunci yang diberikan tidak dapat diakses. Anda harus memiliki DescribeKey izin pada CMK default”
- “Kunci REGEX #kms”

“ACCESS_KEY_ERROR”

- “ AWS Access Key Id membutuhkan langganan untuk layanan”

“HYPERVISOR_OFFLINE”

- “Operasi ini tidak berlaku untuk hypervisor yang ditentukan karena tidak online”

“SUMBER DAYA_NOT_FOUND”

- “Volume yang ditentukan tidak ditemukan.”
- “Mesin virtual tidak ditemukan.”
- “ID kunci yang diberikan tidak ada”
- “REGEX #does tidak ada”
- “REGEX #Could tidak menemukan sumber daya”
- “REGEX #Could tidak menemukan cryopod”
- “REGEX #Cannot temukan titik pemulihan”
- “REGEX #resource tidak ditemukan”
- “REGEX #no lebih lama tersedia”
- “REGEX #is tidak valid”

“SUMBER DAYA_NOT_SUPPORTED”

- “Jenis sumber daya REGEX #unsupported”
- “Jenis sumber daya REGEX #Unsupported”

“TAG_COPY_ERROR”

- “Kami tidak dapat menyalin tag sumber daya ke cadangan Anda karena Kegagalan Internal.”
- “Kami tidak dapat menyalin tag sumber daya ke cadangan Anda karena titik pemulihan sumber atau tujuan tidak tersedia”

“TOKEN_EXPIRED”

- “Token kedaluwarsa. Coba lagi.”

“UNSUPPORTED_OPERATION”

- “CreateSnapshot Metode tidak didukung pada hypervisor selama pembuatan snapshot. Pekerjaan cadangan dibatalkan”
- “UnsupportedOperation : Salinan cadangan Storage Gateway memerlukan brankas cadangan yang dibuat pengguna dan CMK di tempat tujuan.”
- “REGEX #Feature tidak didukung untuk jenis sumber daya yang disediakan.”

“FATAL_ERROR”

- “Terjadi kesalahan internal.”
- “Copy job mengalami kesalahan fatal. Silakan hubungi AWS Support untuk bantuan lebih lanjut.”
- “Salin pekerjaan mengalami kesalahan fatal.”
- “Pekerjaan REGEX #Backup mengalami kesalahan fatal”

Memperoleh data dasbor melalui AWS CLI

Anda dapat menggunakan baris perintah untuk mengambil data yang sama yang muncul di konsol. Gunakan salah satu perintah CLI berikut:

- `list-backup-job-summaries`
- `list-copy-job-summaries`
- `list-restore-job-summaries`

Ada parameter valid yang dapat Anda sertakan dalam setiap perintah:

```
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)
```

Contoh ini menunjukkan permintaan sampel di mana pengguna memiliki input `list-backup-job-summaries` di mana permintaan meminta untuk mengembalikan semua akun yang tersedia dengan status `FAILED` selama 14 hari sebelumnya:

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

Untuk mendapatkan jumlah pekerjaan untuk pekerjaan dengan status`completed with issues`, kurangi jumlah pekerjaan `COMPLETED` pekerjaan dengan a `MessageCategory` `SUCCESS` dari jumlah total`COMPLETED`.

Memantau AWS Backup peristiwa menggunakan Amazon EventBridge

AWS Backup mengirimkan acara ke Amazon EventBridge saat status pekerjaan cadangan atau salinan berubah. Anda dapat menggunakan EventBridge untuk memantau AWS Backup acara. Misalnya, Anda dapat menerima alarm ketika pekerjaan cadangan gagal. AWS Backup memancarkan peristiwa dengan EventBridge upaya terbaik setiap 5 menit.

Untuk melacak peristiwa menggunakan EventBridge, lihat berikut ini:

- Membuat aturan yang bereaksi terhadap peristiwa (Panduan EventBridge Pengguna Amazon)
- CloudWatch Acara dan Metrik Amazon untuk AWS Backup (blog - lihat Mengonfigurasi AWS Backup peristiwa untuk dikirim ke Amazon EventBridge)

Beberapa peristiwa melaporkan `status: COMPLETED` sedangkan laporan peristiwa lainnya`state: COMPLETED`. Ini konsisten dengan AWS Backup API. Beberapa status khusus untuk AWS Backup konsol: status `Completed with issues` status adalah representasi `Completed` pekerjaan dengan pesan status. Untuk memantau `Completed with issues` peristiwa, pantau `COMPLETED` pekerjaan yang memiliki pesan status.

Anda juga dapat menggunakan API AWS Backup notifikasi untuk melacak AWS Backup peristiwa dengan Amazon Simple Notification Service (Amazon SNS). Namun, EventBridge melacak lebih banyak perubahan daripada API notifikasi, termasuk perubahan pada brankas cadangan, status pekerjaan salin, pengaturan Wilayah, dan jumlah titik pemulihan dingin atau hangat.

Peristiwa

- Acara Backup Job
- Acara Backup Plan
- Acara Backup Vault
- Copy Job event
- Acara Recovery Point
- Acara Pengaturan Wilayah
- Pulihkan acara Job

Acara Backup Job

Berikut ini adalah contoh peristiwa.

Status

- Negara: GAGAL
- Negara: SELESAI
- Negara: RUNNING
- Negara: ABORTED
- Negara: EXPIRED

- Negara: PENDING
- Negara: CREATED

Negara: GAGAL


```
{
  "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
  }
}
```


Negara: SELESAI


```
{
  "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
  }
}
```

Negara: RUNNING

```
{
  "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"
    }
  }
}
```

Negara: ABORTED

```
{
  "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
  }
}
```

Negara: EXPIRED

```
{
  "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"
    }
  }
}
```

Negara: PENDING


```
{
  "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
  }
}
```


Negara: CREATED


```
{
  "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"
```

```
  }
}
```

Acara Backup Plan

Berikut ini adalah contoh peristiwa.

Status

- Negara: DIMODIFIKASI
- Negara: DIHAPUS
- Negara: CREATED

Negara: DIMODIFIKASI

```
{
  "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"
  }
}
```

Negara: DIHAPUS

```
{
  "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"
  }
}
```

Negara: CREATED

```
{
  "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"
  }
}
```

Acara Backup Vault

Berikut ini adalah contoh peristiwa.

Status

- Negara: CREATED
- Negara: DIMODIFIKASI
- Negara: DIHAPUS

Negara: CREATED


```
{
  "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"
  }
}
```


Negara: DIMODIFIKASI


```
{
  "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"
  }
}
```

Negara: DIHAPUS

```
{
  "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"
  }
}
```

Copy Job event

Berikut ini adalah contoh peristiwa.

Status

- Negara: GAGAL
- Negara: RUNNING
- Negara: SELESAI
- Negara: CREATED

Negara: GAGAL

```
{
  "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": {}
  }
}
```


Negara: RUNNING


```
{
  "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"
    }
  }
}
```

Negara: SELESAI

```
{
  "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"
    }
  }
}
```

Negara: CREATED

```
{
  "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"
  }
}
```

Acara Recovery Point

Berikut ini adalah contoh peristiwa.

Status

- Negara: SELESAI
- Negara: DIHAPUS
- Negara: DIMODIFIKASI

Negara: SELESAI


```
{
    "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"
        }
    }
}
```

Negara: DIHAPUS

```
{
  "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"
    }
  }
}
```

Negara: DIMODIFIKASI

```
{
  "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"
  }
}
```

Acara Pengaturan Wilayah

Berikut adalah contoh kasusnya.

```
{
  "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"
  }
}
```

Pulihkan acara Job

Berikut ini adalah contoh peristiwa.

Status

- Negara: GAGAL
- Negara: RUNNING

- Negara: SELESAI
- Negara: PENDING
- Negara: CREATED

Negara: GAGAL

```
{
  "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."
  }
}
```

Negara: RUNNING

```
{
  "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"
  }
}
```

Negara: SELESAI

```
{
  "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"
  }
}
```

Negara: PENDING

```
{
  "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"
  }
}
```

Negara: CREATED

```
{
  "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 metrik dengan Amazon CloudWatch

Topik

- CloudWatch Dasbor
- Metrik dengan CloudWatch

CloudWatch Dasbor

> **Note**
>
> Dasbor konsol tergantung pada Wilayah mana yang mengakses konsol. Lihat Ketersediaan fitur oleh Wilayah AWS untuk melihat Wilayah mana yang memiliki akses ke dasbor Pekerjaan. Wilayah yang tidak terdaftar akan dapat mengakses CloudWatch dasbor.

AWS Backup Konsol Anda menyertakan dasbor untuk melihat metrik pada pencadangan, penyalinan, dan pemulihan pekerjaan yang telah selesai atau gagal. Dalam dasbor ini, Anda dapat melihat status pekerjaan berdasarkan periode waktu, disesuaikan dengan kerangka waktu yang Anda inginkan.

UNTUK MENGAKSES DASBOR

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Pilih Dasbor di panel navigasi sebelah kiri.

LIHAT DAN PAHAMI DASBOR

CloudWatch Dasbor menampilkan beberapa widget. Setiap widget menampilkan metrik pekerjaan berdasarkan hitungan. Setiap widget menunjukkan beberapa grafik garis. Setiap baris sesuai dengan sumber daya yang dilindungi (jika Anda tidak melihat sumber daya yang diharapkan ditampilkan, pastikan sumber daya diaktifkan di Pengaturan). Tampilan tidak menampilkan pekerjaan yang sedang berlangsung.

Sumbu y (nilai vertikal) menunjukkan hitungan. Sumbu x (nilai horizontal) menunjukkan titik waktu. Jika tidak ada titik data untuk divisualisasikan dalam status pekerjaan yang dipilih, nilainya akan diatur ke 0 dengan garis horizontal pada sumbu x. Legenda yang menunjukkan sumber daya masih akan terlihat.

Metrik menampilkan informasi khusus akun dan spesifik Wilayah yang terkait dengan login saat ini. Untuk melihat akun atau Wilayah lain, Anda harus masuk di bawah akun yang dipilih.

SESUAIKAN DASBOR

Secara default, kerangka waktu yang ditampilkan adalah satu minggu. Di sepanjang menu atas, ada opsi untuk mendefinisikan ulang kerangka waktu yang ditampilkan. Anda dapat memilih antara 1 jam, 3 jam, 12 jam, 1 hari, 3 hari, dan 1 minggu. Selain itu, Anda dapat memilih Kustom untuk menentukan nilai yang berbeda. Kustomisasi sementara akan mengubah tampilan saat ini ke spesifikasi Anda.

Anda dapat mengarahkan kursor ke widget, yang akan menampilkan tombol Perbesar di kanan atas widget. Klik Perbesar untuk membuka widget dalam tampilan layar penuh. Di layar penuh, ada lebih banyak opsi untuk menyesuaikan tampilan grafik, seperti mengubah periode (waktu antara setiap titik data). Perubahan apa pun tidak akan dipertahankan setelah tampilan layar penuh ditutup.

Untuk melihat hanya satu jenis sumber daya pada satu waktu, klik pada teks label dari jenis sumber daya yang ingin Anda lihat dalam legenda grafik. Ini akan membatalkan pilihan semua jenis sumber daya lainnya. Untuk membalikkan ini, klik pada kotak warna jenis sumber daya dalam legenda. Untuk kembali ke tampilan default semua jenis sumber daya dengan semua label yang dipilih, klik lagi pada teks label dari jenis sumber daya apa pun yang dipilih.

Mengklik tiga titik vertikal di sudut kanan atas widget membuka menu tarik-turun dengan opsi untuk menyegarkan, memperbesar, melihat metrik, dan melihat di log. “Lihat dalam metrik” membuka metrik yang digunakan di widget di CloudWatch konsol. Anda dapat membuat perubahan apa pun pada widget di sana dan menambahkan widget ke dasbor khusus di CloudWatch dasbor. Perubahan apa pun yang Anda buat di CloudWatch dasbor tidak akan tercermin di dasbor di AWS Backup Konsol. “Lihat sebagai log” membuka halaman tampilan log di CloudWatch konsol.

Untuk menambahkan widget yang ditampilkan ke CloudWatch dasbor kustom Anda sendiri, klik tombol Tambahkan ke dasbor yang terletak di kanan atas dasbor. Ini akan membuka CloudWatch konsol tempat Anda dapat memilih dasbor khusus mana untuk menambahkan semua enam widget.

Untuk informasi selengkapnya, lihat Menggunakan CloudWatch metrik Amazon.

Metrik dengan CloudWatch

Anda dapat menggunakan CloudWatch untuk memantau AWS Backup metrik. `AWS/Backup`Namespace memungkinkan Anda melacak metrik berikut. AWS Backup memancarkan metrik yang diperbarui untuk CloudWatch setiap 5 menit.

Tujuan dari halaman dokumentasi ini adalah untuk memberi Anda bahan referensi yang akan digunakan CloudWatch untuk memantau AWS Backup. Untuk mempelajari cara memantau metrik menggunakan CloudWatch, lihat blog CloudWatch Acara dan Metrik Amazon untuk AWS Backup atau Fokus pada Metrik dan Alarm dalam AWS Layanan Tunggal di Panduan Pengguna. CloudWatch Untuk menyetel alarm, lihat Menggunakan CloudWatch Alarm Amazon di CloudWatch Panduan Pengguna.

Kategori	Metrik	Contoh dimensi	Contoh kasus penggunaan
Tugas	Jumlah pekerjaan pencadangan, pemulihan, dan penyalinan di setiap negara bagian`CREATED`, termasuk`PENDING`,`RUNN` ,`FAILED`, dan`EXPIRED`.	Jenis sumber daya, nama brankas. Nama brankas dari pekerjaan salinan adalah brankas tujuan mereka.	Pantau jumlah pekerjaan pencadangan yang gagal dalam satu atau lebih brankas cadangan tertentu. Ketika ada lebih dari lima pekerjaan yang gagal dalam 1 jam, kirim email atau

Kategori	Metrik	Contoh dimensi	Contoh kasus penggunaan
	Jenis pekerjaan yang berbeda memiliki status yang tersedia berbeda.		SMS menggunakan Amazon SNS atau buka tiket ke tim teknik untuk menyelidiki. Reporting criteria: Ada nilai bukan nol
Poin pemulihan	Jumlah titik pemulihan hangat dan dingin di setiap negara bagian:`MODIFIED`,`COMP` ,`PARTIAL`,`EXPIRED`,`DI`	Jenis sumber daya, nama brankas.	Lacak jumlah titik pemulihan yang dihapus untuk volume Amazon EBS Anda, dan lacak secara terpisah jumlah titik pemulihan hangat dan dingin di setiap brankas cadangan. Reporting criteria: Ada nilai bukan nol

> **Note**
>
> Status pekerjaan khusus `Completed with issues` hanya untuk AWS Backup konsol; itu tidak dapat dilacak melalui CloudWatch.

Tabel berikut mencantumkan semua metrik yang tersedia untuk Anda.

Metrik	Deskripsi
`NumberOfBackupJobsCreated`	Jumlah pekerjaan cadangan yang AWS Backup dibuat.

Metrik	Deskripsi
`NumberOfBackupJobsPending`	Jumlah pekerjaan cadangan yang akan dijalankan AWS Backup.
`NumberOfBackupJobsRunning`	Jumlah pekerjaan cadangan yang saat ini berjalan di AWS Backup.
`NumberOfBackupJobsAborted`	Jumlah pengguna membatalkan pekerjaan cadangan.
`NumberOfBackupJobsCompleted`	Jumlah pekerjaan cadangan yang AWS Backup selesai.
`NumberOfBackupJobsFailed`	Jumlah pekerjaan cadangan dengan status`Failed`. Sering disebabkan oleh penjadwalan pekerjaan cadangan selama atau 1 jam sebelum sumber daya database atau 4 jam sebelum atau selama jendela pemelihar aan Amazon FSx atau jendela pencadangan otomatis dan tidak AWS Backup menggunak an untuk melakukan pencadangan point-in-time berkelanjutan untuk pemulihan. Lihat Pemulihan Point-in-Time untuk daftar layanan dan petunjuk yang didukung tentang cara menggunakan AWS Backup untuk melakukan pencadangan berkelanjutan, atau menjadwal ulang pekerjaan pencadangan Anda.
`NumberOfBackupJobsExpired`	Jumlah pekerjaan cadangan yang memiliki status`EXPIRED`. Pekerjaan cadangan berubah dari status `CREATED` menjadi `EXPIRED` jika cadangan tidak dapat dimulai dalam waktu jendela mulai.
`NumberOfCopyJobsCreated`	Jumlah pekerjaan penyalinan lintas akun dan lintas wilayah yang AWS Backup dibuat.

Metrik	Deskripsi
NumberOfCopyJobsRunning	Jumlah pekerjaan penyalinan lintas akun dan lintas wilayah yang saat ini berjalan di. AWS Backup
NumberOfCopyJobsCompleted	Jumlah pekerjaan penyalinan lintas akun dan lintas wilayah yang AWS Backup selesai.
NumberOfCopyJobsFailed	Jumlah pekerjaan penyalinan lintas akun dan lintas wilayah yang AWS Backup dicoba tetapi tidak dapat diselesaikan.
NumberOfRestoreJobsPending	Jumlah pekerjaan pemulihan yang akan dijalankan AWS Backup.
NumberOfRestoreJobsRunning	Jumlah pekerjaan pemulihan yang saat ini berjalan di AWS Backup.
NumberOfRestoreJobsCompleted	Jumlah pekerjaan pemulihan yang AWS Backup selesai.
NumberOfRestoreJobsFailed	Jumlah pekerjaan pemulihan yang AWS Backup berusaha tetapi tidak dapat diselesai kan.
NumberOfRecoveryPointsCompleted	Jumlah titik pemulihan yang AWS Backup dibuat.
NumberOfRecoveryPointsPartial	Jumlah titik pemulihan yang AWS Backup mulai dibuat tetapi tidak bisa selesai. AWS mencoba kembali prosesnya nanti, tetapi karena percobaan ulang terjadi di lain waktu, ia mempertahankan titik pemulihan parsi.

Metrik	Deskripsi
`NumberOfRecoveryPointsExpired`	Jumlah titik pemulihan yang AWS Backup mencoba menghapus berdasarkan siklus hidup retensi cadangan Anda, tetapi tidak dapat dihapus. Anda ditagih untuk penyimpanan yang digunakan cadangan kedaluwarsa dan harus menghapusnya secara manual.
`NumberOfRecoveryPointsDeleting`	Jumlah titik pemulihan yang AWS Backup dihapus.
`NumberOfRecoveryPointsCold`	Jumlah titik pemulihan yang AWS Backup berjenjang ke cold storage.

Lebih banyak dimensi tersedia di luar yang tercantum dalam tabel. Untuk melihat semua dimensi metrik, ketikkan nama metrik tersebut ke dalam `AWS/Backup` namespace bagian Metrik konsol. CloudWatch

Logging panggilan AWS Backup API dengan CloudTrail

AWS Backup terintegrasi dengan layanan AWS CloudTrailyang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS layanan. CloudTrail menangkap semua panggilan API untuk AWS Backup sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari AWS Backup konsol dan panggilan kode ke operasi AWS Backup API. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Backup, alamat IP dari mana permintaan dibuat, kapan dibuat, dan detail tambahan.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut hal ini:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail Acara di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrailDanau.

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan AWS Management Console Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak. Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat Membuat jejak untuk Anda Akun AWS dan Membuat jejak untuk organisasi di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat Bekerja dengan AWS CloudTrail Danau di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa,

dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

AWS Backup peristiwa di CloudTrail

AWS Backup menghasilkan CloudTrail peristiwa ini saat melakukan pencadangan, pemulihan, salinan, atau pemberitahuan. Peristiwa ini belum tentu dihasilkan dengan menggunakan API AWS Backup publik. Untuk informasi selengkapnya, lihat Layanan AWS peristiwa di Panduan AWS CloudTrail Pengguna.

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

Memahami entri file AWS Backup log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan`StartBackupJob`,`StartRestoreJob`, dan `DeleteRecoveryPoint` tindakan dan juga `BackupJobCompleted` acara.

```
{
    "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"
    }
}
```


Pencatatan peristiwa manajemen lintas akun

Dengan AWS Backup, Anda dapat mengelola cadangan Anda di semua Akun AWS bagian dalam struktur Anda AWS Organizations. AWS Backup menghasilkan CloudTrail peristiwa ini ketika Anda membuat, memperbarui, atau menghapus kebijakan AWS Organizations cadangan (yang menerapkan rencana cadangan ke akun anggota Anda) atau ketika ada rencana cadangan organisasi yang tidak valid:

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationalBackupPlan`

Contoh: entri file AWS Backup log untuk manajemen lintas akun

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateOrganizationalBackupPlan` tindakan.


```
{
    "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"
    }
}
```


Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `DeleteOrganizationalBackupPlan` tindakan.


```
{
    "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"
    }
}
```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan peristiwa`InvalidOrganizationBackupPlan`, yang dikirim saat AWS Backup menerima rencana cadangan yang tidak valid dari 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"
}
```

Opsi pemberitahuan dengan AWS Backup

Ada dua cara untuk menerima pemberitahuan tentang AWS Backup:

- AWS Pemberitahuan Pengguna dapat mengirim notifikasi, termasuk CloudWatch alarm Amazon AWS Support, dan notifikasi layanan lainnya.
- Amazon Simple Notification Service dapat memberi tahu Anda tentang AWS Backup acara.

AWS Pemberitahuan Pengguna dan AWS Backup

AWS Backup mendukung pengelolaan pemberitahuan cadangan Anda dari konsol Pemberitahuan AWS Pengguna. Dengan Pemberitahuan AWS Pengguna, Anda dapat melihat kemajuan pencadangan, menyalin, dan memulihkan pekerjaan dan perubahan pada kebijakan pencadangan, brankas, titik pemulihan, dan pengaturan Anda dari Pusat Pemberitahuan Pemberitahuan Pengguna.

Amazon CloudWatch, EventBridge alarm Amazon, dan pembaruan AWS Support kasus adalah beberapa jenis notifikasi lain yang dapat Anda kelola dari konsol. Selain itu, Anda dapat mengatur beberapa opsi pengiriman, termasuk email, AWS Chatbot notifikasi, dan pemberitahuan AWS Console Mobile Application push.

Amazon SNS dan acara AWS Backup

AWS Backup memanfaatkan notifikasi kuat yang dikirimkan oleh Amazon Simple Notification Service (Amazon SNS). Anda dapat mengonfigurasi Amazon SNS untuk memberi tahu Anda tentang AWS Backup peristiwa dari konsol Amazon SNS.

Batasan

- Meskipun layanan Amazon SNS memungkinkan pemberitahuan lintas akun, saat ini AWS Backup tidak mendukung fitur ini. Anda harus menentukan ID AWS akun Anda sendiri dan ARN sumber daya topik Anda.
- AWS Backup mendukung topik Standar untuk deduplikasi upaya terbaik SNS, tetapi saat ini AWS Backup tidak mendukung topik SNS FIFO untuk deduplikasi Ketat.

Kasus penggunaan umum

- Siapkan notifikasi untuk pekerjaan pencadangan yang gagal dengan mengikuti langkah-langkah di Bagaimana saya bisa mendapatkan notifikasi untuk AWS Backup pekerjaan yang gagal? dari AWS Premium Support.
- Tinjau contoh JSON notifikasi Amazon SNS untuk pekerjaan pencadangan yang telah selesai, gagal, dan kedaluwarsa dalam tabel Contoh peristiwa di bawah ini.

Untuk informasi selengkapnya tentang Amazon SNS secara umum, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

AWS Backup API pemberitahuan

Setelah membuat topik menggunakan konsol Amazon SNS atau AWS Command Line Interface (AWS CLI), Anda dapat menggunakan operasi AWS Backup API berikut untuk mengelola notifikasi pencadangan.

- DeleteBackupVaultNotifications— Menghapus pemberitahuan acara untuk brankas cadangan yang ditentukan.
- GetBackupVaultNotifications— Daftar semua pemberitahuan acara untuk brankas cadangan yang ditentukan.
- PutBackupVaultNotifications— Mengaktifkan notifikasi untuk topik dan acara yang ditentukan.

AWS Backup mendukung acara berikut:

Jenis Tugas	Peristiwa
Pekerjaan Backup	`BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `CONTINUOUS_BACKUP_INTERRUPTED`
Salin pekerjaan	`COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
Kembalikan pekerjaan	`RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED`
Titik pemulihan	`RECOVERY_POINT_MODIFIED`

AWS Backup untuk S3 mendukung dua acara tambahan:

- `S3_BACKUP_OBJECT_FAILED`memberi tahu Anda tentang objek S3 apa pun yang AWS Backup gagal dicadangkan selama pekerjaan pencadangan.
- `S3_RESTORE_OBJECT_FAILED`memberi tahu Anda tentang objek S3 yang AWS Backup gagal dipulihkan selama pekerjaan pemulihan.

Contoh acara

Example Contoh: Pekerjaan Backup selesai

```
{
    "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 Contoh: Pekerjaan Backup gagal

```
{
    "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 Contoh: Pekerjaan Backup tidak dapat diselesaikan selama jendela 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 contoh perintah pemberitahuan

Anda dapat menggunakan AWS CLI perintah untuk berlangganan, daftar, dan menghapus notifikasi Amazon SNS untuk acara Anda AWS Backup .

Contoh menempatkan pemberitahuan brankas cadangan

Perintah berikut berlangganan topik Amazon SNS untuk vault cadangan tertentu yang memberi tahu Anda saat pekerjaan pemulihan dimulai atau diselesaikan, atau saat titik pemulihan diubah.

```
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
```

Contoh mendapatkan pemberitahuan brankas cadangan

Perintah berikut mencantumkan semua peristiwa yang saat ini berlangganan topik Amazon SNS untuk vault cadangan yang ditentukan.

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

Output sampel adalah sebagai berikut:

```
{
    "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"
}
```

Contoh menghapus pemberitahuan brankas cadangan

Perintah berikut berhenti berlangganan dari topik Amazon SNS untuk vault cadangan yang ditentukan.

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

Menentukan AWS Backup sebagai kepala layanan

> **Note**
>
> Untuk memungkinkan AWS Backup mempublikasikan topik SNS atas nama Anda, Anda harus menentukan AWS Backup sebagai kepala layanan.

Sertakan JSON berikut dalam kebijakan akses topik Amazon SNS yang Anda gunakan untuk AWS Backup melacak peristiwa. Anda harus menentukan sumber daya Amazon Resource Name (ARN) topik Anda.

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Untuk informasi selengkapnya tentang menentukan prinsip layanan dalam kebijakan akses Amazon SNS, lihat Mengizinkan Sumber Daya AWS Apa Pun Menerbitkan ke Topik di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

> **Note**
>
> Jika topik Anda dienkripsi, Anda harus menyertakan izin tambahan dalam kebijakan Anda agar dapat AWS Backup mempublikasikannya. Untuk informasi selengkapnya tentang mengaktifkan layanan untuk dipublikasikan ke topik terenkripsi, lihat Mengaktifkan Kompatibilitas antara Sumber Peristiwa dari AWS Layanan dan Topik Terenkripsi di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Pemecahan masalah AWS Backup

Saat Anda menggunakannya AWS Backup, Anda mungkin mengalami masalah. Bagian berikut dapat membantu Anda memecahkan masalah beberapa masalah umum yang mungkin terjadi.

Untuk pertanyaan umum tentang AWS Backup, lihat AWS Backup FAQ. Anda juga dapat mencari jawaban dan memposting pertanyaan di AWS Backup forum.

Topik

Memecahkan masalah umum

Ketika Anda mencadangkan dan memulihkan sumber daya, Anda harus memiliki izin untuk menggunakan AWS Backup dan izin untuk mengakses sumber daya yang ingin Anda lindungi. Cara termudah untuk memiliki izin yang tepat adalah dengan memilih peran Default saat Anda menetapkan sumber daya ke paket cadangan. Untuk informasi selengkapnya tentang kontrol akses menggunakan AWS Identity and Access Management (IAM) dengan AWS Backup, lihatPengendalian akses.

Jika Anda mendapatkan `AccessDenied` kesalahan saat mencoba mengakses AWS Backup sumber daya, seperti brankas cadangan, sumber daya tidak ada atau Anda tidak memiliki izin untuk mengakses sumber daya.

Jika Anda mengalami masalah dengan mencadangkan dan memulihkan jenis sumber daya tertentu, akan sangat membantu untuk meninjau topik pencadangan dan memulihkan pemecahan masalah untuk sumber daya tersebut. Untuk informasi selengkapnya, lihat tautan di bawah Cara AWS Backup kerja dengan AWS layanan yang didukung.

Jika AWS Backup gagal membuat atau menghapus sumber daya, Anda dapat mempelajari lebih lanjut tentang masalah ini dengan menggunakan AWS CloudTrail untuk melihat pesan kesalahan atau log. Untuk informasi lebih lanjut tentang menggunakan CloudTrail with AWS Backup, lihatLogging panggilan AWS Backup API dengan CloudTrail.

Memecahkan masalah pembuatan sumber daya

Informasi berikut dapat membantu Anda memecahkan masalah dengan membuat cadangan.

- Secara umum, layanan AWS database tidak dapat memulai pencadangan 1 jam sebelum atau selama jendela pemeliharaan atau jendela pencadangan otomatis. Amazon FSx tidak dapat memulai pencadangan 4 jam sebelum atau selama jendela pemeliharaan atau jendela cadangan otomatis (Amazon Aurora dikecualikan dari pembatasan jendela pemeliharaan ini). Pencadangan snapshot yang dijadwalkan selama waktu itu akan gagal. Satu pengecualian: ketika Anda memilih AWS Backup untuk menggunakan snapshot dan backup berkelanjutan untuk layanan yang didukung, Anda tidak perlu lagi khawatir tentang jendela tersebut karena AWS Backup akan menjadwalkannya untuk Anda. Lihat Point-in-Time Recovery untuk daftar layanan yang didukung dan petunjuk tentang cara menggunakan AWS Backup untuk melakukan backup berkelanjutan.
- Membuat backup untuk tabel DynamoDB akan gagal saat tabel sedang dibuat. Membuat tabel DynamoDB biasanya membutuhkan waktu beberapa menit.
- Mencadangkan sistem file Amazon EFS dapat memakan waktu hingga 7 hari ketika sistem file sangat besar. Hanya satu cadangan bersamaan pada satu waktu yang dapat diantri untuk sistem file Amazon EFS. Jika cadangan berikutnya diantrian sementara yang sebelumnya masih dalam proses, jendela cadangan dapat kedaluwarsa dan tidak ada cadangan yang dibuat.
- Amazon EBS memiliki kuota lunak 100.000 backup Wilayah AWS per akun, dan cadangan tambahan gagal ketika kuota ini tercapai. Jika Anda mencapai kuota ini, Anda dapat menghapus cadangan berlebih atau meminta kenaikan kuota. Untuk informasi selengkapnya tentang meminta peningkatan kuota, lihat Service AWS Quotas.
- Saat membuat backup Amazon Relational Database Service (RDS), pertimbangkan hal berikut:
  - Jika Anda tidak menggunakan AWS Backup untuk mengelola snapshot Amazon RDS dan pencadangan berkelanjutan dengan point-in-time pemulihan, pencadangan Anda akan gagal jika dimulai jika dijadwalkan atau dibuat sesuai permintaan selama jendela pencadangan 30 menit harian yang dapat dikonfigurasi pengguna. Untuk informasi selengkapnya tentang backup Amazon RDS otomatis, lihat Bekerja Dengan Cadangan di Panduan Pengguna Amazon RDS. Anda dapat menghindari batasan ini dengan menggunakan AWS Backup untuk mengelola snapshot Amazon RDS dan pencadangan berkelanjutan dengan pemulihan. point-in-time
  - Jika Anda memulai pekerjaan pencadangan dari konsol Amazon RDS, ini dapat bertentangan dengan pekerjaan pencadangan klaster Aurora, menyebabkan kesalahan `Backup job expired before completion.` Jika ini terjadi, konfigurasikan jendela cadangan yang lebih panjang. AWS Backup

- AWS Backup saat ini tidak meneruskan grup opsi TDE saat pekerjaan salinan dibuat. Jika Anda bermaksud menggunakan grup opsi ini untuk menyalin pekerjaan, Anda harus menggunakan konsol Amazon RDS atau Amazon RDS API alih-alih AWS Backup alat. Lihat Menyalin grup opsi di Panduan Pengguna Amazon Relational Database Service untuk informasi selengkapnya.
- KESALAHAN: Pencadangan sesuai permintaan selesai tetapi pencadangan terjadwal gagal dengan kesalahan “Kunci KMS snapshot sumber tidak ada, tidak diaktifkan atau Anda tidak memiliki izin untuk mengaksesnya.” Pekerjaan sesuai permintaan selesai karena menggunakan panggilan API`CopyDBSnapshot`, yang tidak memerlukan akses KMS.

  OBAT: Tambahkan peran IAM ke kunci KMS Anda. Ini dapat dilakukan dengan mengizinkan peran pada kebijakan kunci KMS Anda.

  Untuk mengedit kebijakan Anda,

  1. Buka konsol KMS.
  2. Pilih kunci yang dikelola pelanggan di navigasi kiri.
  3. Klik kunci terkelola pelanggan yang ingin Anda edit.
  4. Di bawah Kebijakan utama, klik Beralih ke tampilan kebijakan.
  5. Klik Edit.
  6. Tambahkan peran.

Memecahkan masalah menghapus sumber daya

Poin pemulihan yang dibuat oleh AWS Backup tidak dapat dihapus di jendela konsol sumber daya yang dilindungi. Anda dapat menghapusnya di AWS Backup konsol dengan memilihnya di brankas tempat penyimpanan dan kemudian memilih Hapus.

Untuk menghapus titik pemulihan atau brankas cadangan, Anda memerlukan izin yang sesuai. Untuk informasi selengkapnya tentang kontrol akses menggunakan IAM dengan AWS Backup, lihatPengendalian akses.

Memecahkan masalah memulihkan sumber daya

Memulihkan menggunakan API

Untuk memulihkan cadangan secara terprogram, gunakan operasi StartRestoreJob API.

Untuk mendapatkan metadata konfigurasi tempat cadangan Anda dibuat, Anda dapat menelepon. GetRecoveryPointRestoreMetadata

Lihat Memulihkan cadangan untuk informasi selengkapnya.

Memulihkan menggunakan Konsol

- Memulihkan data Amazon S3
- Memulihkan mesin virtual
- Memulihkan sistem file Amazon FSx
- Memulihkan volume Amazon EBS
- Memulihkan sistem file Amazon EFS
- Memulihkan tabel Amazon DynamoDB
- Memulihkan database Amazon RDS
- Memulihkan cluster Aurora
- Memulihkan instans Amazon EC2
- Memulihkan volume Storage Gateway
- Memulihkan cluster Amazon DocumentDB
- Memulihkan cluster Neptunus

Memecahkan masalah kesalahan pemformatan

Ketika wildcard (*) disertakan untuk nilai dalam parameter, wildcard diproses untuk menyertakan nilai selain spasi putih. Nilai dalam pasangan kunci-nilai yang berisi spasi putih tidak akan disertakan sebagai bagian dari wildcard.

API AWS Backup

Selain menggunakan konsol, Anda dapat menggunakanAWS BackupTindakan API dan tipe data untuk mengonfigurasi dan mengelola secara terprogramAWS Backupdan sumber dayanya. Bagian ini menjelaskanAWS Backuptindakan dan tipe data. Ini berisi referensi API untukAWS Backup.

AWS BackupAPI

- AWS BackupTindakan
- AWS BackupTipe Data

Tindakan

Tindakan berikut didukung olehAWS 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

Tindakan berikut didukung olehAWS 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

Tindakan berikut didukung olehAWS 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

Layanan: AWS Backup

Menghapus penahanan hukum yang ditentukan pada titik pemulihan. Tindakan ini hanya dapat dilakukan oleh pengguna dengan izin yang memadai.

Minta Sintaks

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

CancelDescription

String yang menjelaskan alasan untuk menghapus pegangan hukum.

Wajib: Ya

legalHoldId

ID penahanan hukum.

Wajib: Ya

RetainRecordInDays

Jumlah bilangan bulat, dalam beberapa hari, setelah itu untuk menghapus penahanan hukum.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 201
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 201 dengan badan HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidResourceStateException

AWS Backup sudah melakukan tindakan pada titik pemulihan ini. Itu tidak dapat melakukan tindakan yang Anda minta sampai tindakan pertama selesai. Coba lagi nanti.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateBackupPlan

Layanan: AWS Backup

Membuat rencana cadangan menggunakan nama rencana cadangan dan aturan cadangan. Rencana cadangan adalah dokumen yang berisi informasi yang AWS Backup digunakan untuk menjadwalkan tugas yang membuat titik pemulihan untuk sumber daya.

Jika Anda menelepon `CreateBackupPlan` dengan paket yang sudah ada, Anda menerima `AlreadyExistsException` pengecualian.

Minta Sintaks

```
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"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

BackupPlan

Tubuh rencana cadangan. Termasuk satu `BackupPlanName` dan satu atau lebih set`Rules`.

Tipe: Objek BackupPlanInput

Wajib: Ya

BackupPlanTags

Tag untuk ditetapkan ke rencana cadangan.

Tipe: Peta antar string

Wajib: Tidak

CreatorRequestId

Mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Jika permintaan menyertakan `CreatorRequestId` yang cocok dengan rencana cadangan yang ada, paket tersebut dikembalikan. Parameter ini bersifat opsional.

Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AdvancedBackupSettings

Pengaturan untuk jenis sumber daya. Opsi ini hanya tersedia untuk pekerjaan cadangan Windows Volume Shadow Copy Service (VSS).

Tipe: Array objek AdvancedBackupSetting

BackupPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`

Jenis: String

BackupPlanId

ID dari rencana cadangan.

Jenis: String

CreationDate

Tanggal dan waktu rencana cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

VersionId

String berkode UTF-8, Unicode, yang dihasilkan secara acak dan unik, dengan panjang maksimal 1.024 byte. Mereka tidak dapat diedit.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateBackupSelection

Layanan: AWS Backup

Membuat dokumen JSON yang menentukan satu set sumber daya untuk menetapkan rencana cadangan. Sebagai contoh, lihat Menetapkan sumber daya secara terprogram.

Minta Sintaks

```
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"
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

ID dari rencana cadangan.

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

BackupSelection

Badan permintaan untuk menetapkan satu set sumber daya ke rencana cadangan.

Tipe: Objek BackupSelection

Wajib: Ya

CreatorRequestId

String unik yang mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Parameter ini bersifat opsional.

Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlanId

ID dari rencana cadangan.

Jenis: String

CreationDate

Tanggal dan waktu pemilihan cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

SelectionId

Secara unik mengidentifikasi badan permintaan untuk menetapkan satu set sumber daya ke rencana cadangan.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript

- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateBackupVault

Layanan: AWS Backup

Membuat kontainer logis tempat cadangan disimpan. Permintaan `CreateBackupVault` mencakup nama, secara opsional satu atau beberapa tanda sumber daya, kunci enkripsi, dan ID permintaan.

> **Note**
>
> Jangan sertakan data sensitif, seperti nomor paspor, atas nama brankas cadangan.

Minta Sintaks

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat. Mereka terdiri dari huruf, angka, dan tanda hubung.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

BackupVaultTags

Tag yang akan ditetapkan ke brankas cadangan.

Tipe: Peta antar string

Wajib: Tidak

CreatorRequestId

String unik yang mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Parameter ini bersifat opsional.

Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

EncryptionKeyArn

Kunci enkripsi sisi server yang digunakan untuk melindungi cadangan Anda; misalnya, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipe: String

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Jenis: String

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah tempatnya dibuat. Ia terdiri dari huruf kecil, angka, dan tanda hubung.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

Tanggal dan waktu penyimpanan cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateFramework

Layanan: AWS Backup

Membuat kerangka kerja dengan satu atau lebih kontrol. Framework adalah kumpulan kontrol yang dapat Anda gunakan untuk mengevaluasi praktik pencadangan Anda. Dengan menggunakan kontrol yang dapat disesuaikan sebelumnya untuk menentukan kebijakan, Anda dapat mengevaluasi apakah praktik pencadangan sesuai dengan kebijakan Anda dan sumber daya mana yang belum sesuai.

Minta Sintaks

```
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"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

FrameworkControls

Kontrol yang membentuk kerangka kerja. Setiap kontrol dalam daftar memiliki nama, parameter input, dan ruang lingkup.

Tipe: Array objek FrameworkControl

Wajib: Ya

FrameworkDescription

Deskripsi opsional kerangka kerja dengan maksimum 1.024 karakter.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 1024.

Pola: `.*\S.*`

Wajib: Tidak

FrameworkName

Nama unik kerangka kerja. Nama harus antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

FrameworkTags

Tag untuk menetapkan kerangka kerja.

Tipe: Peta antar string

Wajib: Tidak

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `CreateFrameworkInput` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

FrameworkArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Jenis: String

FrameworkName

Nama unik kerangka kerja. Nama harus antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateLegalHold

Layanan: AWS Backup

Membuat penahanan hukum pada titik pemulihan (cadangan). Penahanan hukum adalah pengekangan untuk mengubah atau menghapus cadangan sampai pengguna yang berwenang membatalkan penahanan hukum. Setiap tindakan untuk menghapus atau memisahkan titik pemulihan akan gagal dengan kesalahan jika satu atau lebih penahanan hukum aktif berada di titik pemulihan.

Minta Sintaks

```
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"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

Description

Deskripsi penahanan hukum.

Tipe: String

Diperlukan: Ya

IdempotencyToken

Ini adalah string yang dipilih pengguna yang digunakan untuk membedakan antara panggilan yang identik. Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

RecoveryPointSelection

Kriteria untuk menetapkan satu set sumber daya, seperti jenis sumber daya atau brankas cadangan.

Tipe: Objek RecoveryPointSelection

Wajib: Tidak

Tags

Tag opsional untuk disertakan. Tag adalah pasangan kunci-nilai yang dapat Anda gunakan untuk mengelola, memfilter, dan mencari sumber daya Anda. Karakter yang diizinkan termasuk huruf UTF-8, angka, spasi, dan karakter berikut: + - =. _: /.

Tipe: Peta antar string

Wajib: Tidak

Title

Judul pegangan hukum.

Tipe: String

Diperlukan: Ya

Sintaksis Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CreationDate

Waktu ketika penahanan hukum dibuat.

Tipe: Timestamp

Description

Deskripsi penahanan hukum.

Jenis: String

LegalHoldArn

Nama Sumber Daya Amazon (ARN) dari penangguhan hukum.

Jenis: String

LegalHoldId

ID penahanan hukum.

Jenis: String

RecoveryPointSelection

Kriteria untuk menetapkan ke satu set sumber daya, seperti jenis sumber daya atau brankas cadangan.

Tipe: Objek RecoveryPointSelection

Status

Status penahanan hukum.

Jenis: String

Nilai yang Valid: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

Judul pegangan hukum.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateLogicallyAirGappedBackupVault

Layanan: AWS Backup

Membuat wadah logis ke tempat cadangan dapat disalin.

Permintaan ini mencakup nama, Wilayah, jumlah maksimum hari penyimpanan, jumlah minimum hari penyimpanan, dan secara opsional dapat menyertakan tag dan ID permintaan pembuat konten.

> **Note**
>
> Jangan sertakan data sensitif, seperti nomor paspor, atas nama brankas cadangan.

Minta Sintaks

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Secara logis brankas cadangan celah udara diidentifikasi dengan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah tempat mereka dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

BackupVaultTags

Tag untuk menetapkan ke lemari besi.

Tipe: Peta antar string

Wajib: Tidak

CreatorRequestId

ID permintaan pembuatan.

Parameter ini bersifat opsional. Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

MaxRetentionDays

Periode retensi maksimum bahwa brankas mempertahankan titik pemulihannya. Jika parameter ini tidak ditentukan, AWS Backup tidak memberlakukan periode retensi maksimum pada titik pemulihan di brankas (memungkinkan penyimpanan tidak terbatas).

Jika ditentukan, pekerjaan pencadangan atau penyalinan apa pun ke vault harus memiliki kebijakan siklus hidup dengan periode penyimpanan yang sama atau lebih pendek dari periode retensi maksimum. Jika periode retensi pekerjaan lebih lama dari periode retensi maksimum tersebut, vault akan gagal melakukan pekerjaan pencadangan atau penyalinan, dan Anda harus mengubah setelan siklus hidup atau menggunakan brankas yang berbeda.

Tipe: Long

Wajib: Ya

MinRetentionDays

Setelan ini menentukan periode retensi minimum dimana vault mempertahankan titik pemulihannya. Jika parameter ini tidak ditentukan, tidak ada periode retensi minimum yang diberlakukan.

Jika ditentukan, pekerjaan pencadangan atau penyalinan apa pun ke vault harus memiliki kebijakan siklus hidup dengan periode penyimpanan yang sama dengan atau lebih lama dari periode penyimpanan minimum. Jika periode retensi pekerjaan lebih pendek dari periode retensi minimum tersebut, vault akan gagal melakukan pencadangan atau penyalinan pekerjaan, dan Anda harus mengubah setelan siklus hidup atau menggunakan brankas yang berbeda.

Tipe: Long

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupVaultArn

ARN (Nama Sumber Daya Amazon) dari lemari besi.

Jenis: String

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Secara logis brankas cadangan celah udara diidentifikasi dengan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah tempat mereka dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

Tanggal dan waktu ketika lemari besi dibuat.

Nilai ini dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

VaultState

Keadaan lemari besi saat ini.

Jenis: String

Nilai yang Valid: `CREATING | AVAILABLE | FAILED`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateReportPlan

Layanan: AWS Backup

Membuat rencana laporan. Rencana laporan adalah dokumen yang berisi informasi tentang isi laporan dan di mana AWS Backup akan mengirimkannya.

Jika Anda menelepon `CreateReportPlan` dengan paket yang sudah ada, Anda menerima `AlreadyExistsException` pengecualian.

Minta Sintaks

```
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"
   }
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `CreateReportPlanInput` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

ReportDeliveryChannel

Struktur yang berisi informasi tentang tempat dan cara mengirimkan laporan, khususnya nama bucket Amazon S3, key prefix S3, dan format laporan Anda.

Tipe: Objek ReportDeliveryChannel

Wajib: Ya

ReportPlanDescription

Deskripsi opsional dari rencana laporan dengan maksimum 1.024 karakter.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 1024.

Pola: `.*\S.*`

Wajib: Tidak

ReportPlanName

Nama unik dari rencana laporan. Nama harus antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

ReportPlanTags

Tag untuk ditetapkan ke rencana laporan.

Tipe: Peta antar string

Wajib: Tidak

ReportSetting

Mengidentifikasi template laporan untuk laporan. Laporan dibuat menggunakan template laporan. Template laporan adalah:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Jika template laporan adalah `RESOURCE_COMPLIANCE_REPORT` atau`CONTROL_COMPLIANCE_REPORT`, sumber daya API ini juga menjelaskan cakupan laporan oleh Wilayah AWS dan kerangka kerja.

Tipe: Objek ReportSetting

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CreationTime

Tanggal dan waktu penyimpanan cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

ReportPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Jenis: String

ReportPlanName

Nama unik dari rencana laporan.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateRestoreTestingPlan

Layanan: AWS Backup

Membuat rencana pengujian pemulihan.

Langkah pertama dari dua langkah untuk membuat rencana pengujian pemulihan. Setelah permintaan ini berhasil, selesaikan prosedur menggunakan CreateRestoreTestingSelection.

Minta Sintaks

```
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"
   }
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

CreatorRequestId

Ini adalah string unik yang mengidentifikasi permintaan dan memungkinkan permintaan gagal diambil tanpa risiko menjalankan operasi dua kali. Parameter ini bersifat opsional. Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

RestoreTestingPlan

Rencana pengujian pemulihan harus berisi `RestoreTestingPlanName` string unik yang Anda buat dan harus berisi `ScheduleExpression` cron. Anda dapat secara opsional menyertakan `StartWindowHours` integer dan string. `CreatorRequestId`

`RestoreTestingPlanName`Ini adalah string unik yang merupakan nama dari rencana pengujian pemulihan. Ini tidak dapat diubah setelah pembuatan, dan harus hanya terdiri dari karakter alfanumerik dan garis bawah.

Tipe: Objek RestoreTestingPlanForCreate

Wajib: Ya

Tags

Tag untuk ditetapkan ke rencana pengujian pemulihan.

Tipe: Peta antar string

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respon HTTP 201.

Layanan mengembalikan data berikut dalam format JSON.

CreationTime

Tanggal dan waktu rencana pengujian pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

RestoreTestingPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana pengujian pemulihan yang dibuat.

Jenis: String

RestoreTestingPlanName

String unik ini adalah nama dari rencana pengujian pemulihan.

Nama tidak dapat diubah setelah penciptaan. Nama ini hanya terdiri dari karakter alfanumerik dan garis bawah. Panjang maksimum adalah 50.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

ConflictException

AWS Backup tidak dapat melakukan tindakan yang Anda minta sampai selesai melakukan tindakan sebelumnya. Coba lagi nanti.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python

- AWS SDK for Ruby V3

CreateRestoreTestingSelection

Layanan: AWS Backup

Permintaan ini dapat dikirim setelah CreateRestoreTestingPlan permintaan berhasil dikembalikan. Ini adalah bagian kedua dari membuat rencana pengujian sumber daya, dan itu harus diselesaikan secara berurutan.

Ini terdiri dari`RestoreTestingSelectionName`,`ProtectedResourceType`, dan salah satu dari yang berikut:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Setiap jenis sumber daya yang dilindungi dapat memiliki satu nilai tunggal.

Pilihan pengujian pemulihan dapat menyertakan nilai wildcard (“*”) untuk `ProtectedResourceArns` bersama dengan`ProtectedResourceConditions`. Atau, Anda dapat menyertakan hingga 30 ARN sumber daya terlindungi tertentu di`ProtectedResourceArns`.

Tidak dapat memilih berdasarkan kedua jenis sumber daya yang dilindungi DAN ARN tertentu. Permintaan akan gagal jika keduanya disertakan.

Minta Sintaks

```
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
   }
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

RestoreTestingPlanName

Masukkan nama rencana pengujian pemulihan yang dikembalikan dari CreateRestoreTestingPlan permintaan terkait.

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

CreatorRequestId

Ini adalah string unik opsional yang mengidentifikasi permintaan dan memungkinkan permintaan gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

RestoreTestingSelection

Ini terdiri dari`RestoreTestingSelectionName`,`ProtectedResourceType`, dan salah satu dari yang berikut:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Setiap jenis sumber daya yang dilindungi dapat memiliki satu nilai tunggal.

Pilihan pengujian pemulihan dapat menyertakan nilai wildcard (“*”) untuk `ProtectedResourceArns` bersama dengan`ProtectedResourceConditions`. Atau, Anda dapat menyertakan hingga 30 ARN sumber daya terlindungi tertentu di`ProtectedResourceArns`.

Tipe: Objek RestoreTestingSelectionForCreate

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respon HTTP 201.

Layanan mengembalikan data berikut dalam format JSON.

CreationTime

Waktu pemilihan pengujian sumber daya dibuat.

Tipe: Timestamp

RestoreTestingPlanArn

ARN dari rencana pengujian pemulihan yang terkait dengan pemilihan pengujian pemulihan.

Jenis: String

RestoreTestingPlanName

Nama rencana pengujian pemulihan.

Nama tidak dapat diubah setelah penciptaan. Nama ini hanya terdiri dari karakter alfanumerik dan garis bawah. Panjang maksimum adalah 50.

Jenis: String

RestoreTestingSelectionName

Nama pilihan pengujian pemulihan untuk rencana pengujian pemulihan terkait.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteBackupPlan

Layanan: AWS Backup

Menghapus rencana cadangan. Rencana cadangan hanya dapat dihapus setelah semua pilihan sumber daya yang terkait telah dihapus. Menghapus paket cadangan akan menghapus versi paket cadangan saat ini. Versi sebelumnya, jika ada, masih akan ada.

Minta Sintaks

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

Secara unik mengidentifikasi rencana cadangan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`

Jenis: String

BackupPlanId

Secara unik mengidentifikasi rencana cadangan.

Jenis: String

DeletionDate

Tanggal dan waktu paket cadangan dihapus, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `DeletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

VersionId

String berkode UTF-8, Unicode, yang dihasilkan secara acak dan unik, dengan panjang maksimal 1.024 byte. ID versi tidak dapat diedit.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteBackupSelection

Layanan: AWS Backup

Menghapus pilihan sumber daya yang terkait dengan rencana cadangan yang ditentukan oleh. `SelectionId`

Minta Sintaks

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

Secara unik mengidentifikasi rencana cadangan.

Wajib: Ya

selectionId

Secara unik mengidentifikasi badan permintaan untuk menetapkan satu set sumber daya ke rencana cadangan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteBackupVault

Layanan: AWS Backup

Menghapus brankas cadangan yang diidentifikasi dengan namanya. Sebuah brankas dapat dihapus hanya jika kosong.

Minta Sintaks

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteBackupVaultAccessPolicy

Layanan: AWS Backup

Menghapus dokumen kebijakan yang mengelola izin di brankas cadangan.

Minta Sintaks

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat. Ia terdiri dari huruf kecil, angka, dan tanda hubung.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteBackupVaultLockConfiguration

Layanan: AWS Backup

Menghapus AWS Backup Vault Lock dari brankas cadangan yang ditentukan oleh nama brankas cadangan.

Jika konfigurasi Vault Lock tidak dapat diubah, maka Anda tidak dapat menghapus Vault Lock menggunakan operasi API, dan Anda akan menerima `InvalidRequestException` jika Anda mencoba melakukannya. Untuk informasi selengkapnya, lihat Kunci Vault di Panduan AWS Backup Pengembang.

Minta Sintaks

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama brankas cadangan untuk menghapus AWS Backup Vault Lock.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript

- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteBackupVaultNotifications

Layanan: AWS Backup

Menghapus pemberitahuan acara untuk brankas cadangan yang ditentukan.

Minta Sintaks

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteFramework

Layanan: AWS Backup

Menghapus kerangka kerja yang ditentukan oleh nama kerangka kerja.

Minta Sintaks

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

frameworkName

Nama unik dari sebuah kerangka kerja.

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

AWS Backup tidak dapat melakukan tindakan yang Anda minta sampai selesai melakukan tindakan sebelumnya. Coba lagi nanti.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteRecoveryPoint

Layanan: AWS Backup

Menghapus titik pemulihan yang ditentukan oleh ID titik pemulihan.

Jika ID titik pemulihan milik cadangan berkelanjutan, memanggil titik akhir ini akan menghapus cadangan berkelanjutan yang ada dan menghentikan pencadangan berkelanjutan masa depan.

Ketika izin peran IAM tidak cukup untuk memanggil API ini, layanan mengirimkan kembali respons HTTP 200 dengan badan HTTP kosong, tetapi titik pemulihan tidak dihapus. Sebaliknya, ia memasuki suatu `EXPIRED` negara.

`EXPIRED`titik pemulihan dapat dihapus dengan API ini setelah peran IAM memiliki `iam:CreateServiceLinkedRole` tindakan. Untuk mempelajari selengkapnya tentang menambahkan peran ini, lihat Memecahkan masalah penghapusan manual.

Jika pengguna atau peran dihapus atau izin dalam peran dihapus, penghapusan tidak akan berhasil dan akan memasuki status. `EXPIRED`

Minta Sintaks

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

recoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

InvalidResourceStateException

AWS Backup sudah melakukan tindakan pada titik pemulihan ini. Itu tidak dapat melakukan tindakan yang Anda minta sampai tindakan pertama selesai. Coba lagi nanti.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteReportPlan

Layanan: AWS Backup

Menghapus rencana laporan yang ditentukan oleh nama rencana laporan.

Minta Sintaks

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

reportPlanName

Nama unik dari rencana laporan.

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

AWS Backup tidak dapat melakukan tindakan yang Anda minta sampai selesai melakukan tindakan sebelumnya. Coba lagi nanti.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteRestoreTestingPlan

Layanan: AWS Backup

Permintaan ini menghapus rencana pengujian pemulihan yang ditentukan.

Penghapusan hanya dapat berhasil terjadi jika semua pilihan pengujian pemulihan terkait dihapus terlebih dahulu.

Minta Sintaks

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

RestoreTestingPlanName

Diperlukan nama unik dari rencana pengujian pemulihan yang ingin Anda hapus.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 204
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 204 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteRestoreTestingSelection

Layanan: AWS Backup

Masukkan nama Restore Testing Plan dan Restore Testing Selection name.

Semua pilihan pengujian yang terkait dengan rencana pengujian pemulihan harus dihapus sebelum rencana pengujian pemulihan dapat dihapus.

Minta Sintaks

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

RestoreTestingPlanName

Diperlukan nama unik dari rencana pengujian pemulihan yang berisi pilihan pengujian pemulihan yang ingin Anda hapus.

Wajib: Ya

RestoreTestingSelectionName

Diperlukan nama unik dari pilihan pengujian pemulihan yang ingin Anda hapus.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 204
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 204 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeBackupJob

Layanan: AWS Backup

Mengembalikan rincian pekerjaan cadangan untuk yang ditentukan`BackupJobId`.

Minta Sintaks

```
GET /backup-jobs/backupJobId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupJobId

Secara unik mengidentifikasi permintaan AWS Backup untuk membuat cadangan sumber daya.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AccountId

Mengembalikan ID akun yang memiliki pekerjaan cadangan.

Jenis: String

Pola: `^[0-9]{12}$`

BackupJobId

Secara unik mengidentifikasi permintaan AWS Backup untuk membuat cadangan sumber daya.

Jenis: String

BackupOptions

Merupakan opsi yang ditentukan sebagai bagian dari rencana cadangan atau pekerjaan cadangan sesuai permintaan.

Tipe: Peta string ke string

Pola Kunci: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Pola nilai: `^[a-zA-Z0-9\-\_\.]{1,50}$`

BackupSizeInBytes

Ukuran, dalam byte, cadangan.

Tipe: Long

BackupType

Merupakan jenis cadangan aktual yang dipilih untuk pekerjaan cadangan. Misalnya, jika cadangan Windows Volume Shadow Copy Service (VSS) yang berhasil diambil, `BackupType` kembali`"WindowsVSS"`. Jika `BackupType` kosong, maka jenis cadangan adalah cadangan biasa.

Jenis: String

BackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Jenis: String

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

BytesTransferred

Ukuran dalam byte ditransfer ke brankas cadangan pada saat status pekerjaan ditanyakan.

Tipe: Long

ChildJobsInState

Ini mengembalikan statistik pekerjaan cadangan anak (bersarang) yang disertakan.

Jenis: String ke peta panjang

Kunci yang Valid: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

CompletionDate

Tanggal dan waktu pekerjaan untuk membuat pekerjaan cadangan selesai, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

CreatedBy

Berisi informasi identifikasi tentang pembuatan pekerjaan cadangan, termasuk `BackupPlanArnBackupPlanId`,`BackupPlanVersion`,, dan `BackupRuleId` rencana cadangan yang digunakan untuk membuatnya.

Tipe: Objek RecoveryPointCreator

CreationDate

Tanggal dan waktu pekerjaan cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

ExpectedCompletionDate

Tanggal dan waktu pekerjaan untuk membuat cadangan sumber daya diharapkan selesai, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `ExpectedCompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

IamRoleArn

Menentukan peran IAM ARN digunakan untuk membuat titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Jenis: String

InitiationDate

Tanggal pekerjaan cadangan dimulai.

Tipe: Timestamp

IsParent

Ini mengembalikan nilai boolean bahwa pekerjaan cadangan adalah pekerjaan induk (komposit).

Jenis: Boolean

MessageCategory

Jumlah pekerjaan untuk kategori pesan yang ditentukan.

Contoh string dapat mencakup`AccessDenied`,, `SUCCESSAGGREGATE_ALL`, dan`INVALIDPARAMETERS`. Lihat Monitoring untuk daftar MessageCategory string yang diterima.

Jenis: String

NumberOfChildJobs

Ini mengembalikan jumlah pekerjaan cadangan anak (bersarang).

Tipe: Long

ParentJobId

Ini mengembalikan ID pekerjaan cadangan sumber daya induk (komposit).

Jenis: String

PercentDone

Berisi perkiraan persentase yang selesai dari pekerjaan pada saat status pekerjaan ditanyakan.

Jenis: String

RecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Jenis: String

ResourceArn

ARN yang secara unik mengidentifikasi sumber daya yang disimpan. Format ARN tergantung pada jenis sumber daya.

Jenis: String

ResourceName

Nama non-unik dari sumber daya yang dimiliki oleh cadangan yang ditentukan.

Jenis: String

ResourceType

Jenis AWS sumber daya yang akan dicadangkan; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS).

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

Menentukan waktu dalam format Unix dan Coordinated Universal Time (UTC) ketika pekerjaan cadangan harus dimulai sebelum dibatalkan. Nilai dihitung dengan menambahkan jendela mulai ke waktu yang dijadwalkan. Jadi jika waktu yang dijadwalkan adalah 6:00 PM dan jendela mulai adalah 2 jam, `StartBy` waktunya akan menjadi 8:00 PM pada tanggal yang ditentukan. Nilai akurat `StartBy` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

State

Keadaan pekerjaan cadangan saat ini.

Jenis: String

Nilai yang Valid: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

Pesan terperinci yang menjelaskan status pekerjaan untuk membuat cadangan sumber daya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

DependencyFailureException

AWS Layanan atau sumber daya dependen mengembalikan kesalahan ke AWS Backup layanan, dan tindakan tidak dapat diselesaikan.

Kode Status HTTP: 500

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeBackupVault

Layanan: AWS Backup

Mengembalikan metadata tentang brankas cadangan yang ditentukan oleh namanya.

Minta Sintaks

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

BackupVaultAccountId

ID akun dari brankas cadangan yang ditentukan.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Jenis: String

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah tempatnya dibuat.

Jenis: String

CreationDate

Tanggal dan waktu pembuatan brankas cadangan, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

CreatorRequestId

String unik yang mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Parameter ini bersifat opsional. Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Jenis: String

EncryptionKeyArn

Kunci enkripsi sisi server yang digunakan untuk melindungi cadangan Anda; misalnya, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Jenis: String

LockDate

Tanggal dan waktu ketika konfigurasi AWS Backup Vault Lock tidak dapat diubah atau dihapus.

Jika Anda menerapkan Vault Lock ke vault tanpa menentukan tanggal penguncian, Anda dapat mengubah setelan Vault Lock, atau menghapus Vault Lock dari vault sepenuhnya, kapan saja.

Nilai ini dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Locked

Boolean yang menunjukkan apakah AWS Backup Vault Lock saat ini melindungi brankas cadangan. `True`berarti bahwa Vault Lock menyebabkan operasi hapus atau perbarui pada titik pemulihan yang disimpan di brankas gagal.

Jenis: Boolean

MaxRetentionDays

Pengaturan AWS Backup Vault Lock yang menentukan periode retensi maksimum tempat vault mempertahankan titik pemulihannya. Jika parameter ini tidak ditentukan, Vault Lock tidak memberlakukan periode retensi maksimum pada titik pemulihan di vault (memungkinkan penyimpanan tidak terbatas).

Jika ditentukan, pekerjaan pencadangan atau penyalinan apa pun ke vault harus memiliki kebijakan siklus hidup dengan periode penyimpanan yang sama atau lebih pendek dari periode retensi maksimum. Jika periode retensi pekerjaan lebih lama dari periode retensi maksimum tersebut, vault akan gagal melakukan pekerjaan pencadangan atau penyalinan, dan Anda harus mengubah setelan siklus hidup atau menggunakan brankas yang berbeda. Titik pemulihan yang sudah disimpan di brankas sebelum Vault Lock tidak terpengaruh.

Tipe: Long

MinRetentionDays

Pengaturan AWS Backup Vault Lock yang menentukan periode retensi minimum tempat vault mempertahankan titik pemulihannya. Jika parameter ini tidak ditentukan, Vault Lock tidak akan menerapkan periode retensi minimum.

Jika ditentukan, pekerjaan pencadangan atau penyalinan apa pun ke vault harus memiliki kebijakan siklus hidup dengan periode penyimpanan yang sama dengan atau lebih lama dari periode penyimpanan minimum. Jika periode retensi pekerjaan lebih pendek dari periode retensi minimum tersebut, vault akan gagal melakukan pekerjaan pencadangan atau penyalinan, dan Anda harus mengubah setelan siklus hidup atau menggunakan brankas yang berbeda. Titik pemulihan yang sudah disimpan di brankas sebelum Vault Lock tidak terpengaruh.

Tipe: Long

NumberOfRecoveryPoints

Jumlah titik pemulihan yang disimpan dalam brankas cadangan.

Tipe: Long

VaultType

Jenis lemari besi yang dijelaskan.

Jenis: String

Nilai yang Valid: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeCopyJob

Layanan: AWS Backup

Mengembalikan metadata yang terkait dengan membuat salinan sumber daya.

Minta Sintaks

```
GET /copy-jobs/copyJobId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

copyJobId

Mengidentifikasi pekerjaan fotokopi secara unik.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CopyJob

Berisi informasi terperinci tentang pekerjaan penyalinan.

Tipe: Objek CopyJob

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeFramework

Layanan: AWS Backup

Mengembalikan rincian kerangka kerja untuk yang ditentukan`FrameworkName`.

Minta Sintaks

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

frameworkName

Nama unik dari sebuah kerangka kerja.

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CreationTime

Tanggal dan waktu kerangka kerja dibuat, dalam representasi ISO 8601. Nilai akurat `CreationTime` untuk milidetik. Misalnya, 2020-07-10T 15:00:00.000-08:00 mewakili tanggal 10 Juli 2020 pukul 15:00 8 jam di belakang UTC.

Tipe: Timestamp

DeploymentStatus

Status penyebaran kerangka kerja. Statusnya adalah:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Jenis: String

FrameworkArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Jenis: String

FrameworkControls

Kontrol yang membentuk kerangka kerja. Setiap kontrol dalam daftar memiliki nama, parameter input, dan ruang lingkup.

Tipe: Array objek FrameworkControl

FrameworkDescription

Deskripsi opsional dari kerangka kerja.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 1024.

Pola: `.*\S.*`

FrameworkName

Nama unik dari sebuah kerangka kerja.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

Framework terdiri dari satu atau lebih kontrol. Setiap kontrol mengatur sumber daya, seperti rencana cadangan, pilihan cadangan, brankas cadangan, atau titik pemulihan. Anda juga dapat mengaktifkan atau menonaktifkan AWS Config perekaman untuk setiap sumber daya. Statusnya adalah:

- `ACTIVE`saat perekaman dihidupkan untuk semua sumber daya yang diatur oleh kerangka kerja.
- `PARTIALLY_ACTIVE`saat perekaman dimatikan untuk setidaknya satu sumber daya yang diatur oleh kerangka kerja.
- `INACTIVE`saat perekaman dimatikan untuk semua sumber daya yang diatur oleh kerangka kerja.
- `UNAVAILABLE`ketika AWS Backup tidak dapat memvalidasi status perekaman saat ini.

Jenis: String

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `DescribeFrameworkOutput` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeGlobalSettings

Layanan: AWS Backup

Menjelaskan apakah AWS akun tersebut dipilih untuk pencadangan lintas akun. Mengembalikan kesalahan jika akun bukan anggota organisasi Organizations. Contoh: `describe-global-settings --region us-west-2`

Minta Sintaks

```
GET /global-settings HTTP/1.1
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GlobalSettings

Status benderaisCrossAccountBackupEnabled.

Tipe: Peta string ke string

LastUpdateTime

Tanggal dan waktu bendera `isCrossAccountBackupEnabled` terakhir diperbarui. Pembaruan ini dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastUpdateTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeProtectedResource

Layanan: AWS Backup

Mengembalikan informasi tentang sumber daya yang disimpan, termasuk terakhir kali dicadangkan, Nama Sumber Daya Amazon (ARN), dan jenis AWS layanan sumber daya yang disimpan.

Minta Sintaks

```
GET /resources/resourceArn HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

resourceArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

LastBackupTime

Tanggal dan waktu sumber daya terakhir dicadangkan, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastBackupTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

LastBackupVaultArn

ARN (Nama Sumber Daya Amazon) dari brankas cadangan yang berisi titik pemulihan cadangan terbaru.

Jenis: String

LastRecoveryPointArn

ARN (Nama Sumber Daya Amazon) dari titik pemulihan terbaru.

Jenis: String

LatestRestoreExecutionTimeMinutes

Waktu, dalam hitungan menit, yang dibutuhkan pekerjaan pemulihan terbaru untuk diselesaikan.

Tipe: Long

LatestRestoreJobCreationDate

Tanggal pembuatan pekerjaan pemulihan terbaru.

Tipe: Timestamp

LatestRestoreRecoveryPointCreationDate

Tanggal titik pemulihan terbaru dibuat.

Tipe: Timestamp

ResourceArn

ARN yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Jenis: String

ResourceName

Nama sumber daya milik cadangan yang ditentukan.

Jenis: String

ResourceType

Jenis AWS sumber daya yang disimpan sebagai titik pemulihan; misalnya, volume Amazon EBS atau database Amazon RDS.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeRecoveryPoint

Layanan: AWS Backup

Mengembalikan metadata yang terkait dengan titik pemulihan, termasuk ID, status, enkripsi, dan siklus hidup.

Minta Sintaks

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

BackupVaultAccountId

ID akun dari brankas cadangan yang ditentukan.

Pola: `^[0-9]{12}$`

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

recoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupSizeInBytes

Ukuran, dalam byte, cadangan.

Tipe: Long

BackupVaultArn

ARN yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Jenis: String

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

Sebuah `CalculatedLifecycle` benda yang berisi `DeleteAt` dan `MoveToColdStorageAt` stempel waktu.

Tipe: Objek CalculatedLifecycle

CompletionDate

Tanggal dan waktu pekerjaan untuk membuat titik pemulihan selesai, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

CompositeMemberIdentifier

Pengidentifikasi sumber daya dalam grup komposit, seperti titik pemulihan bersarang (anak) milik tumpukan komposit (induk). ID ditransfer dari ID logis dalam tumpukan.

Jenis: String

CreatedBy

Berisi informasi identifikasi tentang pembuatan titik pemulihan, termasuk`BackupPlanArn`,`BackupPlanId`,`BackupPlanVersion`, dan `BackupRuleId` rencana cadangan yang digunakan untuk membuatnya.

Tipe: Objek RecoveryPointCreator

CreationDate

Tanggal dan waktu titik pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

EncryptionKeyArn

Kunci enkripsi sisi server yang digunakan untuk melindungi cadangan Anda; misalnya,. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`

Jenis: String

IamRoleArn

Menentukan peran IAM ARN digunakan untuk membuat titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Jenis: String

IsEncrypted

Nilai Boolean yang dikembalikan `TRUE` seolah-olah titik pemulihan yang ditentukan dienkripsi, atau `FALSE` jika titik pemulihan tidak dienkripsi.

Jenis: Boolean

IsParent

Ini mengembalikan nilai boolean bahwa titik pemulihan adalah pekerjaan induk (komposit).

Jenis: Boolean

LastRestoreTime

Tanggal dan waktu titik pemulihan terakhir dipulihkan, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastRestoreTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Lifecycle

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Cadangan yang dialihkan ke cold storage harus disimpan dalam cold storage selama minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Tipe: Objek Lifecycle

ParentRecoveryPointArn

Ini adalah ARN yang secara unik mengidentifikasi titik pemulihan induk (komposit); misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Jenis: String

RecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Jenis: String

ResourceArn

ARN yang secara unik mengidentifikasi sumber daya yang disimpan. Format ARN tergantung pada jenis sumber daya.

Jenis: String

ResourceName

Nama sumber daya milik cadangan yang ditentukan.

Jenis: String

ResourceType

Jenis AWS sumber daya untuk disimpan sebagai titik pemulihan; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS).

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

SourceBackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas sumber daya tempat sumber daya awalnya dicadangkan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault` Jika pemulihan dikembalikan ke AWS akun atau Wilayah yang sama, nilai ini akan menjadi`null`.

Jenis: String

Status

Kode status yang menentukan keadaan titik pemulihan.

`PARTIAL`status menunjukkan tidak AWS Backup dapat membuat titik pemulihan sebelum jendela cadangan ditutup. Untuk meningkatkan jendela paket cadangan menggunakan API, lihat UpdateBackupPlan. Anda juga dapat meningkatkan jendela paket cadangan menggunakan Konsol dengan memilih dan mengedit paket cadangan Anda.

`EXPIRED`Status menunjukkan bahwa titik pemulihan telah melebihi periode retensi, tetapi AWS Backup tidak memiliki izin atau tidak dapat menghapusnya. Untuk menghapus titik pemulihan ini secara manual, lihat Langkah 3: Hapus titik pemulihan di bagian Bersihkan sumber daya Memulai.

`STOPPED`status terjadi pada pencadangan berkelanjutan di mana pengguna telah mengambil beberapa tindakan yang menyebabkan pencadangan berkelanjutan dinonaktifkan. Hal ini dapat disebabkan oleh penghapusan izin, mematikan versi, mematikan acara yang dikirim ke EventBridge, atau menonaktifkan EventBridge aturan yang diberlakukan oleh. AWS Backup

Untuk menyelesaikan STOPPED status, pastikan semua izin yang diminta sudah ada dan pembuatan versi diaktifkan di bucket S3. Setelah kondisi ini terpenuhi, contoh berikutnya dari aturan cadangan yang berjalan akan menghasilkan titik pemulihan berkelanjutan baru yang dibuat. Poin pemulihan dengan status STOPTED tidak perlu dihapus.

Untuk SAP HANA di Amazon STOPPED EC2 status terjadi karena tindakan pengguna, kesalahan konfigurasi aplikasi, atau kegagalan cadangan. Untuk memastikan bahwa backup berkelanjutan masa depan berhasil, lihat status titik pemulihan dan periksa SAP HANA untuk detailnya.

Jenis: String

Nilai yang Valid: `COMPLETED | PARTIAL | DELETING | EXPIRED`

StatusMessage

Pesan status yang menjelaskan status titik pemulihan.

Jenis: String

StorageClass

Menentukan kelas penyimpanan dari titik pemulihan. Nilai yang valid adalah `WARM` atau `COLD`.

Jenis: String

Nilai yang Valid: `WARM | COLD | DELETED`

VaultType

Jenis lemari besi tempat titik pemulihan yang dijelaskan disimpan.

Jenis: String

Nilai yang Valid: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeRegionSettings

Layanan: AWS Backup

Mengembalikan pengaturan keikutsertaan layanan saat ini untuk Wilayah. Jika keikutsertaan layanan diaktifkan untuk suatu layanan AWS Backup , cobalah untuk melindungi sumber daya layanan tersebut di Wilayah ini, ketika sumber daya disertakan dalam cadangan sesuai permintaan atau rencana pencadangan terjadwal. Jika AWS Backup tidak, jangan mencoba melindungi sumber daya layanan itu di Wilayah ini.

Minta Sintaks

```
GET /account-settings HTTP/1.1
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ResourceTypeManagementPreference

Mengembalikan apakah AWS Backup sepenuhnya mengelola cadangan untuk jenis sumber daya.

Untuk manfaat AWS Backup manajemen penuh, lihat AWS Backup Manajemen penuh.

Untuk daftar jenis sumber daya dan apakah masing-masing mendukung AWS Backup manajemen penuh, lihat tabel Ketersediaan fitur menurut sumber daya.

Jika`"DynamoDB":false`, Anda dapat mengaktifkan AWS Backup manajemen penuh untuk cadangan DynamoDB dengan AWS Backup mengaktifkan fitur cadangan DynamoDB lanjutan.

Jenis: String ke peta boolean

Pola Kunci: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ResourceTypeOptInPreference

Layanan bersama dengan preferensi keikutsertaan di Wilayah.

Jenis: String ke peta boolean

Pola Kunci: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeReportJob

Layanan: AWS Backup

Mengembalikan rincian yang terkait dengan membuat laporan seperti yang ditentukan oleh nya`ReportJobId`.

Minta Sintaks

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

reportJobId

Pengidentifikasi pekerjaan laporan. String unik yang dihasilkan secara acak, Unicode, UTF-8 yang dikodekan dengan panjang paling banyak 1.024 byte. ID pekerjaan laporan tidak dapat diedit.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
    }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ReportJob

Informasi tentang pekerjaan laporan, termasuk waktu penyelesaian dan pembuatannya, tujuan laporan, ID pekerjaan laporan unik, Nama Sumber Daya Amazon (ARN), templat laporan, status, dan pesan status.

Tipe: Objek ReportJob

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeReportPlan

Layanan: AWS Backup

Mengembalikan daftar semua rencana laporan untuk Akun AWS dan Wilayah AWS.

Minta Sintaks

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

reportPlanName

Nama unik dari rencana laporan.

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
      }
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ReportPlan

Mengembalikan rincian tentang rencana laporan yang ditentukan oleh namanya. Rincian ini mencakup Amazon Resource Name (ARN) paket laporan, deskripsi, pengaturan, saluran pengiriman, status penerapan, waktu pembuatan, dan waktu percobaan terakhir dan berhasil dijalankan.

Tipe: Objek ReportPlan

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DescribeRestoreJob

Layanan: AWS Backup

Mengembalikan metadata terkait dengan pekerjaan pemulihan yang ditentukan oleh ID pekerjaan.

Minta Sintaks

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

restoreJobId

Secara unik mengidentifikasi pekerjaan yang mengembalikan titik pemulihan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AccountId

Mengembalikan ID akun yang memiliki pekerjaan pemulihan.

Jenis: String

Pola: `^[0-9]{12}$`

BackupSizeInBytes

Ukuran, dalam byte, dari sumber daya yang dipulihkan.

Tipe: Long

CompletionDate

Tanggal dan waktu pekerjaan untuk memulihkan titik pemulihan selesai, dalam format Unix dan Waktu Universal Terkoordinasi (UTC). Nilai akurat `CompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

CreatedBy

Berisi informasi identifikasi tentang pembuatan pekerjaan pemulihan.

Tipe: Objek RestoreJobCreator

CreatedResourceArn

Nama Sumber Daya Amazon (ARN) dari sumber daya yang dibuat oleh pekerjaan pemulihan.

Format ARN tergantung pada jenis sumber daya dari sumber daya yang dicadangkan.

Jenis: String

CreationDate

Tanggal dan waktu pekerjaan pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

DeletionStatus

Status data yang dihasilkan oleh tes pemulihan.

Jenis: String

Nilai yang Valid: `DELETING | FAILED | SUCCESSFUL`

DeletionStatusMessage

Ini menjelaskan status penghapusan pekerjaan pemulihan.

Jenis: String

ExpectedCompletionTimeMinutes

Jumlah waktu dalam hitungan menit yang diharapkan diambil oleh pekerjaan memulihkan titik pemulihan.

Tipe: Long

IamRoleArn

Menentukan peran IAM ARN digunakan untuk membuat titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Jenis: String

PercentDone

Berisi perkiraan persentase yang selesai dari pekerjaan pada saat status pekerjaan ditanyakan.

Jenis: String

RecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Jenis: String

RecoveryPointCreationDate

Tanggal pembuatan titik pemulihan yang dibuat oleh pekerjaan pemulihan yang ditentukan.

Tipe: Timestamp

ResourceType

Mengembalikan metadata yang terkait dengan pekerjaan pemulihan yang terdaftar berdasarkan jenis sumber daya.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

Secara unik mengidentifikasi pekerjaan yang mengembalikan titik pemulihan.

Jenis: String

Status

Kode status yang menentukan status pekerjaan yang dimulai oleh AWS Backup untuk mengembalikan titik pemulihan.

Jenis: String

Nilai yang Valid: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

Pesan yang menunjukkan status pekerjaan untuk memulihkan titik pemulihan.

Jenis: String

ValidationStatus

Status validasi berjalan pada pekerjaan pemulihan yang ditunjukkan.

Jenis: String

Nilai yang Valid: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

Pesan status.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

DependencyFailureException

AWS Layanan atau sumber daya dependen mengembalikan kesalahan ke AWS Backup layanan, dan tindakan tidak dapat diselesaikan.

Kode Status HTTP: 500

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DisassociateRecoveryPoint

Layanan: AWS Backup

Menghapus titik pemulihan cadangan berkelanjutan yang ditentukan dari AWS Backup dan melepaskan kontrol cadangan berkelanjutan itu ke layanan sumber, seperti Amazon RDS. Layanan sumber akan terus membuat dan mempertahankan pencadangan berkelanjutan menggunakan siklus hidup yang Anda tentukan dalam paket cadangan asli Anda.

Tidak mendukung titik pemulihan cadangan snapshot.

Minta Sintaks

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama unik AWS Backup lemari besi.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

recoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan. AWS Backup

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

InvalidResourceStateException

AWS Backup sudah melakukan tindakan pada titik pemulihan ini. Itu tidak dapat melakukan tindakan yang Anda minta sampai tindakan pertama selesai. Coba lagi nanti.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DisassociateRecoveryPointFromParent

Layanan: AWS Backup

Tindakan ini ke titik pemulihan anak (bersarang) tertentu menghilangkan hubungan antara titik pemulihan yang ditentukan dan titik pemulihan induknya (komposit).

Minta Sintaks

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama wadah logis tempat titik pemulihan anak (bersarang) disimpan. Brankas cadangan diidentifikasi dengan nama yang unik untuk akun yang digunakan untuk membuatnya dan AWS Wilayah tempat pembuatannya.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

recoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan anak (bersarang); misalnya, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 204
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 204 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ExportBackupPlanTemplate

Layanan: AWS Backup

Mengembalikan rencana cadangan yang ditentukan oleh ID rencana sebagai template cadangan.

Minta Sintaks

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

Secara unik mengidentifikasi rencana cadangan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlanTemplateJson

Tubuh template rencana cadangan dalam format JSON.

> **Note**
>
> Ini adalah dokumen JSON yang ditandatangani yang tidak dapat dimodifikasi sebelum diteruskan ke `GetBackupPlanFromJSON`.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetBackupPlan

Layanan: AWS Backup

Mengembalikan `BackupPlan` rincian untuk yang ditentukan`BackupPlanId`. Detailnya adalah isi dari rencana cadangan dalam format JSON, selain metadata rencana.

Minta Sintaks

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

Secara unik mengidentifikasi rencana cadangan.

Wajib: Ya

VersionId

String berkode UTF-8, Unicode, yang dihasilkan secara acak dan unik, dengan panjang maksimal 1.024 byte. ID versi tidak dapat diedit.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AdvancedBackupSettings

Berisi daftar `BackupOptions` untuk setiap jenis sumber daya. Daftar diisi hanya jika opsi lanjutan diatur untuk paket cadangan.

Tipe: Array objek AdvancedBackupSetting

BackupPlan

Menentukan badan rencana cadangan. Termasuk satu `BackupPlanName` dan satu atau lebih set`Rules`.

Tipe: Objek BackupPlan

BackupPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`

Jenis: String

BackupPlanId

Secara unik mengidentifikasi rencana cadangan.

Jenis: String

CreationDate

Tanggal dan waktu rencana cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

CreatorRequestId

String unik yang mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali.

Jenis: String

DeletionDate

Tanggal dan waktu paket cadangan dihapus, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `DeletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

LastExecutionDate

Terakhir kali rencana cadangan ini dijalankan. Tanggal dan waktu, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastExecutionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

VersionId

String berkode UTF-8, Unicode, yang dihasilkan secara acak dan unik, dengan panjang maksimal 1.024 byte. ID versi tidak dapat diedit.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetBackupPlanFromJSON

Layanan: AWS Backup

Mengembalikan dokumen JSON valid yang menentukan rencana cadangan atau kesalahan.

Minta Sintaks

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

BackupPlanTemplateJson

Dokumen rencana cadangan yang disediakan pelanggan dalam format JSON.

Tipe: String

Diperlukan: Ya

Sintaksis Respons

```
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"
         }
      ]
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlan

Menentukan badan rencana cadangan. Termasuk satu `BackupPlanName` dan satu atau lebih set`Rules`.

Tipe: Objek BackupPlan

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetBackupPlanFromTemplate

Layanan: AWS Backup

Mengembalikan template yang ditentukan oleh `templateId` sebagai rencana cadangan.

Minta Sintaks

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

templateId

Secara unik mengidentifikasi template rencana cadangan yang disimpan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
         }
      ]
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlanDocument

Mengembalikan isi rencana cadangan berdasarkan template target, termasuk nama, aturan, dan brankas cadangan rencana.

Tipe: Objek BackupPlan

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python

- AWS SDK for Ruby V3

GetBackupSelection

Layanan: AWS Backup

Mengembalikan metadata pilihan dan dokumen dalam format JSON yang menentukan daftar sumber daya yang terkait dengan rencana cadangan.

Minta Sintaks

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

Secara unik mengidentifikasi rencana cadangan.

Wajib: Ya

selectionId

Secara unik mengidentifikasi badan permintaan untuk menetapkan satu set sumber daya ke rencana cadangan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlanId

Secara unik mengidentifikasi rencana cadangan.

Jenis: String

BackupSelection

Menentukan tubuh permintaan untuk menetapkan satu set sumber daya untuk rencana cadangan.

Tipe: Objek BackupSelection

CreationDate

Tanggal dan waktu pemilihan cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

CreatorRequestId

String unik yang mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali.

Jenis: String

SelectionId

Secara unik mengidentifikasi badan permintaan untuk menetapkan satu set sumber daya ke rencana cadangan.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetBackupVaultAccessPolicy

Layanan: AWS Backup

Mengembalikan dokumen kebijakan akses yang terkait dengan vault cadangan bernama.

Minta Sintaks

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Jenis: String

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Policy

Dokumen kebijakan akses vault cadangan dalam format JSON.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetBackupVaultNotifications

Layanan: AWS Backup

Mengembalikan pemberitahuan acara untuk brankas cadangan yang ditentukan.

Minta Sintaks

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Jenis: String

BackupVaultEvents

Array peristiwa yang menunjukkan status pekerjaan untuk mencadangkan sumber daya ke vault cadangan.

Tipe: Array string

Nilai yang Valid: `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

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

SNSTopicArn

ARN yang secara unik mengidentifikasi topik Amazon Simple Notification Service (Amazon SNS); misalnya, `arn:aws:sns:us-west-2:111122223333:MyTopic`.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetLegalHold

Layanan: AWS Backup

Tindakan ini mengembalikan rincian untuk penangguhan hukum tertentu. Rinciannya adalah badan penahanan hukum dalam format JSON, selain metadata.

Minta Sintaks

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

legalHoldId

ID penahanan hukum.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CancelDescription

Alasan untuk menghapus pegangan hukum.

Jenis: String

CancellationDate

Waktu ketika penangguhan hukum dibatalkan.

Tipe: Timestamp

CreationDate

Waktu ketika penahanan hukum dibuat.

Tipe: Timestamp

Description

Deskripsi penahanan hukum.

Jenis: String

LegalHoldArn

Kerangka ARN untuk penahanan hukum yang ditentukan. Format ARN tergantung pada jenis sumber daya.

Jenis: String

LegalHoldId

ID penahanan hukum.

Jenis: String

RecoveryPointSelection

Kriteria untuk menetapkan satu set sumber daya, seperti jenis sumber daya atau brankas cadangan.

Tipe: Objek RecoveryPointSelection

RetainRecordUntil

Tanggal dan waktu sampai catatan penahanan hukum dipertahankan.

Tipe: Timestamp

Status

Status penahanan hukum.

Jenis: String

Nilai yang Valid: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

Judul pegangan hukum.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetRecoveryPointRestoreMetadata

Layanan: AWS Backup

Mengembalikan satu set metadata pasangan kunci-nilai yang digunakan untuk membuat cadangan.

Minta Sintaks

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

BackupVaultAccountId

ID akun dari brankas cadangan yang ditentukan.

Pola: `^[0-9]{12}$`

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

recoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupVaultArn

ARN yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Jenis: String

RecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Jenis: String

ResourceType

Jenis sumber daya dari titik pemulihan.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreMetadata

Kumpulan pasangan nilai kunci metadata yang menggambarkan konfigurasi asli sumber daya cadangan. Nilai-nilai ini bervariasi tergantung pada layanan yang sedang dipulihkan.

Tipe: Peta string ke string

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript

- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetRestoreJobMetadata

Layanan: AWS Backup

Permintaan ini mengembalikan metadata untuk pekerjaan pemulihan yang ditentukan.

Minta Sintaks

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

restoreJobId

Ini adalah pengidentifikasi unik dari pekerjaan pemulihan di dalamnya AWS Backup.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Metadata

Ini berisi metadata dari pekerjaan cadangan yang ditentukan.

Tipe: Peta string ke string

RestoreJobId

Ini adalah pengidentifikasi unik dari pekerjaan pemulihan di dalamnya AWS Backup.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetRestoreTestingInferredMetadata

Layanan: AWS Backup

Permintaan ini mengembalikan kumpulan metadata minimal yang diperlukan untuk memulai pekerjaan pemulihan dengan pengaturan default yang aman. `BackupVaultName`dan `RecoveryPointArn` merupakan parameter yang diperlukan. `BackupVaultAccountId`adalah parameter opsional.

Minta Sintaks

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

BackupVaultAccountId

ID akun dari brankas cadangan yang ditentukan.

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Brankas cadangan diidentifikasi dengan nama yang unik untuk akun yang digunakan untuk membuatnya dan AWS Wilayah tempat pembuatannya. Mereka terdiri dari huruf, angka, dan tanda hubung.

Wajib: Ya

RecoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

InferredMetadata

Ini adalah peta string dari metadata yang disimpulkan dari permintaan.

Tipe: Peta string ke string

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetRestoreTestingPlan

Layanan: AWS Backup

Mengembalikan `RestoreTestingPlan` rincian untuk yang ditentukan`RestoreTestingPlanName`. Detailnya adalah isi dari rencana pengujian pemulihan dalam format JSON, selain metadata rencana.

Minta Sintaks

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

RestoreTestingPlanName

Diperlukan nama unik dari rencana pengujian pemulihan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

RestoreTestingPlan

Menentukan badan rencana pengujian pemulihan. TermasukRestoreTestingPlanName.

Tipe: Objek RestoreTestingPlanForGet

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetRestoreTestingSelection

Layanan: AWS Backup

Pengembalian RestoreTestingSelection, yang menampilkan sumber daya dan elemen dari rencana pengujian pemulihan.

Minta Sintaks

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

RestoreTestingPlanName

Diperlukan nama unik dari rencana pengujian pemulihan.

Wajib: Ya

RestoreTestingSelectionName

Diperlukan nama unik dari pilihan pengujian pemulihan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

RestoreTestingSelection

Nama unik dari pilihan pengujian pemulihan.

Tipe: Objek RestoreTestingSelectionForGet

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetSupportedResourceTypes

Layanan: AWS Backup

Mengembalikan jenis AWS sumber daya yang didukung oleh AWS Backup.

Minta Sintaks

```
GET /supported-resource-types HTTP/1.1
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ResourceTypes

Berisi string dengan tipe AWS sumber daya yang didukung:

- `Aurora`untuk Amazon Aurora
- `CloudFormation`untuk AWS CloudFormation
- `DocumentDB`untuk Amazon DocumentDB (dengan kompatibilitas MongoDB)
- `DynamoDB`untuk Amazon DynamoDB
- `EBS`untuk Amazon Elastic Block Store

- `EC2`untuk Amazon Elastic Compute Cloud
- `EFS`untuk Amazon Elastic File System
- `FSX`untuk Amazon FSx
- `Neptune`untuk Amazon Neptunus
- `RDS`untuk Amazon Relational Database Service
- `Redshift`untuk Amazon Redshift
- `SAP HANA on Amazon EC2`untuk database SAP HANA pada instans Amazon Elastic Compute Cloud
- `S3`untuk Amazon Simple Storage Service (Amazon S3)
- `Storage Gateway`untuk AWS Storage Gateway
- `Timestream`untuk Amazon Timestream
- `VirtualMachine`untuk mesin virtual VMware

Tipe: Array string

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListBackupJobs

Layanan: AWS Backup

Mengembalikan daftar pekerjaan cadangan yang ada untuk akun yang diautentikasi selama 30 hari terakhir. Untuk jangka waktu yang lebih lama, pertimbangkan untuk menggunakan alat pemantauan ini.

Minta Sintaks

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

ByAccountId

ID akun untuk daftar pekerjaan dari. Mengembalikan hanya pekerjaan cadangan yang terkait dengan ID akun tertentu.

Jika digunakan dari akun AWS Organizations manajemen, lulus * mengembalikan semua pekerjaan di seluruh organisasi.

Pola: `^[0-9]{12}$`

ByBackupVaultName

Mengembalikan hanya pekerjaan cadangan yang akan disimpan di brankas cadangan yang ditentukan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

ByCompleteAfter

Mengembalikan hanya pekerjaan cadangan yang diselesaikan setelah tanggal yang dinyatakan dalam format Unix dan Waktu Universal Terkoordinasi (UTC).

ByCompleteBefore

Mengembalikan hanya pekerjaan cadangan yang diselesaikan sebelum tanggal yang dinyatakan dalam format Unix dan Waktu Universal Terkoordinasi (UTC).

ByCreatedAfter

Mengembalikan hanya pekerjaan cadangan yang dibuat setelah tanggal yang ditentukan.

ByCreatedBefore

Mengembalikan hanya pekerjaan cadangan yang dibuat sebelum tanggal yang ditentukan.

ByMessageCategory

Ini adalah parameter opsional yang dapat digunakan untuk menyaring pekerjaan dengan MessageCategory yang cocok dengan nilai yang Anda masukkan.

Contoh string dapat mencakup`AccessDenied`,, `SUCCESSAGGREGATE_ALL`, dan`InvalidParameters`.

Lihat Monitoring

Wildcard () mengembalikan jumlah semua kategori pesan.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua kategori pesan dan mengembalikan jumlah.

ByParentJobId

Ini adalah filter untuk mencantumkan pekerjaan anak (bersarang) berdasarkan ID pekerjaan orang tua.

ByResourceArn

Mengembalikan hanya pekerjaan cadangan yang cocok dengan sumber daya yang ditentukan Amazon Resource Name (ARN).

ByResourceType

Mengembalikan hanya pekerjaan cadangan untuk sumber daya yang ditentukan:

- `Aurora`untuk Amazon Aurora
- `CloudFormation`untuk AWS CloudFormation
- `DocumentDB`untuk Amazon DocumentDB (dengan kompatibilitas MongoDB)
- `DynamoDB`untuk Amazon DynamoDB
- `EBS`untuk Amazon Elastic Block Store
- `EC2`untuk Amazon Elastic Compute Cloud
- `EFS`untuk Amazon Elastic File System

- `FSx`untuk Amazon FSx
- `Neptune`untuk Amazon Neptunus
- `Redshift`untuk Amazon Redshift
- `RDS`untuk Amazon Relational Database Service
- `SAP HANA on Amazon EC2`untuk database SAP HANA
- `Storage Gateway`untuk AWS Storage Gateway
- `S3` untuk Amazon S3
- `Timestream`untuk Amazon Timestream
- `VirtualMachine`untuk mesin virtual

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Mengembalikan hanya pekerjaan cadangan yang berada dalam keadaan tertentu.

`Completed with issues`adalah status yang hanya ditemukan di AWS Backup konsol. Untuk API, status ini mengacu pada pekerjaan dengan status `COMPLETED` dan a `MessageCategory` dengan nilai selain`SUCCESS`; yaitu, status selesai tetapi dilengkapi dengan pesan status.

Untuk mendapatkan jumlah pekerjaan`Completed with issues`, jalankan dua permintaan GET, dan kurangi nomor kedua yang lebih kecil:

DAPATKAN /backup-jobs/? State=Selesai

DAPATKAN /backup-jobs/? messageCategory=Success&state=Selesai

Nilai Valid: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupJobs

Array struktur yang berisi metadata tentang pekerjaan cadangan Anda dikembalikan dalam format JSON.

Tipe: Array objek BackupJob

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListBackupJobSummaries

Layanan: AWS Backup

Ini adalah permintaan untuk ringkasan pekerjaan cadangan yang dibuat atau berjalan dalam 30 hari terakhir. Anda dapat menyertakan parameter accountID, State,,, ResourceType, MessageCategory AggregationPeriod MaxResults, NextToken atau untuk memfilter hasil.

Permintaan ini menampilkan ringkasan yang berisi Wilayah, Akun, Negara Bagian, ResourceType, MessageCategory, StartTime,, EndTime, dan Hitungan pekerjaan yang disertakan.

Minta Sintaks

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

AccountId

Mengembalikan jumlah pekerjaan untuk akun tertentu.

Jika permintaan dikirim dari akun anggota atau akun yang bukan bagian dari AWS Organizations, pekerjaan dalam akun pemohon akan dikembalikan.

Akun root, admin, dan administrator yang didelegasikan dapat menggunakan nilai ANY untuk mengembalikan jumlah pekerjaan dari setiap akun di organisasi.

AGGREGATE_ALLagregat jumlah pekerjaan dari semua akun dalam organisasi yang diautentikasi, lalu mengembalikan jumlahnya.

Pola: `^[0-9]{12}$`

AggregationPeriod

Periode untuk hasil yang dikembalikan.

- ONE_DAY- Jumlah pekerjaan harian selama 14 hari sebelumnya.
- SEVEN_DAYS- Jumlah pekerjaan agregat untuk 7 hari sebelumnya.
- FOURTEEN_DAYS- Jumlah pekerjaan agregat selama 14 hari sebelumnya.

Nilai Valid: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Nilainya adalah bilangan bulat. Rentang nilai yang diterima adalah dari 1 hingga 500.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

MessageCategory

Parameter ini mengembalikan jumlah pekerjaan untuk kategori pesan tertentu.

Contoh string yang diterima meliputi`AccessDenied`,`Success`, dan`InvalidParameters`. Lihat Monitoring untuk daftar MessageCategory string yang diterima.

Nilai APAPUN mengembalikan jumlah semua kategori pesan.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua kategori pesan dan mengembalikan jumlah.

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

ResourceType

Mengembalikan jumlah pekerjaan untuk jenis sumber daya tertentu. Gunakan permintaan `GetSupportedResourceTypes` untuk mendapatkan string untuk jenis sumber daya yang didukung.

Nilai ANY mengembalikan jumlah semua jenis sumber daya.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua jenis sumber daya dan mengembalikan jumlah.

Jenis AWS sumber daya yang akan dicadangkan; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS).

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Parameter ini mengembalikan jumlah pekerjaan untuk pekerjaan dengan status tertentu.

Nilai ANY mengembalikan jumlah semua negara.

AGGREGATE_ALLagregat jumlah pekerjaan untuk semua negara bagian dan mengembalikan jumlah.

Completed with issuesadalah status yang hanya ditemukan di AWS Backup konsol. Untuk API, status ini mengacu pada pekerjaan dengan status COMPLETED dan a MessageCategory dengan nilai selainSUCCESS; yaitu, status selesai tetapi dilengkapi dengan pesan status. Untuk mendapatkan jumlah pekerjaanCompleted with issues, jalankan dua permintaan GET, dan kurangi nomor kedua yang lebih kecil:

DAPATKAN /audit/? backup-job-summaries AggregationPeriod=Fourteen_days&state=Selesai

DAPATKAN /audit/? backup-job-summaries AggregationPeriod=FOURTEEN_DAYS& MessageCategory =SUCCES&STATEEN=Selesai

Nilai Valid: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AggregationPeriod

Periode untuk hasil yang dikembalikan.

- `ONE_DAY`- Jumlah pekerjaan harian selama 14 hari sebelumnya.
- `SEVEN_DAYS`- Jumlah pekerjaan agregat untuk 7 hari sebelumnya.
- `FOURTEEN_DAYS`- Jumlah pekerjaan agregat selama 14 hari sebelumnya.

Jenis: String

BackupJobSummaries

Informasi ringkasan.

Tipe: Array objek BackupJobSummary

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListBackupPlans

Layanan: AWS Backup

Daftar paket cadangan aktif untuk akun.

Minta Sintaks

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

IncludeDeleted

Nilai Boolean dengan nilai default yang mengembalikan rencana cadangan `FALSE` yang dihapus saat disetel ke`TRUE`.

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlansList

Informasi tentang rencana cadangan.

Tipe: Array objek BackupPlansListMember

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python

- AWS SDK for Ruby V3

ListBackupPlanTemplates

Layanan: AWS Backup

Daftar templat rencana cadangan.

Minta Sintaks

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
```

```
   "NextToken": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlanTemplatesList

Array item daftar template yang berisi metadata tentang template yang Anda simpan.

Tipe: Array objek BackupPlanTemplatesListMember

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListBackupPlanVersions

Layanan: AWS Backup

Mengembalikan metadata versi paket cadangan Anda, termasuk Nama Sumber Daya Amazon (ARN), ID paket cadangan, tanggal pembuatan dan penghapusan, nama paket, dan ID versi.

Minta Sintaks

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

Secara unik mengidentifikasi rencana cadangan.

Wajib: Ya

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupPlanVersionsList

Array item daftar versi yang berisi metadata tentang rencana cadangan Anda.

Tipe: Array objek BackupPlansListMember

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python

- AWS SDK for Ruby V3

ListBackupSelections

Layanan: AWS Backup

Mengembalikan array yang berisi metadata dari sumber daya yang terkait dengan rencana cadangan target.

Minta Sintaks

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

Secara unik mengidentifikasi rencana cadangan.

Wajib: Ya

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupSelectionsList": [
      {
         "BackupPlanId": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "IamRoleArn": "string",
         "SelectionId": "string",
         "SelectionName": "string"
      }
   ],
   "NextToken": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupSelectionsList

Array item daftar pilihan cadangan yang berisi metadata tentang setiap sumber daya dalam daftar.

Tipe: Array objek BackupSelectionsListMember

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListBackupVaults

Layanan: AWS Backup

Mengembalikan daftar wadah penyimpanan titik pemulihan bersama dengan informasi tentang mereka.

Minta Sintaks

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

[ByShared](#)

Parameter ini akan mengurutkan daftar brankas berdasarkan brankas bersama.

[ByVaultType](#)

Parameter ini akan mengurutkan daftar vault berdasarkan jenis vault.

Nilai Valid: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

[MaxResults](#)

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

[NextToken](#)

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupVaultList

Larik anggota daftar vault cadangan yang berisi metadata vault, termasuk Nama Sumber Daya Amazon (ARN), nama tampilan, tanggal pembuatan, jumlah titik pemulihan yang disimpan, dan informasi enkripsi jika sumber daya yang disimpan di brankas cadangan dienkripsi.

Tipe: Array objek BackupVaultListMember

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript

- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListCopyJobs

Layanan: AWS Backup

Mengembalikan metadata tentang pekerjaan salinan Anda.

Minta Sintaks

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

ByAccountId

ID akun untuk daftar pekerjaan dari. Mengembalikan hanya menyalin pekerjaan yang terkait dengan ID akun tertentu.

Pola: `^[0-9]{12}$`

ByCompleteAfter

Pengembalian hanya menyalin pekerjaan yang diselesaikan setelah tanggal yang dinyatakan dalam format Unix dan Waktu Universal Terkoordinasi (UTC).

ByCompleteBefore

Pengembalian hanya menyalin pekerjaan yang diselesaikan sebelum tanggal yang dinyatakan dalam format Unix dan Waktu Universal Terkoordinasi (UTC).

ByCreatedAfter

Mengembalikan hanya menyalin pekerjaan yang dibuat setelah tanggal yang ditentukan.

ByCreatedBefore

Mengembalikan hanya menyalin pekerjaan yang dibuat sebelum tanggal yang ditentukan.

ByDestinationVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan sumber untuk disalin; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

ByMessageCategory

Ini adalah parameter opsional yang dapat digunakan untuk menyaring pekerjaan dengan MessageCategory yang cocok dengan nilai yang Anda masukkan.

Contoh string dapat mencakup`AccessDenied`,, `SUCCESSAGGREGATE_ALL`, dan`INVALIDPARAMETERS`.

Lihat Monitoring untuk daftar string yang diterima.

Nilai APAPUN mengembalikan jumlah semua kategori pesan.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua kategori pesan dan mengembalikan jumlah.

ByParentJobId

Ini adalah filter untuk mencantumkan pekerjaan anak (bersarang) berdasarkan ID pekerjaan orang tua.

ByResourceArn

Mengembalikan hanya menyalin pekerjaan yang cocok dengan sumber daya yang ditentukan Amazon Resource Name (ARN).

ByResourceType

Mengembalikan hanya pekerjaan cadangan untuk sumber daya yang ditentukan:

- `Aurora`untuk Amazon Aurora
- `CloudFormation`untuk AWS CloudFormation
- `DocumentDB`untuk Amazon DocumentDB (dengan kompatibilitas MongoDB)
- `DynamoDB`untuk Amazon DynamoDB
- `EBS`untuk Amazon Elastic Block Store
- `EC2`untuk Amazon Elastic Compute Cloud
- `EFS`untuk Amazon Elastic File System
- `FSx`untuk Amazon FSx
- `Neptune`untuk Amazon Neptunus
- `Redshift`untuk Amazon Redshift
- `RDS`untuk Amazon Relational Database Service

- `SAP HANA on Amazon EC2`untuk database SAP HANA
- `Storage Gateway`untuk AWS Storage Gateway
- `S3` untuk Amazon S3
- `Timestream`untuk Amazon Timestream
- `VirtualMachine`untuk mesin virtual

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Mengembalikan hanya menyalin pekerjaan yang berada dalam keadaan tertentu.

Nilai Valid: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan MaxResults jumlah item, NextToken memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CopyJobs

Array struktur yang berisi metadata tentang pekerjaan salinan Anda dikembalikan dalam format JSON.

Tipe: Array objek CopyJob

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan MaxResults jumlah item, NextToken memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python

- AWS SDK for Ruby V3

ListCopyJobSummaries

Layanan: AWS Backup

Permintaan ini memperoleh daftar pekerjaan salinan yang dibuat atau dijalankan dalam 30 hari terakhir. Anda dapat menyertakan parameter accountID, State,,, ResourceType, MessageCategory AggregationPeriod MaxResults, NextToken atau untuk memfilter hasil.

Permintaan ini menampilkan ringkasan yang berisi Wilayah, Akun, Negara Bagian, RestourceType, MessageCategory, StartTime,, EndTime, dan Hitungan pekerjaan yang disertakan.

Minta Sintaks

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

AccountId

Mengembalikan jumlah pekerjaan untuk akun yang ditentukan.

Jika permintaan dikirim dari akun anggota atau akun yang bukan bagian dari AWS Organizations, pekerjaan dalam akun pemohon akan dikembalikan.

Akun root, admin, dan administrator yang didelegasikan dapat menggunakan nilai ANY untuk mengembalikan jumlah pekerjaan dari setiap akun di organisasi.

AGGREGATE_ALLagregat jumlah pekerjaan dari semua akun dalam organisasi yang diautentikasi, lalu mengembalikan jumlahnya.

Pola: `^[0-9]{12}$`

AggregationPeriod

Periode untuk hasil yang dikembalikan.

- ONE_DAY- Jumlah pekerjaan harian selama 14 hari sebelumnya.
- SEVEN_DAYS- Jumlah pekerjaan agregat untuk 7 hari sebelumnya.
- FOURTEEN_DAYS- Jumlah pekerjaan agregat selama 14 hari sebelumnya.

Nilai Valid: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Parameter ini menetapkan jumlah maksimum item yang akan dikembalikan.

Nilainya adalah bilangan bulat. Rentang nilai yang diterima adalah dari 1 hingga 500.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

MessageCategory

Parameter ini mengembalikan jumlah pekerjaan untuk kategori pesan tertentu.

Contoh string yang diterima meliputi`AccessDenied`,`Success`, dan`InvalidParameters`. Lihat Monitoring untuk daftar MessageCategory string yang diterima.

Nilai APAPUN mengembalikan jumlah semua kategori pesan.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua kategori pesan dan mengembalikan jumlah.

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

ResourceType

Mengembalikan jumlah pekerjaan untuk jenis sumber daya tertentu. Gunakan permintaan `GetSupportedResourceTypes` untuk mendapatkan string untuk jenis sumber daya yang didukung.

Nilai ANY mengembalikan jumlah semua jenis sumber daya.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua jenis sumber daya dan mengembalikan jumlah.

Jenis AWS sumber daya yang akan dicadangkan; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS).

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Parameter ini mengembalikan jumlah pekerjaan untuk pekerjaan dengan status tertentu.

Nilai ANY mengembalikan jumlah semua negara.

AGGREGATE_ALLagregat jumlah pekerjaan untuk semua negara bagian dan mengembalikan jumlah.

Nilai Valid: CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AggregationPeriod

Periode untuk hasil yang dikembalikan.

- `ONE_DAY`- Jumlah pekerjaan harian selama 14 hari sebelumnya.
- `SEVEN_DAYS`- Jumlah pekerjaan agregat untuk 7 hari sebelumnya.
- `FOURTEEN_DAYS`- Jumlah pekerjaan agregat selama 14 hari sebelumnya.

Jenis: String

CopyJobSummaries

Pengembalian ini menunjukkan ringkasan yang berisi Wilayah, Akun, Negara Bagian, ResourceType,, MessageCategory, StartTime, EndTime, dan Hitungan pekerjaan yang disertakan.

Tipe: Array objek CopyJobSummary

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListFrameworks

Layanan: AWS Backup

Mengembalikan daftar semua kerangka kerja untuk Akun AWS dan Wilayah AWS.

Minta Sintaks

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

MaxResults

Jumlah hasil yang diinginkan dari 1 hingga 1000. Tidak wajib. Jika tidak ditentukan, kueri akan mengembalikan 1 MB data.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Pengidentifikasi yang dikembalikan dari panggilan sebelumnya ke operasi ini, yang dapat digunakan untuk mengembalikan set item berikutnya dalam daftar.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
```

```
            "FrameworkName": "string",
            "NumberOfControls": number
        }
    ],
    "NextToken": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Frameworks

Kerangka kerja dengan detail untuk setiap framework, termasuk nama framework, Amazon Resource Name (ARN), deskripsi, jumlah kontrol, waktu pembuatan, dan status penerapan.

Tipe: Array objek Framework

NextToken

Pengidentifikasi yang dikembalikan dari panggilan sebelumnya ke operasi ini, yang dapat digunakan untuk mengembalikan set item berikutnya dalam daftar.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListLegalHolds

Layanan: AWS Backup

Tindakan ini mengembalikan metadata tentang penahanan hukum aktif dan sebelumnya.

Minta Sintaks

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

MaxResults

Jumlah maksimum item daftar sumber daya yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

LegalHolds

Ini adalah serangkaian pegangan hukum yang dikembalikan, baik aktif maupun sebelumnya.

Tipe: Array objek LegalHold

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListProtectedResources

Layanan: AWS Backup

Mengembalikan larik sumber daya yang berhasil dicadangkan oleh AWS Backup, termasuk waktu sumber daya disimpan, Nama Sumber Daya Amazon (ARN) sumber daya, dan jenis sumber daya.

Minta Sintaks

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
```

```
            "LastRecoveryPointArn": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string"
        }
    ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Results

Larik sumber daya yang berhasil dicadangkan dengan AWS Backup menyertakan waktu sumber daya disimpan, Nama Sumber Daya Amazon (ARN) sumber daya, dan jenis sumber daya.

Tipe: Array objek ProtectedResource

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListProtectedResourcesByBackupVault

Layanan: AWS Backup

Permintaan ini mencantumkan sumber daya yang dilindungi yang sesuai dengan setiap brankas cadangan.

Minta Sintaks

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

BackupVaultAccountId

Daftar sumber daya yang dilindungi oleh brankas cadangan dalam vault yang Anda tentukan berdasarkan ID akun.

Pola: `^[0-9]{12}$`

backupVaultName

Daftar sumber daya yang dilindungi oleh brankas cadangan dalam brankas yang Anda tentukan berdasarkan nama.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Results

Ini adalah hasil yang dikembalikan untuk permintaan tersebut ListProtectedResourcesByBackupVault.

Tipe: Array objek ProtectedResource

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListRecoveryPointsByBackupVault

Layanan: AWS Backup

Mengembalikan informasi rinci tentang titik pemulihan yang disimpan dalam brankas cadangan.

Minta Sintaks

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

BackupVaultAccountId

Parameter ini akan mengurutkan daftar titik pemulihan berdasarkan ID akun.

Pola: `^[0-9]{12}$`

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

> **Note**
>
> Nama brankas cadangan mungkin tidak tersedia saat layanan yang didukung membuat cadangan.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

ByBackupPlanId

Mengembalikan hanya titik pemulihan yang cocok dengan ID rencana cadangan yang ditentukan.

ByCreatedAfter

Mengembalikan hanya titik pemulihan yang dibuat setelah stempel waktu yang ditentukan.

ByCreatedBefore

Mengembalikan hanya titik pemulihan yang dibuat sebelum stempel waktu yang ditentukan.

ByParentRecoveryPointArn

Ini hanya mengembalikan titik pemulihan yang cocok dengan titik pemulihan induk (komposit) yang ditentukan Amazon Resource Name (ARN).

ByResourceArn

Mengembalikan hanya titik pemulihan yang cocok dengan sumber daya yang ditentukan Amazon Resource Name (ARN).

ByResourceType

Mengembalikan hanya titik pemulihan yang cocok dengan jenis sumber daya tertentu:

- `Aurora`untuk Amazon Aurora
- `CloudFormation`untuk AWS CloudFormation
- `DocumentDB`untuk Amazon DocumentDB (dengan kompatibilitas MongoDB)
- `DynamoDB`untuk Amazon DynamoDB
- `EBS`untuk Amazon Elastic Block Store
- `EC2`untuk Amazon Elastic Compute Cloud
- `EFS`untuk Amazon Elastic File System
- `FSx`untuk Amazon FSx
- `Neptune`untuk Amazon Neptunus
- `Redshift`untuk Amazon Redshift
- `RDS`untuk Amazon Relational Database Service
- `SAP HANA on Amazon EC2`untuk database SAP HANA
- `Storage Gateway`untuk AWS Storage Gateway
- `S3` untuk Amazon S3
- `Timestream`untuk Amazon Timestream
- `VirtualMachine`untuk mesin virtual

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

RecoveryPoints

Array objek yang berisi informasi rinci tentang titik pemulihan yang disimpan di brankas cadangan.

Tipe: Array objek RecoveryPointByBackupVault

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListRecoveryPointsByLegalHold

Layanan: AWS Backup

Tindakan ini mengembalikan ARN titik pemulihan (Nama Sumber Daya Amazon) dari penahanan hukum yang ditentukan.

Minta Sintaks

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

legalHoldId

ID penahanan hukum.

Wajib: Ya

MaxResults

Jumlah maksimum item daftar sumber daya yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan.

Jenis: String

RecoveryPoints

Poin pemulihan.

Tipe: Array objek RecoveryPointMember

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListRecoveryPointsByResource

Layanan: AWS Backup

Informasi tentang titik pemulihan dari jenis yang ditentukan oleh sumber daya Amazon Resource Name (ARN).

> **Note**
>
> Untuk Amazon EFS dan Amazon EC2, tindakan ini hanya mencantumkan titik pemulihan yang dibuat oleh. AWS Backup

Minta Sintaks

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

ManagedByAWSBackupOnly

Atribut ini memfilter titik pemulihan berdasarkan kepemilikan.

Jika ini diatur ke`TRUE`, respons akan berisi titik pemulihan yang terkait dengan sumber daya yang dipilih yang dikelola oleh AWS Backup.

Jika ini diatur ke`FALSE`, respons akan berisi semua titik pemulihan yang terkait dengan sumber daya yang dipilih.

Jenis: Boolean

MaxResults

Jumlah maksimum item yang akan dikembalikan.

> **Note**
>
> Amazon RDS membutuhkan nilai minimal 20.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

resourceArn

ARN yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

RecoveryPoints

Array objek yang berisi informasi rinci tentang titik pemulihan dari jenis sumber daya yang ditentukan.

> **Note**
>
> Hanya poin pemulihan Amazon EFS dan Amazon EC2 yang kembali. BackupVaultName

Tipe: Array objek RecoveryPointByResource

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListReportJobs

Layanan: AWS Backup

Mengembalikan detail tentang pekerjaan laporan Anda.

Minta Sintaks

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

ByCreationAfter

Pengembalian hanya melaporkan pekerjaan yang dibuat setelah tanggal dan waktu yang ditentukan dalam format Unix dan Coordinated Universal Time (UTC). Misalnya, nilai 1516925490 mewakili Jumat, 26 Januari 2018 12:11:30.

ByCreationBefore

Pengembalian hanya melaporkan pekerjaan yang dibuat sebelum tanggal dan waktu yang ditentukan dalam format Unix dan Coordinated Universal Time (UTC). Misalnya, nilai 1516925490 mewakili Jumat, 26 Januari 2018 12:11:30.

ByReportPlanName

Mengembalikan hanya pekerjaan laporan dengan nama rencana laporan yang ditentukan.

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

Mengembalikan hanya melaporkan pekerjaan yang berada dalam status tertentu. Statusnya adalah:

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

Jumlah hasil yang diinginkan dari 1 hingga 1000. Tidak wajib. Jika tidak ditentukan, kueri akan mengembalikan 1 MB data.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Pengidentifikasi yang dikembalikan dari panggilan sebelumnya ke operasi ini, yang dapat digunakan untuk mengembalikan set item berikutnya dalam daftar.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Pengidentifikasi yang dikembalikan dari panggilan sebelumnya ke operasi ini, yang dapat digunakan untuk mengembalikan set item berikutnya dalam daftar.

Jenis: String

ReportJobs

Detail tentang pekerjaan laporan Anda dalam format JSON.

Tipe: Array objek ReportJob

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListReportPlans

Layanan: AWS Backup

Mengembalikan daftar rencana laporan Anda. Untuk informasi rinci tentang rencana laporan tunggal, gunakan`DescribeReportPlan`.

Minta Sintaks

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

MaxResults

Jumlah hasil yang diinginkan dari 1 hingga 1000. Tidak wajib. Jika tidak ditentukan, kueri akan mengembalikan 1 MB data.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Pengidentifikasi yang dikembalikan dari panggilan sebelumnya ke operasi ini, yang dapat digunakan untuk mengembalikan set item berikutnya dalam daftar.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
         }
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Pengidentifikasi yang dikembalikan dari panggilan sebelumnya ke operasi ini, yang dapat digunakan untuk mengembalikan set item berikutnya dalam daftar.

Jenis: String

ReportPlans

Laporan tersebut merencanakan dengan informasi terperinci untuk setiap rencana. Informasi ini mencakup Nama Sumber Daya Amazon (ARN), nama rencana laporan, deskripsi, pengaturan, saluran pengiriman, status penerapan, waktu pembuatan, dan terakhir kali rencana laporan dicoba dan berhasil dijalankan.

Tipe: Array objek ReportPlan

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListRestoreJobs

Layanan: AWS Backup

Mengembalikan daftar pekerjaan yang AWS Backup dimulai untuk memulihkan sumber daya yang disimpan, termasuk rincian tentang proses pemulihan.

Minta Sintaks

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

ByAccountId

ID akun untuk daftar pekerjaan dari. Pengembalian hanya mengembalikan pekerjaan yang terkait dengan ID akun yang ditentukan.

Pola: `^[0-9]{12}$`

ByCompleteAfter

Pengembalian hanya menyalin pekerjaan yang diselesaikan setelah tanggal yang dinyatakan dalam format Unix dan Waktu Universal Terkoordinasi (UTC).

ByCompleteBefore

Pengembalian hanya menyalin pekerjaan yang diselesaikan sebelum tanggal yang dinyatakan dalam format Unix dan Waktu Universal Terkoordinasi (UTC).

ByCreatedAfter

Pengembalian hanya mengembalikan pekerjaan yang dibuat setelah tanggal yang ditentukan.

ByCreatedBefore

Pengembalian hanya mengembalikan pekerjaan yang dibuat sebelum tanggal yang ditentukan.

ByResourceType

Sertakan parameter ini untuk mengembalikan hanya memulihkan pekerjaan untuk sumber daya yang ditentukan:

- `Aurora`untuk Amazon Aurora
- `CloudFormation`untuk AWS CloudFormation
- `DocumentDB`untuk Amazon DocumentDB (dengan kompatibilitas MongoDB)
- `DynamoDB`untuk Amazon DynamoDB
- `EBS`untuk Amazon Elastic Block Store
- `EC2`untuk Amazon Elastic Compute Cloud
- `EFS`untuk Amazon Elastic File System
- `FSx`untuk Amazon FSx
- `Neptune`untuk Amazon Neptunus
- `Redshift`untuk Amazon Redshift
- `RDS`untuk Amazon Relational Database Service
- `SAP HANA on Amazon EC2`untuk database SAP HANA
- `Storage Gateway`untuk AWS Storage Gateway
- `S3` untuk Amazon S3
- `Timestream`untuk Amazon Timestream
- `VirtualMachine`untuk mesin virtual

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByRestoreTestingPlanArn

Ini hanya mengembalikan tugas pengujian yang cocok dengan sumber daya yang ditentukan Amazon Resource Name (ARN).

ByStatus

Pengembalian hanya mengembalikan pekerjaan yang terkait dengan status pekerjaan yang ditentukan.

Nilai Valid: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
      }
   ]
```

```
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

RestoreJobs

Array objek yang berisi informasi rinci tentang pekerjaan untuk memulihkan sumber daya yang disimpan.

Tipe: Array objek RestoreJobsListMember

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListRestoreJobsByProtectedResource

Layanan: AWS Backup

Ini mengembalikan pekerjaan pemulihan yang berisi sumber daya terlindungi yang ditentukan.

Anda harus memasukkan`ResourceArn`. Anda dapat secara opsional memasukkan`NextToken`,`ByStatus`,, `MaxResults`,`ByRecoveryPointCreationDateAfter`, dan`ByRecoveryPointCreationDateBefore`.

Minta Sintaks

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

ByRecoveryPointCreationDateAfter

Pengembalian hanya mengembalikan pekerjaan titik pemulihan yang dibuat setelah tanggal yang ditentukan.

ByRecoveryPointCreationDateBefore

Pengembalian hanya mengembalikan pekerjaan titik pemulihan yang dibuat sebelum tanggal yang ditentukan.

ByStatus

Pengembalian hanya mengembalikan pekerjaan yang terkait dengan status pekerjaan yang ditentukan.

Nilai Valid: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda

mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

resourceArn

Pengembalian hanya memulihkan pekerjaan yang cocok dengan sumber daya yang ditentukan Amazon Resource Name (ARN).

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
        }
    ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Andauntuk mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya

Jenis: String

RestoreJobs

Array objek yang berisi informasi rinci tentang pekerjaan untuk memulihkan sumber daya yang disimpan. >

Tipe: Array objek RestoreJobsListMember

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListRestoreJobSummaries

Layanan: AWS Backup

Permintaan ini memperoleh ringkasan pekerjaan pemulihan yang dibuat atau berjalan dalam 30 hari terakhir. Anda dapat menyertakan parameter accountID, State,,,, ResourceType AggregationPeriod MaxResults, NextToken atau untuk memfilter hasil.

Permintaan ini menampilkan ringkasan yang berisi Wilayah, Akun, Negara Bagian, RestourceType, MessageCategory, StartTime,, EndTime, dan Hitungan pekerjaan yang disertakan.

Minta Sintaks

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

AccountId

Mengembalikan jumlah pekerjaan untuk akun yang ditentukan.

Jika permintaan dikirim dari akun anggota atau akun yang bukan bagian dari AWS Organizations, pekerjaan dalam akun pemohon akan dikembalikan.

Akun root, admin, dan administrator yang didelegasikan dapat menggunakan nilai ANY untuk mengembalikan jumlah pekerjaan dari setiap akun di organisasi.

AGGREGATE_ALLagregat jumlah pekerjaan dari semua akun dalam organisasi yang diautentikasi, lalu mengembalikan jumlahnya.

Pola: `^[0-9]{12}$`

AggregationPeriod

Periode untuk hasil yang dikembalikan.

- ONE_DAY- Jumlah pekerjaan harian selama 14 hari sebelumnya.
- SEVEN_DAYS- Jumlah pekerjaan agregat untuk 7 hari sebelumnya.

- `FOURTEEN_DAYS`- Jumlah pekerjaan agregat selama 14 hari sebelumnya.

Nilai Valid: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Parameter ini menetapkan jumlah maksimum item yang akan dikembalikan.

Nilainya adalah bilangan bulat. Rentang nilai yang diterima adalah dari 1 hingga 500.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

ResourceType

Mengembalikan jumlah pekerjaan untuk jenis sumber daya tertentu. Gunakan permintaan `GetSupportedResourceTypes` untuk mendapatkan string untuk jenis sumber daya yang didukung.

Nilai ANY mengembalikan jumlah semua jenis sumber daya.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua jenis sumber daya dan mengembalikan jumlah.

Jenis AWS sumber daya yang akan dicadangkan; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS).

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Parameter ini mengembalikan jumlah pekerjaan untuk pekerjaan dengan status tertentu.

Nilai ANY mengembalikan jumlah semua negara.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua negara bagian dan mengembalikan jumlah.

Nilai Valid: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AggregationPeriod

Periode untuk hasil yang dikembalikan.

- `ONE_DAY`- Jumlah pekerjaan harian selama 14 hari sebelumnya.
- `SEVEN_DAYS`- Jumlah pekerjaan agregat untuk 7 hari sebelumnya.
- `FOURTEEN_DAYS`- Jumlah pekerjaan agregat selama 14 hari sebelumnya.

Jenis: String

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Jenis: String

RestoreJobSummaries

Pengembalian ini berisi ringkasan yang berisi Wilayah, Akun, Negara Bagian, ResourceType,, MessageCategory, StartTime, EndTime, dan Hitungan pekerjaan yang disertakan.

Tipe: Array objek RestoreJobSummary

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListRestoreTestingPlans

Layanan: AWS Backup

Mengembalikan daftar rencana pengujian pemulihan.

Minta Sintaks

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh nexttoken.

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
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
        }
    ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh nexttoken.

Jenis: String

RestoreTestingPlans

Ini adalah daftar rencana pengujian pemulihan yang dikembalikan.

Tipe: Array objek RestoreTestingPlanForList

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListRestoreTestingSelections

Layanan: AWS Backup

Mengembalikan daftar pilihan pengujian pemulihan. Dapat disaring oleh `MaxResults` dan`RestoreTestingPlanName`.

Minta Sintaks

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh nexttoken.

RestoreTestingPlanName

Mengembalikan pilihan pengujian pemulihan dengan nama rencana pengujian pemulihan yang ditentukan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh nexttoken.

Jenis: String

RestoreTestingSelections

Pilihan pengujian pemulihan yang dikembalikan terkait dengan rencana pengujian pemulihan.

Tipe: Array objek RestoreTestingSelectionForList

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListTags

Layanan: AWS Backup

Mengembalikan tag yang ditetapkan ke sumber daya, seperti titik pemulihan target, rencana cadangan, atau brankas cadangan.

`ListTags`hanya berfungsi untuk jenis sumber daya yang mendukung AWS Backup manajemen penuh cadangan mereka. Jenis sumber daya tersebut tercantum dalam tabel Ketersediaan fitur menurut sumber daya.

Minta Sintaks

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

MaxResults

Jumlah maksimum item yang akan dikembalikan.

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 1000.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

resourceArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya. Target yang valid untuk `ListTags` adalah titik pemulihan, rencana cadangan, dan brankas cadangan.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar item yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah item, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Tags

Informasi tentang tag.

Tipe: Peta string ke string

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

PutBackupVaultAccessPolicy

Layanan: AWS Backup

Menetapkan kebijakan berbasis sumber daya yang digunakan untuk mengelola izin akses pada vault cadangan target. Memerlukan nama vault cadangan dan dokumen kebijakan akses dalam format JSON.

Minta Sintaks

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

Policy

Dokumen kebijakan akses vault cadangan dalam format JSON.

Tipe: String

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

PutBackupVaultLockConfiguration

Layanan: AWS Backup

Menerapkan AWS Backup Vault Lock ke brankas cadangan, mencegah upaya untuk menghapus titik pemulihan apa pun yang disimpan atau dibuat di brankas cadangan. Vault Lock juga mencegah upaya untuk memperbarui kebijakan siklus hidup yang mengontrol periode penyimpanan titik pemulihan apa pun yang saat ini disimpan di brankas cadangan. Jika ditentukan, Vault Lock memberlakukan periode retensi minimum dan maksimum untuk pekerjaan pencadangan dan penyalinan di masa mendatang yang menargetkan brankas cadangan.

> **Note**
>
> AWS Backup Vault Lock telah dinilai oleh Cohasset Associates untuk digunakan di lingkungan yang tunduk pada peraturan SEC 17a-4, CFTC, dan FINRA. Untuk informasi selengkapnya tentang bagaimana AWS Backup Vault Lock berhubungan dengan peraturan ini, lihat Penilaian Kepatuhan Cohasset Associates.

Untuk informasi selengkapnya, lihat Kunci Penyimpanan AWS Backup.

Minta Sintaks

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Konfigurasi AWS Backup Vault Lock yang menentukan nama brankas cadangan yang dilindunginya.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

ChangeableForDays

Konfigurasi AWS Backup Vault Lock yang menentukan jumlah hari sebelum tanggal penguncian. Misalnya, pengaturan `ChangeableForDays` ke 30 pada 1 Januari 2022 pukul 8 malam UTC akan menetapkan tanggal kunci menjadi 31 Januari 2022 pukul 8 malam UTC.

AWS Backup memberlakukan periode pendinginan 72 jam sebelum Vault Lock berlaku dan menjadi tidak dapat diubah. Oleh karena itu, Anda harus mengatur `ChangeableForDays` ke 3 atau lebih besar.

Sebelum tanggal penguncian, Anda dapat menghapus Vault Lock dari vault menggunakan `DeleteBackupVaultLockConfiguration` atau mengubah konfigurasi Vault Lock menggunakan. `PutBackupVaultLockConfiguration` Pada dan setelah tanggal penguncian, Kunci Vault menjadi tidak dapat diubah dan tidak dapat diubah atau dihapus.

Jika parameter ini tidak ditentukan, Anda dapat menghapus Vault Lock dari vault menggunakan `DeleteBackupVaultLockConfiguration` atau mengubah konfigurasi Vault Lock menggunakan `PutBackupVaultLockConfiguration` kapan saja.

Tipe: Panjang

Wajib: Tidak

MaxRetentionDays

Konfigurasi AWS Backup Vault Lock yang menentukan periode retensi maksimum dimana vault mempertahankan titik pemulihannya. Pengaturan ini dapat berguna jika, misalnya, kebijakan organisasi Anda mengharuskan Anda untuk menghancurkan data tertentu setelah menyimpannya selama empat tahun (1460 hari).

Jika parameter ini tidak disertakan, Vault Lock tidak menerapkan periode retensi maksimum pada titik pemulihan di vault. Jika parameter ini disertakan tanpa nilai, Vault Lock tidak akan menerapkan periode retensi maksimum.

Jika parameter ini ditentukan, pekerjaan pencadangan atau penyalinan apa pun ke vault harus memiliki kebijakan siklus hidup dengan periode retensi sama dengan atau lebih pendek dari

periode retensi maksimum. Jika periode retensi pekerjaan lebih lama dari periode retensi maksimum tersebut, vault akan gagal melakukan pekerjaan pencadangan atau penyalinan, dan Anda harus mengubah setelan siklus hidup atau menggunakan brankas yang berbeda. Periode retensi maksimum terpanjang yang dapat Anda tentukan adalah 36500 hari (sekitar 100 tahun). Titik pemulihan yang sudah disimpan di brankas sebelum Vault Lock tidak terpengaruh.

Tipe: Panjang

Wajib: Tidak

MinRetentionDays

Konfigurasi AWS Backup Vault Lock yang menentukan periode retensi minimum tempat vault mempertahankan titik pemulihannya. Pengaturan ini dapat berguna jika, misalnya, kebijakan organisasi Anda mengharuskan Anda menyimpan data tertentu setidaknya selama tujuh tahun (2555 hari).

Parameter ini diperlukan saat kunci vault dibuat AWS CloudFormation; jika tidak, parameter ini opsional. Jika parameter ini tidak ditentukan, Vault Lock tidak akan menerapkan periode retensi minimum.

Jika parameter ini ditentukan, pekerjaan pencadangan atau penyalinan apa pun ke vault harus memiliki kebijakan siklus hidup dengan periode retensi sama dengan atau lebih lama dari periode penyimpanan minimum. Jika periode retensi pekerjaan lebih pendek dari periode retensi minimum tersebut, vault akan gagal melakukan pencadangan atau penyalinan pekerjaan tersebut, dan Anda harus mengubah setelan siklus hidup atau menggunakan vault yang berbeda. Periode retensi minimum terpendek yang dapat Anda tentukan adalah 1 hari. Titik pemulihan yang sudah disimpan di brankas sebelum Vault Lock tidak terpengaruh.

Tipe: Panjang

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

PutBackupVaultNotifications

Layanan: AWS Backup

Mengaktifkan notifikasi pada brankas cadangan untuk topik dan acara yang ditentukan.

Minta Sintaks

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

BackupVaultEvents

Array peristiwa yang menunjukkan status pekerjaan untuk mencadangkan sumber daya ke vault cadangan.

Untuk kasus penggunaan umum dan contoh kode, lihat Menggunakan Amazon SNS untuk melacak AWS Backup peristiwa.

Peristiwa berikut didukung:

- 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**
>
> Daftar di bawah ini mencakup peristiwa yang didukung dan peristiwa usang yang tidak lagi digunakan (untuk referensi). Peristiwa yang tidak digunakan lagi tidak menampilkan status atau pemberitahuan. Lihat daftar di atas untuk acara yang didukung.

Tipe: Array string

Nilai yang Valid: `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`

Wajib: Ya

SNSTopicArn

Nama Sumber Daya Amazon (ARN) yang menentukan topik untuk peristiwa vault cadangan; misalnya,. `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`

Tipe: String

Diperlukan: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python

- AWS SDK for Ruby V3

PutRestoreValidationResult

Layanan: AWS Backup

Permintaan ini memungkinkan Anda mengirim hasil validasi pengujian pemulihan mandiri mandiri Anda. `RestoreJobId`dan `ValidationStatus` diperlukan. Secara opsional, Anda dapat memasukkan file. `ValidationStatusMessage`

Minta Sintaks

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

restoreJobId

Ini adalah pengidentifikasi unik dari pekerjaan pemulihan di dalamnya AWS Backup.

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

ValidationStatus

Status validasi pemulihan Anda.

Jenis: String

Nilai yang Valid: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Wajib: Ya

ValidationStatusMessage

Ini adalah string pesan opsional yang dapat Anda masukan untuk menggambarkan status validasi untuk validasi pengujian pemulihan.

Tipe: String

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 204
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 204 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

StartBackupJob

Layanan: AWS Backup

Memulai pekerjaan pencadangan sesuai permintaan untuk sumber daya yang ditentukan.

Minta Sintaks

```
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
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

BackupOptions

Opsi cadangan untuk sumber daya yang dipilih. Opsi ini hanya tersedia untuk pekerjaan cadangan Windows Volume Shadow Copy Service (VSS).

Nilai yang valid: Setel `"WindowsVSS":"enabled"` untuk mengaktifkan opsi `WindowsVSS` cadangan dan membuat cadangan Windows VSS. Setel `"WindowsVSS""disabled"` untuk membuat cadangan reguler. `WindowsVSS`Opsi ini tidak diaktifkan secara default.

Tipe: Peta string ke string

Pola Kunci: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Pola nilai: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

CompleteWindowMinutes

Nilai dalam hitungan menit di mana pencadangan yang berhasil dimulai harus diselesaikan, atau AWS Backup akan membatalkan pekerjaan. Nilai ini bersifat opsional. Nilai ini mulai menghitung mundur dari saat cadangan dijadwalkan. Itu tidak menambah waktu tambahan untuk`StartWindowMinutes`, atau jika cadangan dimulai lebih lambat dari yang dijadwalkan.

Seperti`StartWindowMinutes`, parameter ini memiliki nilai maksimum 100 tahun (52.560.000 menit).

Tipe: Panjang

Wajib: Tidak

IamRoleArn

Menentukan peran IAM ARN digunakan untuk membuat titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Diperlukan: Ya

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `StartBackupJob` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

Lifecycle

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup akan transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Parameter ini memiliki nilai maksimum 100 tahun (36.500 hari).

Tipe: Objek Lifecycle

Wajib: Tidak

RecoveryPointTags

Tag untuk menetapkan sumber daya.

Tipe: Peta antar string

Wajib: Tidak

ResourceArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Tipe: String

Diperlukan: Ya

StartWindowMinutes

Nilai dalam hitungan menit setelah pencadangan dijadwalkan sebelum pekerjaan akan dibatalkan jika tidak berhasil dimulai. Nilai ini opsional, dan defaultnya adalah 8 jam. Jika nilai ini disertakan, setidaknya harus 60 menit untuk menghindari kesalahan.

Parameter ini memiliki nilai maksimum 100 tahun (52.560.000 menit).

Selama jendela mulai, status pekerjaan cadangan tetap dalam `CREATED` status sampai berhasil dimulai atau sampai waktu jendela mulai habis. Jika dalam waktu jendela mulai AWS Backup menerima kesalahan yang memungkinkan pekerjaan untuk dicoba lagi, secara otomatis AWS Backup akan mencoba lagi untuk memulai pekerjaan setidaknya setiap 10 menit sampai pencadangan berhasil dimulai (status pekerjaan berubah menjadi`RUNNING`) atau sampai status pekerjaan berubah menjadi `EXPIRED` (yang diharapkan terjadi ketika waktu jendela mulai selesai).

Tipe: Panjang

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupJobId

Secara unik mengidentifikasi permintaan AWS Backup untuk membuat cadangan sumber daya.

Jenis: String

CreationDate

Tanggal dan waktu pekerjaan cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

IsParent

Ini adalah nilai boolean yang dikembalikan yang menunjukkan ini adalah pekerjaan cadangan induk (komposit).

Jenis: Boolean

RecoveryPointArn

Catatan: Bidang ini hanya dikembalikan untuk sumber daya Amazon EFS dan Advanced DynamoDB.

ARN yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

StartCopyJob

Layanan: AWS Backup

Memulai pekerjaan untuk membuat salinan satu kali dari sumber daya yang ditentukan.

Tidak mendukung pencadangan berkelanjutan.

Minta Sintaks

```
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"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

DestinationBackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan tujuan untuk disalin; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Tipe: String

Diperlukan: Ya

IamRoleArn

Menentukan peran IAM ARN digunakan untuk menyalin titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Diperlukan: Ya

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `StartCopyJob` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

Lifecycle

Menentukan periode waktu, dalam beberapa hari, sebelum transisi titik pemulihan ke cold storage atau dihapus.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pada konsol, pengaturan retensi harus 90 hari lebih besar dari transisi ke pengaturan dingin setelah hari. Transisi ke pengaturan dingin setelah hari tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Untuk menghapus siklus hidup dan periode retensi yang ada dan menjaga titik pemulihan Anda tanpa batas waktu, tentukan -1 untuk dan. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Tipe: Objek Lifecycle

Wajib: Tidak

RecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan yang akan digunakan untuk pekerjaan penyalinan; misalnya, arn:aws:backup:us-east- 1:123456789012: titik pemulihan: 1eb3b5e7-9eb0-435a-a80b-108b488b0d45.

Tipe: String

Diperlukan: Ya

SourceBackupVaultName

Nama wadah sumber logis tempat cadangan disimpan. Brankas cadangan diidentifikasi dengan nama yang unik untuk akun yang digunakan untuk membuatnya dan AWS Wilayah tempat pembuatannya.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Diperlukan: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CopyJobId

Mengidentifikasi pekerjaan fotokopi secara unik.

Jenis: String

CreationDate

Tanggal dan waktu pekerjaan salinan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

IsParent

Ini adalah nilai boolean yang dikembalikan yang menunjukkan ini adalah pekerjaan salinan induk (komposit).

Jenis: Boolean

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

StartReportJob

Layanan: AWS Backup

Memulai pekerjaan laporan sesuai permintaan untuk rencana laporan yang ditentukan.

Minta Sintaks

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

reportPlanName

Nama unik dari rencana laporan.

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `StartReportJobInput` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ReportJobId

Pengidentifikasi pekerjaan laporan. String unik yang dihasilkan secara acak, Unicode, UTF-8 yang dikodekan dengan panjang paling banyak 1.024 byte. ID pekerjaan laporan tidak dapat diedit.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

StartRestoreJob

Layanan: AWS Backup

Memulihkan sumber daya tersimpan yang diidentifikasi oleh Amazon Resource Name (ARN).

Minta Sintaks

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

CopySourceTagsToRestoredResource

Ini adalah parameter opsional. Jika ini sama`True`, tag yang disertakan dalam cadangan akan disalin ke sumber daya yang dipulihkan.

Ini hanya dapat diterapkan pada cadangan yang dibuat melalui. AWS Backup

Tipe: Boolean

Wajib: Tidak

IamRoleArn

Nama Sumber Daya Amazon (ARN) dari peran IAM yang AWS Backup digunakan untuk membuat sumber daya target; misalnya:. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Wajib: Tidak

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `StartRestoreJob` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

Metadata

Satu set pasangan nilai kunci metadata.

Anda bisa mendapatkan metadata konfigurasi tentang sumber daya pada saat itu dicadangkan dengan menelepon. `GetRecoveryPointRestoreMetadata` Namun, nilai selain yang disediakan oleh `GetRecoveryPointRestoreMetadata` mungkin diperlukan untuk memulihkan sumber daya. Misalnya, Anda mungkin perlu memberikan nama sumber daya baru jika yang asli sudah ada.

Untuk informasi selengkapnya tentang metadata untuk setiap sumber daya, lihat berikut ini:

- Metadata untuk Amazon Aurora
- Metadata untuk Amazon DocumentDB
- Metadata untuk AWS CloudFormation
- Metadata untuk Amazon DynamoDB
- Metadata untuk Amazon EBS
- Metadata untuk Amazon EC2
- Metadata untuk Amazon EFS
- Metadata untuk Amazon FSx
- Metadata untuk Amazon Neptunus
- Metadata untuk Amazon RDS
- Metadata untuk Amazon Redshift
- Metadata untuk AWS Storage Gateway
- Metadata untuk Amazon S3

- Metadata untuk Amazon Timestream
- Metadata untuk mesin virtual

Tipe: Peta string ke string

Wajib: Ya

RecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipe: String

Diperlukan: Ya

ResourceType

Memulai pekerjaan untuk memulihkan titik pemulihan untuk salah satu sumber daya berikut:

- `Aurora`- Amazon Aurora
- `DocumentDB`- Amazon DocumentDB
- `CloudFormation` - AWS CloudFormation
- `DynamoDB`- Amazon DynamoDB
- `EBS`- Toko Blok Elastis Amazon
- `EC2`- Awan Komputasi Elastis Amazon
- `EFS`- Amazon Elastic File System
- `FSx`- Amazon FSx
- `Neptune`- Amazon Neptunus
- `RDS`- Amazon Relational Database Service
- `Redshift`- Pergeseran Merah Amazon
- `Storage Gateway` - AWS Storage Gateway
- `S3`- Layanan Penyimpanan Sederhana Amazon
- `Timestream`- Amazon Timestream
- `VirtualMachine`- Mesin virtual

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Diperlukan: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

RestoreJobId

Secara unik mengidentifikasi pekerjaan yang mengembalikan titik pemulihan.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

StopBackupJob

Layanan: AWS Backup

Mencoba membatalkan pekerjaan untuk membuat cadangan sumber daya satu kali.

Tindakan ini tidak didukung untuk layanan berikut: Amazon FSx untuk Windows File Server, Amazon FSx for Lustre, Amazon FSx untuk ONTAP, Amazon NetApp FSx untuk OpenZFS, Amazon DocumentDB (dengan kompatibilitas MongoDB), Amazon RDS, Amazon Aurora, dan Amazon Amazon Neptunus.

Minta Sintaks

```
POST /backup-jobs/backupJobId HTTP/1.1
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupJobId

Secara unik mengidentifikasi permintaan AWS Backup untuk membuat cadangan sumber daya.

Wajib: Ya

Isi Permintaan

Permintaan tidak memiliki isi permintaan.

Sintaks Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript

- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

TagResource

Layanan: AWS Backup

Menetapkan satu set pasangan nilai kunci ke titik pemulihan, paket cadangan, atau brankas cadangan yang diidentifikasi oleh Amazon Resource Name (ARN).

API ini didukung untuk titik pemulihan untuk jenis sumber daya termasuk Aurora, Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptunus, dan Amazon RDS.

Minta Sintaks

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

resourceArn

ARN yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya yang ditandai.

ARN yang tidak termasuk tidak `backup` kompatibel dengan penandaan. `TagResource`dan `UntagResource` dengan ARN yang tidak valid akan menghasilkan kesalahan. Konten ARN yang dapat diterima dapat mencakup. `arn:aws:backup:us-east` Konten ARN yang tidak valid mungkin terlihat seperti. `arn:aws:ec2:us-east`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

Tags

Pasangan nilai kunci yang digunakan untuk membantu mengatur sumber daya Anda. Anda dapat menetapkan metadata Anda sendiri ke sumber daya yang Anda buat. Untuk kejelasan, ini adalah struktur untuk menetapkan tag:`[{"Key":"string","Value":"string"}]`.

Tipe: Peta string ke string

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UntagResource

Layanan: AWS Backup

Menghapus satu set pasangan nilai kunci dari titik pemulihan, paket cadangan, atau brankas cadangan yang diidentifikasi oleh Amazon Resource Name (ARN)

API ini tidak didukung untuk titik pemulihan untuk jenis sumber daya termasuk Aurora, Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptunus, dan Amazon RDS.

Minta Sintaks

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

resourceArn

ARN yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya yang ditandai.

ARN yang tidak termasuk tidak `backup` kompatibel dengan penandaan. `TagResource`dan `UntagResource` dengan ARN yang tidak valid akan menghasilkan kesalahan. Konten ARN yang dapat diterima dapat mencakup. `arn:aws:backup:us-east` Konten ARN yang tidak valid mungkin terlihat seperti. `arn:aws:ec2:us-east`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

TagKeyList

Kunci untuk mengidentifikasi tag nilai kunci mana yang akan dihapus dari sumber daya.

Tipe: Array string

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateBackupPlan

Layanan: AWS Backup

Memperbarui rencana cadangan yang ditentukan. Versi baru diidentifikasi secara unik oleh ID-nya.

Minta Sintaks

```
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"
         }
      ]
   }
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupPlanId

ID dari rencana cadangan.

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

BackupPlan

Tubuh rencana cadangan. Termasuk satu `BackupPlanName` dan satu atau lebih set`Rules`.

Tipe: Objek BackupPlanInput

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
```

```
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AdvancedBackupSettings

Berisi daftar `BackupOptions` untuk setiap jenis sumber daya.

Tipe: Array objek AdvancedBackupSetting

BackupPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`

Jenis: String

BackupPlanId

Secara unik mengidentifikasi rencana cadangan.

Jenis: String

CreationDate

Tanggal dan waktu rencana cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

VersionId

String berkode UTF-8, Unicode, yang dihasilkan secara acak dan unik, dengan panjang maksimal 1.024 byte. Id versi tidak dapat diedit.

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateFramework

Layanan: AWS Backup

Memperbarui kerangka kerja yang ditentukan.

Minta Sintaks

```
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"
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

frameworkName

Nama unik dari sebuah kerangka kerja. Nama ini antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

FrameworkControls

Kontrol yang membentuk kerangka kerja. Setiap kontrol dalam daftar memiliki nama, parameter input, dan ruang lingkup.

Tipe: Array objek FrameworkControl

Wajib: Tidak

FrameworkDescription

Deskripsi opsional kerangka kerja dengan maksimum 1.024 karakter.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 1024.

Pola: `.*\S.*`

Wajib: Tidak

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `UpdateFrameworkInput` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "CreationTime": number,
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CreationTime

Tanggal dan waktu kerangka kerja dibuat, dalam representasi ISO 8601. Nilai akurat `CreationTime` untuk milidetik. Misalnya, 2020-07-10T 15:00:00.000-08:00 mewakili tanggal 10 Juli 2020 pukul 15:00 8 jam di belakang UTC.

Tipe: Timestamp

FrameworkArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Jenis: String

FrameworkName

Nama unik dari sebuah kerangka kerja. Nama ini antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AlreadyExistsException

Sumber daya yang dibutuhkan sudah ada.

Kode Status HTTP: 400

ConflictException

AWS Backup tidak dapat melakukan tindakan yang Anda minta sampai selesai melakukan tindakan sebelumnya. Coba lagi nanti.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

LimitExceededException

Batas permintaan telah terlampaui; misalnya, jumlah maksimum item yang diizinkan dalam permintaan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateGlobalSettings

Layanan: AWS Backup

Memperbarui apakah AWS akun tersebut dipilih untuk pencadangan lintas akun. Mengembalikan kesalahan jika akun bukan akun manajemen Organizations. Gunakan `DescribeGlobalSettings` API untuk menentukan pengaturan saat ini.

Minta Sintaks

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

GlobalSettings

Nilai untuk `isCrossAccountBackupEnabled` dan Wilayah. Contoh:`update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Tipe: Peta antar string

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateRecoveryPointLifecycle

Layanan: AWS Backup

Menetapkan siklus hidup transisi dari titik pemulihan.

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Operasi ini tidak mendukung pencadangan berkelanjutan.

Minta Sintaks

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

backupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

recoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

Lifecycle

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Tipe: Objek Lifecycle

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
```

```
    },
    "Lifecycle": {
       "DeleteAfterDays": number,
       "MoveToColdStorageAfterDays": number,
       "OptInToArchiveForSupportedResources": boolean
    },
    "RecoveryPointArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BackupVaultArn

ARN yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Jenis: String

CalculatedLifecycle

Sebuah `CalculatedLifecycle` benda yang berisi `DeleteAt` dan `MoveToColdStorageAt` stempel waktu.

Tipe: Objek CalculatedLifecycle

Lifecycle

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Tipe: Objek Lifecycle

RecoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Jenis: String

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

InvalidRequestException

Menunjukkan bahwa ada sesuatu yang salah dengan input ke permintaan. Misalnya, parameter adalah tipe yang salah.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateRegionSettings

Layanan: AWS Backup

Memperbarui pengaturan keikutsertaan layanan saat ini untuk Wilayah.

Gunakan `DescribeRegionSettings` API untuk menentukan jenis sumber daya yang didukung.

Minta Sintaks

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

ResourceTypeManagementPreference

Mengaktifkan atau menonaktifkan AWS Backup manajemen penuh cadangan untuk jenis sumber daya. Untuk mengaktifkan AWS Backup manajemen penuh untuk DynamoDB bersama dengan fitur cadangan AWS Backup DynamoDB lanjutan, ikuti prosedur untuk mengaktifkan cadangan DynamoDB lanjutan secara terprogram.

Jenis: String ke peta boolean

Pola Kunci: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

ResourceTypeOptInPreference

Memperbarui daftar layanan bersama dengan preferensi keikutsertaan untuk Wilayah.

Jika penetapan sumber daya hanya didasarkan pada tag, maka pengaturan keikutsertaan layanan diterapkan. Jika jenis sumber daya ditetapkan secara eksplisit ke paket cadangan, seperti Amazon S3, Amazon EC2, atau Amazon RDS, itu akan disertakan dalam cadangan meskipun keikutsertaan tidak diaktifkan untuk layanan tertentu. Jika kedua jenis sumber daya dan tag ditentukan dalam penetapan sumber daya, jenis sumber daya yang ditentukan dalam rencana cadangan akan diprioritaskan di atas kondisi tag. Pengaturan keikutsertaan layanan diabaikan dalam situasi ini.

Jenis: String ke peta boolean

Pola Kunci: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateReportPlan

Layanan: AWS Backup

Memperbarui rencana laporan yang ditentukan.

Minta Sintaks

```
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"
   }
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

reportPlanName

Nama unik dari rencana laporan. Nama ini antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

IdempotencyToken

String yang dipilih pelanggan yang dapat Anda gunakan untuk membedakan antara panggilan yang identik. `UpdateReportPlanInput` Mencoba kembali permintaan yang berhasil dengan token idempotensi yang sama menghasilkan pesan sukses tanpa tindakan yang diambil.

Tipe: String

Wajib: Tidak

ReportDeliveryChannel

Informasi tentang tempat mengirimkan laporan, khususnya nama bucket Amazon S3, key prefix S3, dan format laporan Anda.

Tipe: Objek ReportDeliveryChannel

Wajib: Tidak

ReportPlanDescription

Deskripsi opsional dari rencana laporan dengan maksimum 1.024 karakter.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 1024.

Pola: `.*\S.*`

Wajib: Tidak

ReportSetting

Template laporan untuk laporan. Laporan dibuat menggunakan template laporan. Template laporan adalah:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Jika template laporan adalah `RESOURCE_COMPLIANCE_REPORT` atau`CONTROL_COMPLIANCE_REPORT`, sumber daya API ini juga menjelaskan cakupan laporan oleh Wilayah AWS dan kerangka kerja.

Tipe: Objek ReportSetting

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CreationTime

Tanggal dan waktu rencana laporan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

ReportPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Jenis: String

ReportPlanName

Nama unik dari rencana laporan.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

AWS Backup tidak dapat melakukan tindakan yang Anda minta sampai selesai melakukan tindakan sebelumnya. Coba lagi nanti.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateRestoreTestingPlan

Layanan: AWS Backup

Permintaan ini akan mengirimkan perubahan pada rencana pengujian pemulihan yang Anda tentukan. `RestoreTestingPlanName`tidak dapat diperbarui setelah dibuat.

`RecoveryPointSelection`dapat berisi:

- `Algorithm`
- `ExcludeVaults`
- `IncludeVaults`
- `RecoveryPointTypes`
- `SelectionWindowDays`

Minta Sintaks

```
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
   }
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

RestoreTestingPlanName

Nama nama rencana pengujian pemulihan.

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

RestoreTestingPlan

Menentukan badan rencana pengujian pemulihan.

Tipe: Objek RestoreTestingPlanForUpdate

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CreationTime

Waktu rencana pengujian sumber daya dibuat.

Tipe: Timestamp

RestoreTestingPlanArn

ARN unik (Nama Sumber Daya Amazon) dari rencana pengujian pemulihan.

Jenis: String

RestoreTestingPlanName

Nama tidak dapat diubah setelah penciptaan. Nama ini hanya terdiri dari karakter alfanumerik dan garis bawah. Panjang maksimum adalah 50.

Jenis: String

UpdateTime

Waktu pembaruan selesai untuk rencana pengujian pemulihan.

Tipe: Timestamp

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

AWS Backup tidak dapat melakukan tindakan yang Anda minta sampai selesai melakukan tindakan sebelumnya. Coba lagi nanti.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateRestoreTestingSelection

Layanan: AWS Backup

Memperbarui pilihan pengujian pemulihan yang ditentukan.

Sebagian besar elemen kecuali `RestoreTestingSelectionName` dapat diperbarui dengan permintaan ini.

Anda dapat menggunakan ARN atau kondisi sumber daya yang dilindungi, tetapi tidak keduanya.

Minta Sintaks

```
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
   }
}
```

Parameter Permintaan URI

Permintaan menggunakan parameter URI berikut.

RestoreTestingPlanName

Nama rencana pengujian pemulihan diperlukan untuk memperbarui rencana pengujian yang ditunjukkan.

Wajib: Ya

RestoreTestingSelectionName

Nama pilihan pengujian pemulihan yang diperlukan dari pilihan pengujian pemulihan yang ingin Anda perbarui.

Wajib: Ya

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

RestoreTestingSelection

Untuk memperbarui pilihan pengujian pemulihan, Anda dapat menggunakan ARN atau kondisi sumber daya yang dilindungi, tetapi tidak keduanya. Artinya, jika pilihan Anda memiliki`ProtectedResourceArns`, meminta pembaruan dengan parameter tidak `ProtectedResourceConditions` akan berhasil.

Tipe: Objek RestoreTestingSelectionForUpdate

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
```

```
   "RestoreTestingSelectionName": "string",
   "UpdateTime": number
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

CreationTime

Waktu pemilihan pengujian sumber daya berhasil diperbarui.

Tipe: Timestamp

RestoreTestingPlanArn

String unik yang merupakan nama dari rencana pengujian pemulihan.

Jenis: String

RestoreTestingPlanName

Rencana pengujian pemulihan yang terkait dengan pemilihan pengujian pemulihan yang diperbarui.

Jenis: String

RestoreTestingSelectionName

Nama pilihan pengujian pemulihan yang dikembalikan.

Jenis: String

UpdateTime

Waktu pembaruan selesai untuk pemilihan pengujian pemulihan.

Tipe: Timestamp

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

AWS Backup tidak dapat melakukan tindakan yang Anda minta sampai selesai melakukan tindakan sebelumnya. Coba lagi nanti.

Kode Status HTTP: 400

InvalidParameterValueException

Menunjukkan bahwa ada sesuatu yang salah dengan nilai parameter. Misalnya, nilainya di luar jangkauan.

Kode Status HTTP: 400

MissingParameterValueException

Menunjukkan bahwa parameter yang diperlukan tidak ada.

Kode Status HTTP: 400

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ada.

Kode Status HTTP: 400

ServiceUnavailableException

Permintaan gagal karena kegagalan sementara server.

Kode Status HTTP: 500

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript

- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

AWS Backup gateway

Tindakan berikut didukungAWS 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

Layanan: AWS Backup gateway

Mengaitkan gateway cadangan dengan server Anda. Setelah Anda menyelesaikan proses asosiasi, Anda dapat mencadangkan dan memulihkan VM Anda melalui gateway.

Sintaksis Permintaan

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway. Gunakan `ListGateways` operasi untuk mengembalikan daftar gateway untuk akun Anda dan. Wilayah AWS

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Ya

ServerArn

Nama Sumber Daya Amazon (ARN) dari server yang meng-host mesin virtual Anda.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "GatewayArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

CreateGateway

Layanan: AWS Backup gateway

Membuat gateway cadangan. Setelah Anda membuat gateway, Anda dapat mengaitkannya dengan server menggunakan `AssociateGatewayToServer` operasi.

Sintaksis Permintaan

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

ActivationKey

Kunci aktivasi gateway yang dibuat.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Pola: `^[0-9a-zA-Z\-]+$`

Wajib: Ya

GatewayDisplayName

Nama tampilan gateway yang dibuat.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Ya

GatewayType

Jenis gateway yang dibuat.

Jenis: String

Nilai yang Valid: `BACKUP_VM`

Wajib: Ya

Tags

Daftar hingga 50 tag untuk ditetapkan ke gateway. Setiap tag adalah pasangan nilai kunci.

Tipe: Array objek Tag

Wajib: Tidak

Sintaksis Respons

```
{
   "GatewayArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway yang Anda buat.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteGateway

Layanan: AWS Backup gateway

Menghapus gateway cadangan.

Sintaksis Permintaan

```
{
   "GatewayArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway yang akan dihapus.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "GatewayArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway yang Anda hapus.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DeleteHypervisor

Layanan: AWS Backup gateway

Menghapus hypervisor.

Sintaksis Permintaan

```
{
   "HypervisorArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor untuk dihapus.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "HypervisorArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor yang Anda hapus.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi tidak dapat dilanjutkan karena Anda memiliki izin yang tidak memadai.

Kode Status HTTP: 400

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

DisassociateGatewayFromServer

Layanan: AWS Backup gateway

Memutus gateway cadangan dari server yang ditentukan. Setelah proses disasosiasi selesai, gateway tidak dapat lagi mengakses mesin virtual di server.

Sintaksis Permintaan

```
{
   "GatewayArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway untuk memisahkan.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "GatewayArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway yang Anda lepaskan.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetBandwidthRateLimitSchedule

Layanan: AWS Backup gateway

Mengambil jadwal batas tingkat bandwidth untuk gateway tertentu. Secara default, gateway tidak memiliki jadwal batas laju bandwidth, yang berarti tidak ada pembatasan laju bandwidth yang berlaku. Gunakan ini untuk mendapatkan jadwal batas tingkat bandwidth gateway.

Sintaksis Permintaan

```
{
   "GatewayArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway. Gunakan `ListGateways`operasi untuk mengembalikan daftar gateway untuk akun Anda dan. Wilayah AWS

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
```

```
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
         }
      ],
      "GatewayArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

BandwidthRateLimitIntervals

Array yang berisi interval jadwal batas laju bandwidth untuk gateway. Ketika tidak ada interval batas laju bandwidth yang dijadwalkan, array kosong.

Tipe: Array objek BandwidthRateLimitInterval

Anggota Array: Jumlah minimum 0 item. Jumlah maksimum 20 item.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway. Gunakan `ListGateways`operasi untuk mengembalikan daftar gateway untuk akun Anda dan. Wilayah AWS

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetGateway

Layanan: AWS Backup gateway

Dengan menyediakan ARN (Amazon Resource Name), API ini mengembalikan gateway.

Sintaksis Permintaan

```
{
   "GatewayArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
```

```
            "DayOfWeek": number,
            "HourOfDay": number,
            "MinuteOfHour": number
        },
        "NextUpdateAvailabilityTime": number,
        "VpcEndpoint": "string"
    }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Gateway

Dengan menyediakan ARN (Amazon Resource Name), API ini mengembalikan gateway.

Tipe: Objek GatewayDetails

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetHypervisor

Layanan: AWS Backup gateway

Tindakan ini meminta informasi tentang hypervisor yang ditentukan yang akan terhubung dengan gateway. Hypervisor adalah perangkat keras, perangkat lunak, atau firmware yang membuat dan mengelola mesin virtual, dan mengalokasikan sumber daya untuk mereka.

Sintaksis Permintaan

```
{
   "HypervisorArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
      "LatestMetadataSyncStatus": "string",
```

```
        "LatestMetadataSyncStatusMessage": "string",
        "LogGroupArn": "string",
        "Name": "string",
        "State": "string"
    }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Hypervisor

Detail tentang hypervisor yang diminta.

Tipe: Objek HypervisorDetails

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetHypervisorPropertyMappings

Layanan: AWS Backup gateway

Tindakan ini mengambil pemetaan properti untuk hypervisor yang ditentukan. Pemetaan properti hypervisor menampilkan hubungan properti entitas yang tersedia dari hypervisor ke properti yang tersedia di. AWS

Sintaksis Permintaan

```
{
   "HypervisorArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
```

```
            "VmwareTagName": "string"
        }
    ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

Amazon Resource Name (ARN) dari IAM role.

Jenis: String

Batasan Panjang: Panjang minimum 20. Panjang maksimum 2048.

Pola: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

Ini adalah tampilan pemetaan tag VMware ke tag. AWS

Tipe: Array objek VmwareToAwsTagMapping

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

GetVirtualMachine

Layanan: AWS Backup gateway

Dengan menyediakan ARN (Amazon Resource Name), API ini mengembalikan mesin virtual.

Sintaksis Permintaan

```
{
   "ResourceArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

ResourceArn

Nama Sumber Daya Amazon (ARN) dari mesin virtual.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
         {
```

```
            "VmwareCategory": "string",
            "VmwareTagDescription": "string",
            "VmwareTagName": "string"
         }
      ]
   }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

VirtualMachine

Objek ini berisi atribut dasar `VirtualMachine` yang terkandung oleh output dari `GetVirtualMachine`

Tipe: Objek VirtualMachineDetails

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ImportHypervisorConfiguration

Layanan: AWS Backup gateway

Connect ke hypervisor dengan mengimpor konfigurasinya.

Sintaksis Permintaan

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

Host

Host server hypervisor. Ini bisa berupa alamat IP atau nama domain yang sepenuhnya memenuhi syarat (FQDN).

Jenis: String

Batasan Panjang: Panjang minimum 3. Panjang maksimum 128.

Pola: `^.+$`

Wajib: Ya

KmsKeyArn

AWS Key Management Service Untuk hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Wajib: Tidak

Name

Nama hypervisor.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Ya

Password

Kata sandi untuk hypervisor.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[ -~]+$`

Wajib: Tidak

Tags

Tag konfigurasi hypervisor untuk diimpor.

Tipe: Array objek Tag

Wajib: Tidak

Username

Nama pengguna untuk hypervisor.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Diperlukan: Tidak

Sintaksis Respons

```
{
   "HypervisorArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor yang Anda lepaskan.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi tidak dapat dilanjutkan karena Anda memiliki izin yang tidak memadai.

Kode Status HTTP: 400

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListGateways

Layanan: AWS Backup gateway

Daftar gateway cadangan yang dimiliki oleh Akun AWS dalam. Wilayah AWS Daftar yang dikembalikan diurutkan berdasarkan gateway Amazon Resource Name (ARN).

Sintaksis Permintaan

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

MaxResults

Jumlah maksimum gateway untuk daftar.

Jenis: Integer

Rentang yang Valid: Nilai minimum 1.

Wajib: Tidak

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `MaxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 1000.

Pola: `^.+$`

Diperlukan: Tidak

Sintaksis Respons

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Gateways

Daftar gateway Anda.

Tipe: Array objek Gateway

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `maxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 1000.

Pola: `^.+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListHypervisors

Layanan: AWS Backup gateway

Daftar hypervisor Anda.

Sintaksis Permintaan

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

MaxResults

Jumlah maksimum hypervisor untuk daftar.

Jenis: Integer

Rentang yang Valid: Nilai minimum 1.

Wajib: Tidak

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `maxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 1000.

Pola: `^.+$`

Diperlukan: Tidak

Sintaksis Respons

```
{
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Hypervisors

Daftar `Hypervisor` objek Anda, diurutkan berdasarkan Amazon Resource Names (ARN) mereka.

Tipe: Array objek Hypervisor

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `maxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjuk oleh token berikutnya.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 1000.

Pola: `^.+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListTagsForResource

Layanan: AWS Backup gateway

Daftar tag yang diterapkan ke sumber daya yang diidentifikasi oleh Amazon Resource Name (ARN).

Sintaksis Permintaan

```
{
   "ResourceArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

ResourceArn

Nama Sumber Daya Amazon (ARN) dari tag sumber daya yang akan dicantumkan.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ResourceArn

Nama Sumber Daya Amazon (ARN) dari tag sumber daya yang Anda cantumkan.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

Daftar tag sumber daya.

Tipe: Array objek Tag

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

ListVirtualMachines

Layanan: AWS Backup gateway

Daftar mesin virtual Anda.

Sintaksis Permintaan

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor yang terhubung ke mesin virtual Anda.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Tidak

MaxResults

Jumlah maksimum mesin virtual untuk daftar.

Jenis: Integer

Rentang yang Valid: Nilai minimum 1.

Wajib: Tidak

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `maxResults` jumlah sumber daya, `NextToken`

memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 1000.

Pola: `^.+$`

Diperlukan: Tidak

Sintaksis Respons

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

NextToken

Item berikutnya mengikuti sebagian daftar sumber daya yang dikembalikan. Misalnya, jika permintaan dibuat untuk mengembalikan `maxResults` jumlah sumber daya, `NextToken` memungkinkan Anda mengembalikan lebih banyak item dalam daftar Anda mulai dari lokasi yang ditunjukkan oleh token berikutnya.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 1000.

Pola: `^.+$`

VirtualMachines

Daftar `VirtualMachine` objek Anda, diurutkan berdasarkan Nama Sumber Daya Amazon (ARN) mereka.

Tipe: Array objek VirtualMachine

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

PutBandwidthRateLimitSchedule

Layanan: AWS Backup gateway

Tindakan ini menetapkan jadwal batas laju bandwidth untuk gateway tertentu. Secara default, gateway tidak memiliki jadwal batas laju bandwidth, yang berarti tidak ada pembatasan laju bandwidth yang berlaku. Gunakan ini untuk memulai jadwal batas tingkat bandwidth gateway.

Sintaksis Permintaan

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

BandwidthRateLimitIntervals

Array yang berisi interval jadwal batas laju bandwidth untuk gateway. Ketika tidak ada interval batas laju bandwidth yang dijadwalkan, array kosong.

Tipe: Array objek BandwidthRateLimitInterval

Anggota Array: Jumlah minimum 0 item. Jumlah maksimum 20 item.

Wajib: Ya

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway. Gunakan `ListGateways`operasi untuk mengembalikan daftar gateway untuk akun Anda dan. Wilayah AWS

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "GatewayArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway. Gunakan `ListGateways`operasi untuk mengembalikan daftar gateway untuk akun Anda dan. Wilayah AWS

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

PutHypervisorPropertyMappings

Layanan: AWS Backup gateway

Tindakan ini menetapkan pemetaan properti untuk hypervisor yang ditentukan. Pemetaan properti hypervisor menampilkan hubungan properti entitas yang tersedia dari hypervisor ke properti yang tersedia di. AWS

Sintaksis Permintaan

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Ya

IamRoleArn

Amazon Resource Name (ARN) dari IAM role.

Jenis: String

Batasan Panjang: Panjang minimum 20. Panjang maksimum 2048.

Pola: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

Wajib: Ya

VmwareToAwsTagMappings

Tindakan ini meminta pemetaan tag VMware ke tag. AWS

Tipe: Array objek VmwareToAwsTagMapping

Wajib: Ya

Sintaksis Respons

```
{
   "HypervisorArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi tidak dapat dilanjutkan karena Anda memiliki izin yang tidak memadai.

Kode Status HTTP: 400

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

PutMaintenanceStartTime

Layanan: AWS Backup gateway

Atur waktu mulai pemeliharaan untuk gateway.

Sintaksis Permintaan

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

DayOfMonth

Hari dalam sebulan memulai pemeliharaan di gateway.

Nilai yang valid berkisar dari `Sunday` sampai `Saturday`.

Jenis: Integer

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 31.

Wajib: Tidak

DayOfWeek

Hari dalam seminggu untuk memulai pemeliharaan di gateway.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 6.

Wajib: Tidak

GatewayArn

Nama Sumber Daya Amazon (ARN) untuk gateway, digunakan untuk menentukan waktu mulai pemeliharaannya.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Ya

HourOfDay

Jam dalam sehari untuk memulai pemeliharaan di gateway.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 23.

Wajib: Ya

MinuteOfHour

Menit jam untuk memulai pemeliharaan di gateway.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 59.

Wajib: Ya

Sintaksis Respons

```
{
   "GatewayArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway tempat Anda mengatur waktu mulai pemeliharaan.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

StartVirtualMachinesMetadataSync

Layanan: AWS Backup gateway

Tindakan ini mengirimkan permintaan untuk menyinkronkan metadata di seluruh mesin virtual yang ditentukan.

Sintaksis Permintaan

```
{
   "HypervisorArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "HypervisorArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi tidak dapat dilanjutkan karena Anda memiliki izin yang tidak memadai.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

TagResource

Layanan: AWS Backup gateway

Tandai sumber daya.

Sintaksis Permintaan

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

ResourceARN

Nama Sumber Daya Amazon (ARN) dari sumber daya yang akan diberi tag.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Ya

Tags

Daftar tag untuk ditetapkan ke sumber daya.

Tipe: Array objek Tag

Wajib: Ya

Sintaksis Respons

```
{
   "ResourceARN": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ResourceARN

Nama Sumber Daya Amazon (ARN) dari sumber daya yang Anda tag.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

TestHypervisorConfiguration

Layanan: AWS Backup gateway

Menguji konfigurasi hypervisor Anda untuk memvalidasi bahwa gateway cadangan dapat terhubung dengan hypervisor dan sumber dayanya.

Sintaksis Permintaan

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway ke hypervisor untuk menguji.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Ya

Host

Host server hypervisor. Ini bisa berupa alamat IP atau nama domain yang sepenuhnya memenuhi syarat (FQDN).

Jenis: String

Batasan Panjang: Panjang minimum 3. Panjang maksimum 128.

Pola: `^.+$`

Wajib: Ya

Password

Kata sandi untuk hypervisor.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[ -~]+$`

Wajib: Tidak

Username

Nama pengguna untuk hypervisor.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Diperlukan: Tidak

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UntagResource

Layanan: AWS Backup gateway

Menghapus tag dari sumber daya.

Sintaksis Permintaan

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

ResourceARN

Nama Sumber Daya Amazon (ARN) dari sumber daya untuk menghapus tag.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Ya

TagKeys

Daftar kunci tag yang menentukan tag mana yang akan dihapus.

Tipe: Array string

Batasan Panjang: Panjang minimum 1. Panjang maksimum 128.

Pola: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "ResourceARN": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ResourceARN

Nama Sumber Daya Amazon (ARN) dari sumber daya tempat Anda menghapus tag.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateGatewayInformation

Layanan: AWS Backup gateway

Memperbarui nama gateway. Tentukan gateway mana yang akan diperbarui menggunakan Nama Sumber Daya Amazon (ARN) gateway dalam permintaan Anda.

Sintaksis Permintaan

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway untuk memperbarui.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Ya

GatewayDisplayName

Nama tampilan gateway yang diperbarui.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Diperlukan: Tidak

Sintaksis Respons

```
{
   "GatewayArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway yang Anda perbarui.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateGatewaySoftwareNow

Layanan: AWS Backup gateway

Memperbarui perangkat lunak gateway virtual machine (VM). Permintaan segera memicu pembaruan perangkat lunak.

> **Note**
>
> Ketika Anda membuat permintaan ini, Anda mendapatkan respon `200 OK` sukses segera. Namun, mungkin perlu beberapa waktu untuk pembaruan selesai.

Sintaksis Permintaan

```
{
   "GatewayArn": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway yang akan diperbarui.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Ya

Sintaksis Respons

```
{
   "GatewayArn": "string"
```

```
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway yang Anda perbarui.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

UpdateHypervisor

Layanan: AWS Backup gateway

Memperbarui metadata hypervisor, termasuk host, nama pengguna, dan kata sandinya. Tentukan hypervisor mana yang akan diperbarui menggunakan Nama Sumber Daya Amazon (ARN) hypervisor dalam permintaan Anda.

Sintaksis Permintaan

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

Parameter Permintaan

Untuk informasi tentang parameter yang umum untuk semua tindakan, lihat Parameter Umum.

Permintaan menerima data berikut dalam format JSON.

Host

Host hypervisor yang diperbarui. Ini bisa berupa alamat IP atau nama domain yang sepenuhnya memenuhi syarat (FQDN).

Jenis: String

Batasan Panjang: Panjang minimum 3. Panjang maksimum 128.

Pola: `^.+$`

Wajib: Tidak

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor untuk diperbarui.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Ya

LogGroupArn

Nama Sumber Daya Amazon (ARN) dari grup gateway dalam log yang diminta.

Jenis: String

Batasan Panjang: Panjang minimum sebesar 0. Panjang maksimum 2048.

Pola: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Wajib: Tidak

Name

Nama yang diperbarui untuk hypervisor

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

Password

Kata sandi yang diperbarui untuk hypervisor.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[ -~]+$`

Wajib: Tidak

Username

Nama pengguna yang diperbarui untuk hypervisor.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Diperlukan: Tidak

Sintaksis Respons

```
{
   "HypervisorArn": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor yang Anda perbarui.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Kesalahan Umum.

AccessDeniedException

Operasi tidak dapat dilanjutkan karena Anda memiliki izin yang tidak memadai.

Kode Status HTTP: 400

ConflictException

Operasi tidak dapat dilanjutkan karena tidak didukung.

Kode Status HTTP: 400

InternalServerException

Operasi tidak berhasil karena terjadi kesalahan internal. Coba lagi nanti.

Kode Status HTTP: 500

ResourceNotFoundException

Sumber daya yang diperlukan untuk tindakan tidak ditemukan.

Kode Status HTTP: 400

ThrottlingException

TPS telah dibatasi untuk melindungi terhadap volume permintaan tinggi yang disengaja atau tidak disengaja.

Kode Status HTTP: 400

ValidationException

Operasi tidak berhasil karena kesalahan validasi terjadi.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS Antarmuka Baris Perintah
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK untuk V3 JavaScript
- AWS SDK for PHP V3
- AWS SDK untuk Python
- AWS SDK for Ruby V3

Tipe Data

Tipe data berikut didukung olehAWS 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

Tipe data berikut didukung olehAWS Backup gateway:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor

- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

Tipe data berikut didukung olehAWS 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

Layanan: AWS Backup

Opsi cadangan untuk setiap jenis sumber daya.

Daftar Isi

BackupOptions

Menentukan opsi cadangan untuk sumber daya yang dipilih. Opsi ini hanya tersedia untuk pekerjaan cadangan Windows VSS.

Nilai valid:

Atur `"WindowsVSS":"enabled"` untuk mengaktifkan opsi `WindowsVSS` cadangan dan membuat cadangan Windows VSS.

Setel `"WindowsVSS":"disabled"` untuk membuat cadangan reguler. `WindowsVSS`Opsi ini tidak diaktifkan secara default.

Jika Anda menentukan opsi yang tidak valid, Anda mendapatkan pengecualian`InvalidParameterValueException`.

Untuk informasi selengkapnya tentang cadangan Windows VSS, lihat Membuat Cadangan Windows berkemampuan VSS.

Tipe: Peta string ke string

Pola Kunci: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Pola nilai: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

ResourceType

Menentukan objek yang berisi jenis sumber daya dan opsi cadangan. Satu-satunya jenis sumber daya yang didukung adalah instans Amazon EC2 dengan Windows Volume Shadow Copy Service (VSS). Sebagai CloudFormation contoh, lihat contoh CloudFormation template untuk mengaktifkan Windows VSS di Panduan AWS Backup Pengguna.

Nilai yang valid:`EC2`.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Diperlukan: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupJob

Layanan: AWS Backup

Berisi informasi rinci tentang pekerjaan cadangan.

Daftar Isi

AccountId

ID akun yang memiliki pekerjaan cadangan.

Jenis: String

Pola: `^[0-9]{12}$`

Wajib: Tidak

BackupJobId

Secara unik mengidentifikasi permintaan AWS Backup untuk membuat cadangan sumber daya.

Tipe: String

Wajib: Tidak

BackupOptions

Menentukan opsi cadangan untuk sumber daya yang dipilih. Opsi ini hanya tersedia untuk pekerjaan cadangan Windows Volume Shadow Copy Service (VSS).

Nilai yang valid: Setel `"WindowsVSS":"enabled"` untuk mengaktifkan opsi `WindowsVSS` cadangan dan membuat cadangan Windows VSS. Setel `"WindowsVSS":"disabled"` untuk membuat cadangan reguler. Jika Anda menentukan opsi yang tidak valid, Anda mendapatkan pengecualian`InvalidParameterValueException`.

Tipe: Peta string ke string

Pola Kunci: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Pola nilai: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

BackupSizeInBytes

Ukuran, dalam byte, cadangan.

Tipe: Panjang

Wajib: Tidak

BackupType

Merupakan jenis cadangan untuk pekerjaan cadangan.

Tipe: String

Wajib: Tidak

BackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Tipe: String

Wajib: Tidak

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Tidak

BytesTransferred

Ukuran dalam byte ditransfer ke brankas cadangan pada saat status pekerjaan ditanyakan.

Tipe: Panjang

Wajib: Tidak

CompletionDate

Tanggal dan waktu pekerjaan untuk membuat pekerjaan cadangan selesai, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

CreatedBy

Berisi informasi identifikasi tentang pembuatan pekerjaan cadangan, termasuk`BackupPlanArn`,`BackupPlanId`,`BackupPlanVersion`, dan `BackupRuleId` rencana cadangan yang digunakan untuk membuatnya.

Tipe: Objek RecoveryPointCreator

Wajib: Tidak

CreationDate

Tanggal dan waktu pekerjaan cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

ExpectedCompletionDate

Tanggal dan waktu pekerjaan untuk membuat cadangan sumber daya diharapkan selesai, dalam format Unix dan Waktu Universal Terkoordinasi (UTC). Nilai akurat `ExpectedCompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

IamRoleArn

Menentukan peran IAM ARN digunakan untuk membuat titik pemulihan target. Peran IAM selain peran default harus menyertakan salah satu `AWSBackup` atau `AwsBackup` dalam nama peran. Misalnya, `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. Nama peran tanpa string tersebut tidak memiliki izin untuk melakukan pekerjaan pencadangan.

Tipe: String

Wajib: Tidak

InitiationDate

Tanggal di mana pekerjaan cadangan dimulai.

Tipe: Timestamp

Wajib: Tidak

IsParent

Ini adalah nilai boolean yang menunjukkan ini adalah pekerjaan cadangan induk (komposit).

Tipe: Boolean

Wajib: Tidak

MessageCategory

Parameter ini adalah jumlah pekerjaan untuk kategori pesan yang ditentukan.

Contoh string dapat mencakup`AccessDenied`,, `SUCCESSAGGREGATE_ALL`, dan`INVALIDPARAMETERS`. Lihat Monitoring untuk daftar MessageCategory string.

Nilai APAPUN mengembalikan jumlah semua kategori pesan.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua kategori pesan dan mengembalikan jumlah.

Tipe: String

Wajib: Tidak

ParentJobId

Ini secara unik mengidentifikasi permintaan AWS Backup untuk membuat cadangan sumber daya. Pengembalian akan menjadi ID pekerjaan induk (komposit).

Tipe: String

Wajib: Tidak

PercentDone

Berisi perkiraan persentase penyelesaian pekerjaan pada saat status pekerjaan ditanyakan.

Tipe: String

Wajib: Tidak

RecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipe: String

Wajib: Tidak

ResourceArn

ARN yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Tipe: String

Wajib: Tidak

ResourceName

Nama non-unik dari sumber daya yang dimiliki oleh cadangan yang ditentukan.

Tipe: String

Wajib: Tidak

ResourceType

Jenis AWS sumber daya yang akan dicadangkan; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS). Untuk backup Windows Volume Shadow Copy Service (VSS), satu-satunya jenis sumber daya yang didukung adalah Amazon EC2.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

StartBy

Menentukan waktu dalam format Unix dan Coordinated Universal Time (UTC) ketika pekerjaan cadangan harus dimulai sebelum dibatalkan. Nilai dihitung dengan menambahkan jendela mulai ke waktu yang dijadwalkan. Jadi jika waktu yang dijadwalkan adalah 6:00 PM dan jendela mulai

adalah 2 jam, `StartBy` waktunya akan menjadi 8:00 PM pada tanggal yang ditentukan. Nilai akurat `StartBy` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

State

Keadaan pekerjaan cadangan saat ini.

Jenis: String

Nilai yang Valid: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

Wajib: Tidak

StatusMessage

Pesan terperinci yang menjelaskan status pekerjaan untuk membuat cadangan sumber daya.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupJobSummary

Layanan: AWS Backup

Ini adalah ringkasan pekerjaan yang dibuat atau berjalan dalam 30 hari terakhir.

Ringkasan yang dikembalikan dapat berisi hal-hal berikut: Wilayah, Akun, Negara Bagian, RestourceType,, MessageCategory, StartTime, EndTime, dan Hitungan pekerjaan yang disertakan.

Daftar Isi

AccountId

ID akun yang memiliki pekerjaan dalam ringkasan.

Jenis: String

Pola: `^[0-9]{12}$`

Wajib: Tidak

Count

Nilai sebagai sejumlah pekerjaan dalam ringkasan pekerjaan.

Tipe: Integer

Wajib: Tidak

EndTime

Nilai waktu dalam format angka waktu akhir pekerjaan.

Nilai ini adalah waktu dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

MessageCategory

Parameter ini adalah jumlah pekerjaan untuk kategori pesan yang ditentukan.

Contoh string termasuk`AccessDenied`,`Success`, dan`InvalidParameters`. Lihat Monitoring untuk daftar MessageCategory string.

Nilai APAPUN mengembalikan jumlah semua kategori pesan.

AGGREGATE_ALLagregat jumlah pekerjaan untuk semua kategori pesan dan mengembalikan jumlah.

Tipe: String

Wajib: Tidak

Region

AWS Wilayah dalam ringkasan pekerjaan.

Tipe: String

Wajib: Tidak

ResourceType

Nilai ini adalah jumlah pekerjaan untuk jenis sumber daya yang ditentukan. Permintaan `GetSupportedResourceTypes` mengembalikan string untuk jenis sumber daya yang didukung.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

StartTime

Nilai waktu dalam format angka waktu mulai pekerjaan.

Nilai ini adalah waktu dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

State

Nilai ini adalah jumlah pekerjaan untuk pekerjaan dengan status yang ditentukan.

Jenis: String

Nilai yang Valid: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupPlan

Layanan: AWS Backup

Berisi nama tampilan rencana cadangan opsional dan array objek `BackupRule`, masing-masing yang menentukan aturan cadangan. Setiap aturan dalam rencana cadangan adalah tugas terjadwal yang terpisah dan dapat mencadangkan pilihan sumber daya AWS yang berbeda.

Daftar Isi

BackupPlanName

Nama tampilan rencana cadangan. Harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Diperlukan: Ya

Rules

Array objek `BackupRule`, masing-masing yang menentukan tugas terjadwal yang digunakan untuk mencadangkan pilihan sumber daya.

Tipe: Array objek BackupRule

Wajib: Ya

AdvancedBackupSettings

Berisi daftar `BackupOptions` untuk setiap jenis sumber daya.

Tipe: Array objek AdvancedBackupSetting

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupPlanInput

Layanan: AWS Backup

Berisi nama tampilan rencana cadangan opsional dan array objek `BackupRule`, masing-masing yang menentukan aturan cadangan. Setiap aturan dalam rencana cadangan adalah tugas terjadwal yang terpisah.

Daftar Isi

BackupPlanName

Nama tampilan rencana cadangan. Harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Diperlukan: Ya

Rules

Array objek `BackupRule`, masing-masing yang menentukan tugas terjadwal yang digunakan untuk mencadangkan pilihan sumber daya.

Tipe: Array objek BackupRuleInput

Wajib: Ya

AdvancedBackupSettings

Menentukan daftar `BackupOptions` untuk setiap jenis sumber daya. Pengaturan ini hanya tersedia untuk pekerjaan cadangan Windows Volume Shadow Copy Service (VSS).

Tipe: Array objek AdvancedBackupSetting

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

BackupPlansListMember

Layanan: AWS Backup

Berisi metadata tentang rencana cadangan.

Daftar Isi

AdvancedBackupSettings

Berisi daftar `BackupOptions` untuk jenis sumber daya.

Tipe: Array objek AdvancedBackupSetting

Wajib: Tidak

BackupPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`

Tipe: String

Wajib: Tidak

BackupPlanId

Secara unik mengidentifikasi rencana cadangan.

Tipe: String

Wajib: Tidak

BackupPlanName

Nama tampilan paket cadangan yang disimpan.

Tipe: String

Wajib: Tidak

CreationDate

Tanggal dan waktu rencana cadangan sumber daya dibuat, dalam format Unix dan Waktu Universal Terkoordinasi (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

CreatorRequestId

String unik yang mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Parameter ini bersifat opsional.

Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

DeletionDate

Tanggal dan waktu paket cadangan dihapus, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `DeletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

LastExecutionDate

Terakhir kali rencana cadangan ini dijalankan. Tanggal dan waktu, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastExecutionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

VersionId

String berkode UTF-8, Unicode, yang dihasilkan secara acak dan unik, dengan panjang maksimal 1.024 byte. ID versi tidak dapat diedit.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupPlanTemplatesListMember

Layanan: AWS Backup

Objek yang menentukan metadata yang terkait dengan template rencana cadangan.

Daftar Isi

BackupPlanTemplateId

Secara unik mengidentifikasi template rencana cadangan yang disimpan.

Tipe: String

Wajib: Tidak

BackupPlanTemplateName

Nama tampilan opsional dari template rencana cadangan.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupRule

Layanan: AWS Backup

Menentukan tugas terjadwal yang digunakan untuk mencadangkan pilihan sumber daya.

Daftar Isi

RuleName

Nama tampilan untuk aturan backup. Harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Ya

TargetBackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

CompletionWindowMinutes

Nilai dalam hitungan menit setelah pekerjaan cadangan berhasil dimulai sebelum harus diselesaikan atau akan dibatalkan oleh AWS Backup. Nilai ini bersifat opsional.

Tipe: Panjang

Wajib: Tidak

CopyActions

Sebuah array `CopyAction` objek, yang berisi rincian operasi copy.

Tipe: Array objek CopyAction

Wajib: Tidak

EnableContinuousBackup

Menentukan apakah AWS Backup membuat backup terus menerus. Penyebab sebenarnya AWS Backup untuk membuat cadangan berkelanjutan yang mampu point-in-time memulihkan (PITR). Salah (atau tidak ditentukan) menyebabkan AWS Backup membuat cadangan snapshot.

Tipe: Boolean

Wajib: Tidak

Lifecycle

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Tipe: Objek Lifecycle

Wajib: Tidak

RecoveryPointTags

Tag yang ditetapkan ke sumber daya yang terkait dengan aturan ini saat dipulihkan dari cadangan.

Tipe: Peta antar string

Wajib: Tidak

RuleId

Secara unik mengidentifikasi aturan yang digunakan untuk menjadwalkan cadangan pilihan sumber daya.

Tipe: String

Wajib: Tidak

ScheduleExpression

Ekspresi cron di UTC yang menentukan kapan AWS Backup memulai pekerjaan cadangan. Untuk informasi selengkapnya tentang ekspresi AWS cron, lihat Menjadwalkan Ekspresi untuk Aturan di Panduan Pengguna CloudWatch Acara Amazon. . Dua contoh ekspresi AWS cron adalah `15 * ? * * *` (ambil cadangan setiap jam pada 15 menit melewati satu jam) dan `0 12 * * ? *` (ambil cadangan setiap hari pada 12 siang UTC). Untuk tabel contoh, klik tautan sebelumnya dan gulir ke bawah halaman.

Tipe: String

Wajib: Tidak

ScheduleExpressionTimezone

Zona waktu di mana ekspresi jadwal diatur. Secara default, ScheduleExpressions ada di UTC. Anda dapat memodifikasi ini ke zona waktu tertentu.

Tipe: String

Wajib: Tidak

StartWindowMinutes

Nilai dalam hitungan menit setelah pencadangan dijadwalkan sebelum pekerjaan akan dibatalkan jika tidak berhasil dimulai. Nilai ini bersifat opsional. Jika nilai ini disertakan, setidaknya harus 60 menit untuk menghindari kesalahan.

Selama jendela mulai, status pekerjaan cadangan tetap dalam `CREATED` status sampai berhasil dimulai atau sampai waktu jendela mulai habis. Jika dalam waktu jendela mulai AWS Backup menerima kesalahan yang memungkinkan pekerjaan untuk dicoba lagi, secara otomatis AWS Backup akan mencoba lagi untuk memulai pekerjaan setidaknya setiap 10 menit sampai pencadangan berhasil dimulai (status pekerjaan berubah menjadi`RUNNING`) atau sampai status pekerjaan berubah menjadi `EXPIRED` (yang diharapkan terjadi ketika waktu jendela mulai selesai).

Tipe: Panjang

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupRuleInput

Layanan: AWS Backup

Menentukan tugas terjadwal yang digunakan untuk mencadangkan pilihan sumber daya.

Daftar Isi

RuleName

Nama tampilan untuk aturan backup. Harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Ya

TargetBackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Ya

CompletionWindowMinutes

Nilai dalam hitungan menit setelah pekerjaan cadangan berhasil dimulai sebelum harus diselesaikan atau akan dibatalkan oleh AWS Backup. Nilai ini bersifat opsional.

Tipe: Panjang

Wajib: Tidak

CopyActions

Sebuah array `CopyAction` objek, yang berisi rincian operasi copy.

Tipe: Array objek CopyAction

Wajib: Tidak

EnableContinuousBackup

Menentukan apakah AWS Backup membuat backup terus menerus. Penyebab sebenarnya AWS Backup untuk membuat cadangan berkelanjutan yang mampu point-in-time memulihkan (PITR). Salah (atau tidak ditentukan) menyebabkan AWS Backup membuat cadangan snapshot.

Tipe: Boolean

Wajib: Tidak

Lifecycle

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup akan transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke penyimpanan dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Parameter ini memiliki nilai maksimum 100 tahun (36.500 hari).

Tipe: Objek Lifecycle

Wajib: Tidak

RecoveryPointTags

Tag untuk menetapkan sumber daya.

Tipe: Peta antar string

Wajib: Tidak

ScheduleExpression

Ekspresi CRON di UTC yang menentukan kapan AWS Backup memulai pekerjaan cadangan.

Tipe: String

Wajib: Tidak

ScheduleExpressionTimezone

Zona waktu di mana ekspresi jadwal diatur. Secara default, ScheduleExpressions ada di UTC. Anda dapat memodifikasi ini ke zona waktu tertentu.

Tipe: String

Wajib: Tidak

StartWindowMinutes

Nilai dalam hitungan menit setelah pencadangan dijadwalkan sebelum pekerjaan akan dibatalkan jika tidak berhasil dimulai. Nilai ini bersifat opsional. Jika nilai ini disertakan, setidaknya harus 60 menit untuk menghindari kesalahan.

Parameter ini memiliki nilai maksimum 100 tahun (52.560.000 menit).

Selama jendela mulai, status pekerjaan cadangan tetap dalam `CREATED` status sampai berhasil dimulai atau sampai waktu jendela mulai habis. Jika dalam waktu jendela mulai AWS Backup menerima kesalahan yang memungkinkan pekerjaan untuk dicoba lagi, secara otomatis AWS Backup akan mencoba lagi untuk memulai pekerjaan setidaknya setiap 10 menit sampai pencadangan berhasil dimulai (status pekerjaan berubah menjadi`RUNNING`) atau sampai status pekerjaan berubah menjadi `EXPIRED` (yang diharapkan terjadi ketika waktu jendela mulai selesai).

Tipe: Panjang

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupSelection

Layanan: AWS Backup

Digunakan untuk menentukan satu set sumber daya untuk rencana cadangan.

Kami menyarankan Anda menentukan kondisi, tag, atau sumber daya untuk disertakan atau dikecualikan. Jika tidak, Backup mencoba untuk memilih semua sumber daya penyimpanan yang didukung dan ikut serta, yang dapat memiliki implikasi biaya yang tidak diinginkan.

Untuk informasi selengkapnya, lihat Menetapkan sumber daya secara terprogram.

Daftar Isi

IamRoleArn

ARN dari peran IAM yang AWS Backup digunakan untuk mengautentikasi saat mencadangkan sumber daya target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Diperlukan: Ya

SelectionName

Nama tampilan dokumen pilihan sumber daya. Harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Ya

Conditions

Kondisi yang Anda tentukan untuk menetapkan sumber daya ke rencana cadangan Anda menggunakan tag. Misalnya, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }`.

`Conditions`mendukung`StringEquals`,`StringLike`,`StringNotEquals`, dan`StringNotLike`. Operator kondisi peka huruf besar/kecil.

Jika Anda menentukan beberapa kondisi, sumber daya sangat cocok dengan semua kondisi (DAN logika).

Tipe: Objek Conditions

Wajib: Tidak

ListOfTags

Kondisi yang Anda tentukan untuk menetapkan sumber daya ke rencana cadangan Anda menggunakan tag. Misalnya, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}`.

`ListOfTags`hanya mendukung`StringEquals`. Operator kondisi peka huruf besar/kecil.

Jika Anda menentukan beberapa kondisi, sumber daya akan cocok dengan salah satu kondisi (logika OR).

Tipe: Array objek Condition

Wajib: Tidak

NotResources

Nama Sumber Daya Amazon (ARN) dari sumber daya yang akan dikecualikan dari paket cadangan. Jumlah maksimum ARN adalah 500 tanpa wildcard, atau 30 ARN dengan wildcard.

Jika Anda perlu mengecualikan banyak sumber daya dari rencana cadangan, pertimbangkan strategi pemilihan sumber daya yang berbeda, seperti menetapkan hanya satu atau beberapa jenis sumber daya atau menyempurnakan pilihan sumber daya Anda menggunakan tag.

Tipe: Array string

Wajib: Tidak

Resources

Nama Sumber Daya Amazon (ARN) sumber daya yang akan ditetapkan ke paket cadangan. Jumlah maksimum ARN adalah 500 tanpa wildcard, atau 30 ARN dengan wildcard.

Jika Anda perlu menetapkan banyak sumber daya ke rencana cadangan, pertimbangkan strategi pemilihan sumber daya yang berbeda, seperti menetapkan semua sumber daya dari jenis sumber daya atau menyempurnakan pemilihan sumber daya Anda menggunakan tag.

Jika Anda menentukan beberapa ARN, sumber daya akan sangat cocok dengan ARN (logika OR) mana pun.

Tipe: Array string

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupSelectionsListMember

Layanan: AWS Backup

Berisi metadata tentang objek. `BackupSelection`

Daftar Isi

BackupPlanId

Secara unik mengidentifikasi rencana cadangan.

Tipe: String

Wajib: Tidak

CreationDate

Tanggal dan waktu rencana cadangan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

CreatorRequestId

String unik yang mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Parameter ini bersifat opsional.

Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

IamRoleArn

Menentukan peran IAM Amazon Resource Name (ARN) untuk membuat titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Wajib: Tidak

SelectionId

Uniknya mengidentifikasi permintaan untuk menetapkan satu set sumber daya untuk rencana cadangan.

Tipe: String

Wajib: Tidak

SelectionName

Nama tampilan dokumen pilihan sumber daya.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Diperlukan: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupVaultListMember

Layanan: AWS Backup

Berisi metadata tentang brankas cadangan.

Daftar Isi

BackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Tipe: String

Wajib: Tidak

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Tidak

CreationDate

Tanggal dan waktu cadangan sumber daya dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

CreatorRequestId

String unik yang mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Parameter ini bersifat opsional.

Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

EncryptionKeyArn

Kunci enkripsi sisi server yang dapat Anda tentukan untuk mengenkripsi cadangan Anda dari layanan yang mendukung manajemen penuh AWS Backup ; misalnya,. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Jika Anda menentukan kunci, Anda harus menentukan ARN, bukan aliasnya. Jika Anda tidak menentukan kunci, AWS Backup buat kunci KMS untuk Anda secara default.

Untuk mempelajari AWS Backup layanan mana yang mendukung AWS Backup manajemen penuh dan cara AWS Backup menangani enkripsi untuk cadangan dari layanan yang belum mendukung penuh AWS Backup, lihat Enkripsi untuk cadangan di AWS Backup

Tipe: String

Wajib: Tidak

LockDate

Tanggal dan waktu ketika konfigurasi AWS Backup Vault Lock menjadi tidak dapat diubah, artinya tidak dapat diubah atau dihapus.

Jika Anda menerapkan Vault Lock ke vault tanpa menentukan tanggal penguncian, Anda dapat mengubah pengaturan Vault Lock, atau menghapus Vault Lock dari vault sepenuhnya, kapan saja.

Nilai ini dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

Locked

Nilai Boolean yang menunjukkan apakah AWS Backup Vault Lock berlaku untuk brankas cadangan yang dipilih. Jika`true`, Vault Lock mencegah menghapus dan memperbarui operasi pada titik pemulihan di brankas yang dipilih.

Tipe: Boolean

Wajib: Tidak

MaxRetentionDays

Pengaturan AWS Backup Vault Lock yang menentukan periode retensi maksimum tempat vault mempertahankan titik pemulihannya. Jika parameter ini tidak ditentukan, Vault Lock tidak memberlakukan periode retensi maksimum pada titik pemulihan di vault (memungkinkan penyimpanan tidak terbatas).

Jika ditentukan, pekerjaan pencadangan atau penyalinan apa pun ke vault harus memiliki kebijakan siklus hidup dengan periode penyimpanan yang sama atau lebih pendek dari periode retensi maksimum. Jika periode retensi pekerjaan lebih lama dari periode retensi maksimum tersebut, vault akan gagal melakukan pekerjaan pencadangan atau penyalinan, dan Anda harus mengubah setelan siklus hidup atau menggunakan brankas yang berbeda. Titik pemulihan yang sudah disimpan di brankas sebelum Vault Lock tidak terpengaruh.

Tipe: Panjang

Wajib: Tidak

MinRetentionDays

Pengaturan AWS Backup Vault Lock yang menentukan periode retensi minimum tempat vault mempertahankan titik pemulihannya. Jika parameter ini tidak ditentukan, Vault Lock tidak memberlakukan periode retensi minimum.

Jika ditentukan, pekerjaan pencadangan atau penyalinan apa pun ke vault harus memiliki kebijakan siklus hidup dengan periode penyimpanan yang sama dengan atau lebih lama dari periode penyimpanan minimum. Jika periode retensi pekerjaan lebih pendek dari periode retensi minimum tersebut, vault akan gagal melakukan pekerjaan pencadangan atau penyalinan, dan Anda harus mengubah setelan siklus hidup atau menggunakan brankas yang berbeda. Titik pemulihan yang sudah disimpan di brankas sebelum Vault Lock tidak terpengaruh.

Tipe: Panjang

Wajib: Tidak

NumberOfRecoveryPoints

Jumlah titik pemulihan yang disimpan dalam brankas cadangan.

Tipe: Panjang

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CalculatedLifecycle

Layanan: AWS Backup

Berisi `DeleteAt` dan `MoveToColdStorageAt` stempel waktu, yang digunakan untuk menentukan siklus hidup untuk titik pemulihan.

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Daftar Isi

DeleteAt

Stempel waktu yang menentukan kapan harus menghapus titik pemulihan.

Tipe: Timestamp

Wajib: Tidak

MoveToColdStorageAt

Stempel waktu yang menentukan kapan harus mentransisikan titik pemulihan ke cold storage.

Tipe: Timestamp

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Condition

Layanan: AWS Backup

Berisi array kembar tiga yang terdiri dari tipe kondisi (sepertiStringEquals), kunci, dan nilai. Digunakan untuk memfilter sumber daya menggunakan tag mereka dan menetapkannya ke rencana cadangan. Peka huruf besar/huruf.

Daftar Isi

ConditionKey

Kunci dalam pasangan nilai kunci. Misalnya, dalam tagDepartment: Accounting, Department adalah kuncinya.

Tipe: String

Diperlukan: Ya

ConditionType

Operasi yang diterapkan pada pasangan nilai kunci yang digunakan untuk menetapkan sumber daya ke paket cadangan Anda. Kondisi hanya mendukungStringEquals. Untuk opsi penugasan yang lebih fleksibel, termasuk StringLike dan kemampuan untuk mengecualikan sumber daya dari paket cadangan Anda, gunakan Conditions (dengan “s” di bagian akhir) untuk Anda BackupSelection.

Jenis: String

Nilai yang Valid: STRINGEQUALS

Wajib: Ya

ConditionValue

Nilai dalam pasangan nilai kunci. Misalnya, dalam tagDepartment: Accounting, Accounting adalah nilainya.

Tipe: String

Wajib: Ya

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ConditionParameter

Layanan: AWS Backup

Menyertakan informasi tentang tag yang Anda tentukan untuk menetapkan sumber daya yang ditandai ke rencana cadangan.

Sertakan awalan `aws:ResourceTag` di tag Anda. Misalnya, `"aws:ResourceTag/TagKey1": "Value1"`.

Daftar Isi

ConditionKey

Kunci dalam pasangan nilai kunci. Misalnya, dalam tag`Department: Accounting`, `Department` adalah kuncinya.

Tipe: String

Wajib: Tidak

ConditionValue

Nilai dalam pasangan nilai kunci. Misalnya, dalam tag`Department: Accounting`, `Accounting` adalah nilainya.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Conditions

Layanan: AWS Backup

Berisi informasi tentang sumber daya mana yang akan disertakan atau dikecualikan dari rencana cadangan menggunakan tag mereka. Kondisi peka huruf besar/kecil.

Daftar Isi

StringEquals

Memfilter nilai sumber daya yang ditandai hanya untuk sumber daya yang Anda beri tag dengan nilai yang sama. Juga disebut “pencocokan tepat.”

Tipe: Array objek ConditionParameter

Wajib: Tidak

StringLike

Memfilter nilai sumber daya yang ditandai untuk mencocokkan nilai tag dengan penggunaan karakter wildcard (*) di mana saja dalam string. Misalnya, “prod*” atau “*rod*” cocok dengan nilai tag “production”.

Tipe: Array objek ConditionParameter

Wajib: Tidak

StringNotEquals

Memfilter nilai sumber daya yang ditandai hanya untuk sumber daya yang Anda beri tag yang tidak memiliki nilai yang sama. Juga disebut “pencocokan yang dinegasikan.”

Tipe: Array objek ConditionParameter

Wajib: Tidak

StringNotLike

Memfilter nilai sumber daya yang ditandai untuk nilai tag yang tidak cocok dengan penggunaan karakter wildcard (*) di mana saja dalam string.

Tipe: Array objek ConditionParameter

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ControlInputParameter

Layanan: AWS Backup

Parameter untuk kontrol. Kontrol dapat memiliki nol, satu, atau lebih dari satu parameter. Contoh kontrol dengan dua parameter adalah: “frekuensi rencana cadangan setidaknya `daily` dan periode retensi setidaknya`1 year`”. Parameter pertama adalah`daily`. Parameter kedua adalah`1 year`.

Daftar Isi

ParameterName

Nama parameter, misalnya,`BackupPlanFrequency`.

Tipe: String

Wajib: Tidak

ParameterValue

Nilai parameter, misalnya,`hourly`.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ControlScope

Layanan: AWS Backup

Framework terdiri dari satu atau lebih kontrol. Setiap kontrol memiliki ruang lingkup kontrolnya sendiri. Cakupan kontrol dapat mencakup satu atau beberapa jenis sumber daya, kombinasi kunci tag dan nilai, atau kombinasi dari satu jenis sumber daya dan satu ID sumber daya. Jika tidak ada cakupan yang ditentukan, evaluasi untuk aturan akan dipicu ketika sumber daya apa pun dalam grup rekaman Anda berubah dalam konfigurasi.

> **Note**
>
> Untuk mengatur cakupan kontrol yang mencakup semua sumber daya tertentu, biarkan `ControlScope` kosong atau jangan teruskan saat memanggil`CreateFramework`.

Daftar Isi

ComplianceResourceIds

ID dari satu-satunya AWS sumber daya yang Anda inginkan untuk memuat cakupan kontrol Anda.

Tipe: Array string

Anggota Array: Jumlah minimum 1 item. Jumlah maksimum 100 item.

Wajib: Tidak

ComplianceResourceTypes

Menjelaskan apakah ruang lingkup kontrol mencakup satu atau lebih jenis sumber daya, seperti `EFS` atau`RDS`.

Tipe: Array string

Wajib: Tidak

Tags

Pasangan nilai kunci tag diterapkan pada AWS sumber daya yang ingin Anda picu evaluasi untuk aturan. Maksimal satu pasangan kunci-nilai dapat disediakan. Nilai tag bersifat opsional, tetapi tidak bisa berupa string kosong jika Anda membuat atau mengedit kerangka kerja dari konsol (meskipun nilainya bisa berupa string kosong saat disertakan dalam CloudFormation templat).

Struktur untuk menetapkan tag adalah:`[{"Key":"string","Value":"string"}]`.

Tipe: Peta antar string

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyAction

Layanan: AWS Backup

Rincian operasi penyalinan.

Daftar Isi

DestinationBackupVaultArn

Sebuah Amazon Resource Name (ARN) yang secara unik mengidentifikasi kubah backup tujuan untuk backup yang disalin. Sebagai contoh, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipe: String

Diperlukan: Ya

Lifecycle

Menentukan periode waktu, dalam beberapa hari, sebelum transisi titik pemulihan ke cold storage atau dihapus.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pada konsol, pengaturan retensi harus 90 hari lebih besar dari transisi ke pengaturan dingin setelah hari. Transisi ke pengaturan dingin setelah hari tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Untuk menghapus siklus hidup dan periode retensi yang ada dan menjaga titik pemulihan Anda tanpa batas waktu, tentukan -1 untuk dan. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Tipe: Objek Lifecycle

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyJob

Layanan: AWS Backup

Berisi informasi terperinci tentang pekerjaan penyalinan.

Daftar Isi

AccountId

ID akun yang memiliki pekerjaan fotokopi.

Jenis: String

Pola: `^[0-9]{12}$`

Wajib: Tidak

BackupSizeInBytes

Ukuran, dalam byte, dari pekerjaan salinan.

Tipe: Panjang

Wajib: Tidak

ChildJobsInState

Ini mengembalikan statistik pekerjaan salinan anak (bersarang) yang disertakan.

Jenis: String ke peta panjang

Kunci yang valid: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Wajib: Tidak

CompletionDate

Tanggal dan waktu pekerjaan copy selesai, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

CompositeMemberIdentifier

Pengidentifikasi sumber daya dalam grup komposit, seperti titik pemulihan bersarang (anak) milik tumpukan komposit (induk). ID ditransfer dari ID logis dalam tumpukan.

Tipe: String

Wajib: Tidak

CopyJobId

Mengidentifikasi pekerjaan fotokopi secara unik.

Tipe: String

Wajib: Tidak

CreatedBy

Berisi informasi tentang rencana cadangan dan aturan yang AWS Backup digunakan untuk memulai pencadangan titik pemulihan.

Tipe: Objek RecoveryPointCreator

Wajib: Tidak

CreationDate

Tanggal dan waktu pekerjaan copy dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

DestinationBackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas salinan tujuan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Tipe: String

Wajib: Tidak

DestinationRecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan tujuan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipe: String

Wajib: Tidak

IamRoleArn

Menentukan peran IAM ARN digunakan untuk menyalin titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Wajib: Tidak

IsParent

Ini adalah nilai boolean yang menunjukkan ini adalah pekerjaan salinan induk (komposit).

Tipe: Boolean

Wajib: Tidak

MessageCategory

Parameter ini adalah jumlah pekerjaan untuk kategori pesan yang ditentukan.

Contoh string dapat mencakup`AccessDenied`,, `SUCCESSAGGREGATE_ALL`, dan`InvalidParameters`. Lihat Monitoring untuk daftar MessageCategory string.

Nilai APAPUN mengembalikan jumlah semua kategori pesan.

`AGGREGATE_ALL`agregat jumlah pekerjaan untuk semua kategori pesan dan mengembalikan jumlah

Tipe: String

Wajib: Tidak

NumberOfChildJobs

Jumlah pekerjaan fotokopi anak (bersarang).

Tipe: Panjang

Wajib: Tidak

ParentJobId

Ini secara unik mengidentifikasi permintaan AWS Backup untuk menyalin sumber daya. Pengembalian akan menjadi ID pekerjaan induk (komposit).

Tipe: String

Wajib: Tidak

ResourceArn

AWS Sumber daya yang akan disalin; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS).

Tipe: String

Wajib: Tidak

ResourceName

Nama non-unik dari sumber daya yang dimiliki oleh cadangan yang ditentukan.

Tipe: String

Wajib: Tidak

ResourceType

Jenis AWS sumber daya yang akan disalin; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS).

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

SourceBackupVaultArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi brankas salinan sumber; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Tipe: String

Wajib: Tidak

SourceRecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan sumber; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipe: String

Wajib: Tidak

State

Keadaan pekerjaan fotokopi saat ini.

Jenis: String

Nilai yang Valid: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Wajib: Tidak

StatusMessage

Pesan terperinci yang menjelaskan status pekerjaan untuk menyalin sumber daya.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyJobSummary

Layanan: AWS Backup

Ini adalah ringkasan pekerjaan salinan yang dibuat atau berjalan dalam 30 hari terakhir.

Ringkasan yang dikembalikan dapat berisi hal-hal berikut: Wilayah, Akun, Negara Bagian, RestourceType,, MessageCategory, StartTime, EndTime, dan Hitungan pekerjaan yang disertakan.

Daftar Isi

AccountId

ID akun yang memiliki pekerjaan dalam ringkasan.

Jenis: String

Pola: `^[0-9]{12}$`

Wajib: Tidak

Count

Nilai sebagai sejumlah pekerjaan dalam ringkasan pekerjaan.

Tipe: Integer

Wajib: Tidak

EndTime

Nilai waktu dalam format angka waktu akhir pekerjaan.

Nilai ini adalah waktu dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

MessageCategory

Parameter ini adalah jumlah pekerjaan untuk kategori pesan yang ditentukan.

Contoh string termasuk`AccessDenied`,`Success`, dan`InvalidParameters`. Lihat Monitoring untuk daftar MessageCategory string.

Nilai APAPUN mengembalikan jumlah semua kategori pesan.

AGGREGATE_ALLagregat jumlah pekerjaan untuk semua kategori pesan dan mengembalikan jumlah.

Tipe: String

Wajib: Tidak

Region

AWS Wilayah dalam ringkasan pekerjaan.

Tipe: String

Wajib: Tidak

ResourceType

Nilai ini adalah jumlah pekerjaan untuk jenis sumber daya yang ditentukan. Permintaan GetSupportedResourceTypes mengembalikan string untuk jenis sumber daya yang didukung

Jenis: String

Pola: ^[a-zA-Z0-9\-_\.]{1,50}$

Wajib: Tidak

StartTime

Nilai waktu dalam format angka waktu mulai pekerjaan.

Nilai ini adalah waktu dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

State

Nilai ini adalah jumlah pekerjaan untuk pekerjaan dengan status yang ditentukan.

Jenis: String

Nilai yang Valid: CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DateRange

Layanan: AWS Backup

Ini adalah filter sumber daya yang berisi FromDate: DateTime dan ToDate: DateTime. Kedua nilai tersebut diperlukan. DateTime Nilai masa depan tidak diizinkan.

Tanggal dan waktu dalam format Unix dan Coordinated Universal Time (UTC), dan akurat hingga milidetik ((milidetik adalah opsional). Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Daftar Isi

FromDate

Nilai ini adalah tanggal awal, inklusif.

Tanggal dan waktu dalam format Unix dan Coordinated Universal Time (UTC), dan akurat hingga milidetik (milidetik adalah opsional).

Tipe: Timestamp

Wajib: Ya

ToDate

Nilai ini adalah tanggal akhir, inklusif.

Tanggal dan waktu dalam format Unix dan Coordinated Universal Time (UTC), dan akurat hingga milidetik (milidetik adalah opsional).

Tipe: Timestamp

Wajib: Ya

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Framework

Layanan: AWS Backup

Berisi informasi rinci tentang kerangka kerja. Kerangka kerja berisi kontrol, yang mengevaluasi dan melaporkan peristiwa dan sumber daya cadangan Anda. Kerangka kerja menghasilkan hasil kepatuhan harian.

Daftar Isi

CreationTime

Tanggal dan waktu kerangka kerja dibuat, dalam representasi ISO 8601. Nilai akurat `CreationTime` untuk milidetik. Misalnya, 2020-07-10T 15:00:00.000-08:00 mewakili tanggal 10 Juli 2020 pukul 15:00 8 jam di belakang UTC.

Tipe: Timestamp

Wajib: Tidak

DeploymentStatus

Status penyebaran kerangka kerja. Statusnya adalah:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Tipe: String

Wajib: Tidak

FrameworkArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Tipe: String

Wajib: Tidak

FrameworkDescription

Deskripsi opsional kerangka kerja dengan maksimum 1.024 karakter.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 1024.

Pola: `.*\S.*`

Wajib: Tidak

FrameworkName

Nama unik dari sebuah kerangka kerja. Nama ini antara 1 dan 256 karakter, dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Tidak

NumberOfControls

Jumlah kontrol yang terkandung oleh kerangka kerja.

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FrameworkControl

Layanan: AWS Backup

Berisi informasi rinci tentang semua kontrol kerangka kerja. Setiap kerangka kerja harus berisi setidaknya satu kontrol.

Daftar Isi

ControlName

Nama kontrol. Nama ini antara 1 dan 256 karakter.

Tipe: String

Diperlukan: Ya

ControlInputParameters

Pasangan nama/nilai.

Tipe: Array objek ControlInputParameter

Wajib: Tidak

ControlScope

Ruang lingkup kontrol. Ruang lingkup kontrol mendefinisikan apa yang akan dievaluasi oleh kontrol. Tiga contoh cakupan kontrol adalah: rencana cadangan khusus, semua rencana cadangan dengan tag tertentu, atau semua rencana cadangan.

Untuk informasi lebih lanjut, lihat `ControlScope.`

Tipe: Objek ControlScope

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

KeyValue

Layanan: AWS Backup

Sepasang dua string terkait. Karakter yang diizinkan adalah huruf, spasi putih, dan angka yang dapat direpresentasikan dalam UTF-8 dan karakter berikut: `+ - = . _ : /`

Daftar Isi

Key

Kunci tag (String). Kunci tidak dapat diawali dengan `aws:`.

Batasan Panjang: Panjang minimum 1. Panjang maksimum 128.

Pola: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Tipe: String

Diperlukan: Ya

Value

Nilai kuncinya.

Batasan Panjang: Panjang maksimum 256.

Pola: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Tipe: String

Wajib: Ya

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LegalHold

Layanan: AWS Backup

Penahanan hukum adalah alat administratif yang membantu mencegah cadangan dihapus saat berada di bawah penahanan. Saat penahanan dilakukan, pencadangan di bawah penahanan tidak dapat dihapus dan kebijakan siklus hidup yang akan mengubah status pencadangan (seperti transisi ke penyimpanan dingin) ditunda hingga penahanan hukum dihapus. Cadangan dapat memiliki lebih dari satu pegangan hukum. Penahanan hukum diterapkan pada satu atau lebih cadangan (juga dikenal sebagai titik pemulihan). Cadangan ini dapat difilter berdasarkan jenis sumber daya dan ID sumber daya.

Daftar Isi

CancellationDate

Waktu ketika penangguhan hukum dibatalkan.

Tipe: Timestamp

Wajib: Tidak

CreationDate

Waktu ketika penahanan hukum dibuat.

Tipe: Timestamp

Wajib: Tidak

Description

Deskripsi penahanan hukum.

Tipe: String

Wajib: Tidak

LegalHoldArn

Nama Sumber Daya Amazon (ARN) dari penangguhan hukum; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipe: String

Wajib: Tidak

LegalHoldId

ID penahanan hukum.

Tipe: String

Wajib: Tidak

Status

Status penahanan hukum.

Jenis: String

Nilai yang Valid: `CREATING | ACTIVE | CANCELING | CANCELED`

Wajib: Tidak

Title

Judul pegangan hukum.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Lifecycle

Layanan: AWS Backup

Menentukan periode waktu, dalam beberapa hari, sebelum transisi titik pemulihan ke cold storage atau dihapus.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pada konsol, pengaturan retensi harus 90 hari lebih besar dari transisi ke pengaturan dingin setelah hari. Transisi ke pengaturan dingin setelah hari tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Untuk menghapus siklus hidup dan periode retensi yang ada dan menjaga titik pemulihan Anda tanpa batas waktu, tentukan -1 untuk dan. `MoveToColdStorageAfterDays` `DeleteAfterDays`

Daftar Isi

DeleteAfterDays

Jumlah hari setelah pembuatan bahwa titik pemulihan dihapus. Nilai ini harus setidaknya 90 hari setelah jumlah hari yang ditentukan dalam`MoveToColdStorageAfterDays`.

Tipe: Panjang

Wajib: Tidak

MoveToColdStorageAfterDays

Jumlah hari setelah penciptaan bahwa titik pemulihan dipindahkan ke cold storage.

Tipe: Panjang

Wajib: Tidak

OptInToArchiveForSupportedResources

Jika nilainya benar, paket cadangan Anda mentransisikan sumber daya yang didukung ke tingkat penyimpanan arsip (dingin) sesuai dengan pengaturan siklus hidup Anda.

Tipe: Boolean

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectedResource

Layanan: AWS Backup

Struktur yang berisi informasi tentang sumber daya yang dicadangkan.

Daftar Isi

LastBackupTime

Tanggal dan waktu sumber daya terakhir dicadangkan, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastBackupTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

LastBackupVaultArn

ARN (Nama Sumber Daya Amazon) dari brankas cadangan yang berisi titik pemulihan cadangan terbaru.

Tipe: String

Wajib: Tidak

LastRecoveryPointArn

ARN (Nama Sumber Daya Amazon) dari titik pemulihan terbaru.

Tipe: String

Wajib: Tidak

ResourceArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Tipe: String

Wajib: Tidak

ResourceName

Nama non-unik dari sumber daya yang dimiliki oleh cadangan yang ditentukan.

Tipe: String

Wajib: Tidak

ResourceType

Jenis AWS sumber daya; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS). Untuk backup Windows Volume Shadow Copy Service (VSS), satu-satunya jenis sumber daya yang didukung adalah Amazon EC2.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Diperlukan: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectedResourceConditions

Layanan: AWS Backup

Kondisi yang Anda tentukan untuk sumber daya dalam rencana pengujian pemulihan menggunakan tag.

Misalnya, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Operator kondisi peka huruf besar/kecil.

Daftar Isi

StringEquals

Memfilter nilai sumber daya yang ditandai hanya untuk sumber daya yang Anda beri tag dengan nilai yang sama. Juga disebut “pencocokan tepat.”

Tipe: Array objek KeyValue

Wajib: Tidak

StringNotEquals

Memfilter nilai sumber daya yang ditandai hanya untuk sumber daya yang Anda beri tag yang tidak memiliki nilai yang sama. Juga disebut “pencocokan yang dinegasikan.”

Tipe: Array objek KeyValue

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointByBackupVault

Layanan: AWS Backup

Berisi informasi rinci tentang titik pemulihan yang disimpan dalam brankas cadangan.

Daftar Isi

BackupSizeInBytes

Ukuran, dalam byte, cadangan.

Tipe: Panjang

Wajib: Tidak

BackupVaultArn

ARN yang secara unik mengidentifikasi brankas cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`

Tipe: String

Wajib: Tidak

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Tidak

CalculatedLifecycle

Sebuah `CalculatedLifecycle` benda yang berisi `DeleteAt` dan `MoveToColdStorageAt` stempel waktu.

Tipe: Objek CalculatedLifecycle

Wajib: Tidak

CompletionDate

Tanggal dan waktu pekerjaan untuk memulihkan titik pemulihan selesai, dalam format Unix dan Waktu Universal Terkoordinasi (UTC). Nilai akurat `CompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

CompositeMemberIdentifier

Pengidentifikasi sumber daya dalam grup komposit, seperti titik pemulihan bersarang (anak) milik tumpukan komposit (induk). ID ditransfer dari ID logis dalam tumpukan.

Tipe: String

Wajib: Tidak

CreatedBy

Berisi informasi identifikasi tentang pembuatan titik pemulihan, termasuk `BackupPlanArnBackupPlanId`,`BackupPlanVersion`,, dan `BackupRuleId` rencana cadangan yang digunakan untuk membuatnya.

Tipe: Objek RecoveryPointCreator

Wajib: Tidak

CreationDate

Tanggal dan waktu titik pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

EncryptionKeyArn

Kunci enkripsi sisi server yang digunakan untuk melindungi cadangan Anda; misalnya, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipe: String

Wajib: Tidak

IamRoleArn

Menentukan peran IAM ARN digunakan untuk membuat titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Wajib: Tidak

IsEncrypted

Nilai Boolean yang dikembalikan `TRUE` seolah-olah titik pemulihan yang ditentukan dienkripsi, atau `FALSE` jika titik pemulihan tidak dienkripsi.

Tipe: Boolean

Wajib: Tidak

IsParent

Ini adalah nilai boolean yang menunjukkan ini adalah titik pemulihan induk (komposit).

Tipe: Boolean

Wajib: Tidak

LastRestoreTime

Tanggal dan waktu titik pemulihan terakhir dipulihkan, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastRestoreTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

Lifecycle

Siklus hidup menentukan kapan sumber daya yang dilindungi dialihkan ke penyimpanan dingin dan kapan sumber daya tersebut kedaluwarsa. AWS Backup transisi dan kedaluwarsa backup secara otomatis sesuai dengan siklus hidup yang Anda tentukan.

Backup yang dialihkan ke penyimpanan dingin harus disimpan dalam penyimpanan dingin minimal 90 hari. Oleh karena itu, pengaturan “retensi” harus 90 hari lebih besar dari pengaturan “transisi ke dingin setelah hari”. Pengaturan “transisi ke dingin setelah hari” tidak dapat diubah setelah cadangan dialihkan ke dingin.

Jenis sumber daya yang dapat bertransisi ke penyimpanan dingin tercantum dalam tabel Ketersediaan fitur menurut sumber daya. AWS Backup mengabaikan ekspresi ini untuk jenis sumber daya lainnya.

Tipe: Objek Lifecycle

Wajib: Tidak

ParentRecoveryPointArn

Nama Sumber Daya Amazon (ARN) dari titik pemulihan induk (komposit).

Tipe: String

Wajib: Tidak

RecoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipe: String

Wajib: Tidak

ResourceArn

ARN yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Tipe: String

Wajib: Tidak

ResourceName

Nama non-unik dari sumber daya yang dimiliki oleh cadangan yang ditentukan.

Tipe: String

Wajib: Tidak

ResourceType

Jenis AWS sumber daya yang disimpan sebagai titik pemulihan; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS). Untuk backup Windows Volume Shadow Copy Service (VSS), satu-satunya jenis sumber daya yang didukung adalah Amazon EC2.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

SourceBackupVaultArn

Brankas cadangan tempat titik pemulihan awalnya disalin. Jika titik pemulihan dikembalikan ke akun yang sama, nilai ini akan menjadi`null`.

Tipe: String

Wajib: Tidak

Status

Kode status yang menentukan keadaan titik pemulihan.

Jenis: String

Nilai yang Valid: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Wajib: Tidak

StatusMessage

Pesan yang menjelaskan status titik pemulihan saat ini.

Tipe: String

Wajib: Tidak

VaultType

Jenis lemari besi tempat titik pemulihan yang dijelaskan disimpan.

Jenis: String

Nilai yang Valid: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointByResource

Layanan: AWS Backup

Berisi informasi terperinci tentang titik pemulihan yang disimpan.

Daftar Isi

BackupSizeBytes

Ukuran, dalam byte, cadangan.

Tipe: Panjang

Wajib: Tidak

BackupVaultName

Nama kontainer logis tempat cadangan disimpan. Vault cadangan diidentifikasi berdasarkan nama yang unik untuk akun yang digunakan untuk membuatnya dan Wilayah AWS tempatnya dibuat.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Tidak

CreationDate

Tanggal dan waktu titik pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

EncryptionKeyArn

Kunci enkripsi sisi server yang digunakan untuk melindungi cadangan Anda; misalnya, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipe: String

Wajib: Tidak

IsParent

Ini adalah nilai boolean yang menunjukkan ini adalah titik pemulihan induk (komposit).

Tipe: Boolean

Wajib: Tidak

ParentRecoveryPointArn

Nama Sumber Daya Amazon (ARN) dari titik pemulihan induk (komposit).

Tipe: String

Wajib: Tidak

RecoveryPointArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipe: String

Wajib: Tidak

ResourceName

Nama non-unik dari sumber daya yang dimiliki oleh cadangan yang ditentukan.

Tipe: String

Wajib: Tidak

Status

Kode status yang menentukan keadaan titik pemulihan.

Jenis: String

Nilai yang Valid: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Wajib: Tidak

StatusMessage

Pesan yang menjelaskan status titik pemulihan saat ini.

Tipe: String

Wajib: Tidak

VaultType

Jenis lemari besi tempat titik pemulihan yang dijelaskan disimpan.

Jenis: String

Nilai yang Valid: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointCreator

Layanan: AWS Backup

Berisi informasi tentang rencana cadangan dan aturan yang AWS Backup digunakan untuk memulai pencadangan titik pemulihan.

Daftar Isi

BackupPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana cadangan; misalnya,. `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`

Tipe: String

Wajib: Tidak

BackupPlanId

Secara unik mengidentifikasi rencana cadangan.

Tipe: String

Wajib: Tidak

BackupPlanVersion

ID versi adalah string unik, dibuat secara acak, Unicode, UTF-8 yang dikodekan dengan panjang paling banyak 1.024 byte. Mereka tidak dapat diedit.

Tipe: String

Wajib: Tidak

BackupRuleId

Secara unik mengidentifikasi aturan yang digunakan untuk menjadwalkan cadangan pilihan sumber daya.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointMember

Layanan: AWS Backup

Ini adalah titik pemulihan yang merupakan titik pemulihan anak (bersarang) dari titik pemulihan induk (komposit). Poin pemulihan ini dapat terlepas dari titik pemulihan induk (komposit) mereka, dalam hal ini mereka tidak akan lagi menjadi anggota.

Daftar Isi

BackupVaultName

Nama brankas cadangan (wadah logis tempat cadangan disimpan).

Jenis: String

Pola: `^[a-zA-Z0-9\-\_]{2,50}$`

Wajib: Tidak

RecoveryPointArn

Nama Sumber Daya Amazon (ARN) dari titik pemulihan induk (komposit).

Tipe: String

Wajib: Tidak

ResourceArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya yang disimpan.

Tipe: String

Wajib: Tidak

ResourceType

Jenis AWS sumber daya yang disimpan sebagai titik pemulihan.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Diperlukan: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointSelection

Layanan: AWS Backup

Ini menentukan kriteria untuk menetapkan satu set sumber daya, seperti jenis sumber daya atau brankas cadangan.

Daftar Isi

DateRange

Ini adalah filter sumber daya yang berisi FromDate: DateTime dan ToDate: DateTime. Kedua nilai tersebut diperlukan. DateTime Nilai masa depan tidak diizinkan.

Tanggal dan waktu dalam format Unix dan Coordinated Universal Time (UTC), dan akurat hingga milidetik ((milidetik adalah opsional). Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Objek DateRange

Wajib: Tidak

ResourceIdentifiers

Ini adalah sumber daya yang termasuk dalam pemilihan sumber daya (termasuk jenis sumber daya dan brankas).

Tipe: Array string

Wajib: Tidak

VaultNames

Ini adalah nama-nama brankas di mana titik pemulihan yang dipilih terkandung.

Tipe: Array string

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportDeliveryChannel

Layanan: AWS Backup

Berisi informasi dari paket laporan Anda tentang tempat pengiriman laporan, khususnya nama bucket Amazon S3, key prefix S3, dan format laporan Anda.

Daftar Isi

S3BucketName

Nama unik bucket S3 yang menerima laporan Anda.

Tipe: String

Diperlukan: Ya

Formats

Format laporan Anda:`CSV`,`JSON`, atau keduanya. Jika tidak ditentukan, format defaultnya adalah`CSV`.

Tipe: Array string

Wajib: Tidak

S3KeyPrefix

Awalan tempat AWS Backup Audit Manager mengirimkan laporan Anda ke Amazon S3. Awalan ini adalah bagian dari jalur berikut: s3:///your-bucket-name/backup/us-west-2/year/month/day/report-name. `prefix` Jika tidak ditentukan, tidak ada awalan.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

ReportDestination

Layanan: AWS Backup

Berisi informasi dari pekerjaan laporan Anda tentang tujuan laporan Anda.

Daftar Isi

S3BucketName

Nama unik bucket Amazon S3 yang menerima laporan Anda.

Tipe: String

Wajib: Tidak

S3Keys

Kunci objek yang secara unik mengidentifikasi laporan Anda di bucket S3 Anda.

Tipe: Array string

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportJob

Layanan: AWS Backup

Berisi informasi rinci tentang pekerjaan laporan. Pekerjaan laporan mengkompilasi laporan berdasarkan rencana laporan dan menerbitkannya ke Amazon S3.

Daftar Isi

CompletionTime

Tanggal dan waktu pekerjaan laporan selesai, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CompletionTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

CreationTime

Tanggal dan waktu pekerjaan laporan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

ReportDestination

Nama bucket S3 dan kunci S3 untuk tujuan tempat pekerjaan laporan menerbitkan laporan.

Tipe: Objek ReportDestination

Wajib: Tidak

ReportJobId

Pengidentifikasi untuk pekerjaan laporan. String unik yang dihasilkan secara acak, Unicode, UTF-8 yang dikodekan dengan panjang paling banyak 1.024 byte. Laporan ID pekerjaan tidak dapat diedit.

Tipe: String

Wajib: Tidak

ReportPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Tipe: String

Wajib: Tidak

ReportTemplate

Mengidentifikasi template laporan untuk laporan. Laporan dibuat menggunakan template laporan. Template laporan adalah:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Tipe: String

Wajib: Tidak

Status

Status pekerjaan laporan. Statusnya adalah:

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED`berarti bahwa laporan tersedia untuk ditinjau di tujuan yang Anda tentukan. Jika statusnya`FAILED`, tinjau `StatusMessage` alasannya.

Tipe: String

Wajib: Tidak

StatusMessage

Pesan yang menjelaskan status pekerjaan laporan.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportPlan

Layanan: AWS Backup

Berisi informasi rinci tentang rencana laporan.

Daftar Isi

CreationTime

Tanggal dan waktu rencana laporan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

DeploymentStatus

Status penyebaran rencana laporan. Statusnya adalah:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED`

Tipe: String

Wajib: Tidak

LastAttemptedExecutionTime

Tanggal dan waktu pekerjaan laporan yang terkait dengan rencana laporan ini terakhir kali dicoba untuk dijalankan, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastAttemptedExecutionTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

LastSuccessfulExecutionTime

Tanggal dan waktu pekerjaan laporan yang terkait dengan rencana laporan ini terakhir berhasil dijalankan, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastSuccessfulExecutionTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

ReportDeliveryChannel

Berisi informasi tentang tempat dan cara mengirimkan laporan, khususnya nama bucket Amazon S3, key prefix S3, dan format laporan Anda.

Tipe: Objek ReportDeliveryChannel

Wajib: Tidak

ReportPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Tipe: String

Wajib: Tidak

ReportPlanDescription

Deskripsi opsional dari rencana laporan dengan maksimum 1.024 karakter.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 1024.

Pola: `.*\S.*`

Wajib: Tidak

ReportPlanName

Nama unik dari rencana laporan. Nama ini antara 1 dan 256 karakter dimulai dengan huruf, dan terdiri dari huruf (a-z, A-Z), angka (0-9), dan garis bawah (_).

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Pola: `[a-zA-Z][_a-zA-Z0-9]*`

Wajib: Tidak

ReportSetting

Mengidentifikasi template laporan untuk laporan. Laporan dibuat menggunakan template laporan. Template laporan adalah:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Jika template laporan adalah `RESOURCE_COMPLIANCE_REPORT` atau`CONTROL_COMPLIANCE_REPORT`, sumber daya API ini juga menjelaskan cakupan laporan oleh Wilayah AWS dan kerangka kerja.

Tipe: Objek ReportSetting

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportSetting

Layanan: AWS Backup

Berisi informasi rinci tentang pengaturan laporan.

Daftar Isi

ReportTemplate

Mengidentifikasi template laporan untuk laporan. Laporan dibuat menggunakan template laporan. Template laporan adalah:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Tipe: String

Diperlukan: Ya

Accounts

Ini adalah akun yang akan dimasukkan dalam laporan.

Gunakan nilai string `ROOT` untuk menyertakan semua unit organisasi.

Tipe: Array string

Wajib: Tidak

FrameworkArns

Nama Sumber Daya Amazon (ARN) dari kerangka kerja yang dicakup laporan.

Tipe: Array string

Wajib: Tidak

NumberOfFrameworks

Jumlah kerangka kerja yang dicakup laporan.

Tipe: Integer

Wajib: Tidak

OrganizationUnits

Ini adalah Unit Organisasi yang akan dimasukkan dalam laporan.

Tipe: Array string

Wajib: Tidak

Regions

Ini adalah Wilayah yang akan dimasukkan dalam laporan.

Gunakan wildcard sebagai nilai string untuk menyertakan semua Wilayah.

Tipe: Array string

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobCreator

Layanan: AWS Backup

Berisi informasi tentang rencana pengujian pemulihan yang AWS Backup digunakan untuk memulai pekerjaan pemulihan.

Daftar Isi

RestoreTestingPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana pengujian pemulihan.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobsListMember

Layanan: AWS Backup

Berisi metadata tentang pekerjaan pemulihan.

Daftar Isi

AccountId

ID akun yang memiliki pekerjaan pemulihan.

Jenis: String

Pola: `^[0-9]{12}$`

Wajib: Tidak

BackupSizeInBytes

Ukuran, dalam byte, dari sumber daya yang dipulihkan.

Tipe: Panjang

Wajib: Tidak

CompletionDate

Tanggal dan waktu pekerjaan untuk memulihkan titik pemulihan selesai, dalam format Unix dan Waktu Universal Terkoordinasi (UTC). Nilai akurat `CompletionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

CreatedBy

Berisi informasi identifikasi tentang pembuatan pekerjaan pemulihan.

Tipe: Objek RestoreJobCreator

Wajib: Tidak

CreatedResourceArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi sumber daya. Format ARN tergantung pada jenis sumber daya.

Tipe: String

Wajib: Tidak

CreationDate

Tanggal dan waktu pekerjaan pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

DeletionStatus

Ini mencatat status data yang dihasilkan oleh tes pemulihan. Statusnya mungkin`Deleting`,`Failed`, atau`Successful`.

Jenis: String

Nilai yang Valid: `DELETING | FAILED | SUCCESSFUL`

Wajib: Tidak

DeletionStatusMessage

Ini menjelaskan status penghapusan pekerjaan pemulihan.

Tipe: String

Wajib: Tidak

ExpectedCompletionTimeMinutes

Jumlah waktu dalam hitungan menit yang diharapkan diambil oleh pekerjaan memulihkan titik pemulihan.

Tipe: Panjang

Wajib: Tidak

IamRoleArn

Menentukan peran IAM ARN digunakan untuk membuat titik pemulihan target; misalnya,. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Wajib: Tidak

PercentDone

Berisi perkiraan persentase penyelesaian pekerjaan pada saat status pekerjaan ditanyakan.

Tipe: String

Wajib: Tidak

RecoveryPointArn

ARN yang secara unik mengidentifikasi titik pemulihan; misalnya,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipe: String

Wajib: Tidak

RecoveryPointCreationDate

Tanggal di mana titik pemulihan dibuat.

Tipe: Timestamp

Wajib: Tidak

ResourceType

Jenis sumber daya dari pekerjaan pemulihan yang terdaftar; misalnya, volume Amazon Elastic Block Store (Amazon EBS) atau database Amazon Relational Database Service (Amazon RDS). Untuk backup Windows Volume Shadow Copy Service (VSS), satu-satunya jenis sumber daya yang didukung adalah Amazon EC2.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

RestoreJobId

Secara unik mengidentifikasi pekerjaan yang mengembalikan titik pemulihan.

Tipe: String

Wajib: Tidak

Status

Kode status yang menentukan status pekerjaan yang diprakarsai oleh AWS Backup untuk mengembalikan titik pemulihan.

Jenis: String

Nilai yang Valid: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

Wajib: Tidak

StatusMessage

Pesan terperinci yang menjelaskan status pekerjaan untuk memulihkan titik pemulihan.

Tipe: String

Wajib: Tidak

ValidationStatus

Status validasi berjalan pada pekerjaan pemulihan yang ditunjukkan.

Jenis: String

Nilai yang Valid: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Wajib: Tidak

ValidationStatusMessage

Ini menjelaskan status validasi yang dijalankan pada pekerjaan pemulihan yang ditunjukkan.

Tipe: String

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobSummary

Layanan: AWS Backup

Ini adalah ringkasan pekerjaan pemulihan yang dibuat atau berjalan dalam 30 hari terakhir.

Ringkasan yang dikembalikan dapat berisi hal-hal berikut: Wilayah, Akun, Negara Bagian, ResourceType,, MessageCategory, StartTime, EndTime, dan Hitungan pekerjaan yang disertakan.

Daftar Isi

AccountId

ID akun yang memiliki pekerjaan dalam ringkasan.

Jenis: String

Pola: `^[0-9]{12}$`

Wajib: Tidak

Count

Nilai sebagai sejumlah pekerjaan dalam ringkasan pekerjaan.

Tipe: Integer

Wajib: Tidak

EndTime

Nilai waktu dalam format angka waktu akhir pekerjaan.

Nilai ini adalah waktu dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

Region

AWS Wilayah dalam ringkasan pekerjaan.

Tipe: String

Wajib: Tidak

ResourceType

Nilai ini adalah jumlah pekerjaan untuk jenis sumber daya yang ditentukan. Permintaan `GetSupportedResourceTypes` mengembalikan string untuk jenis sumber daya yang didukung.

Jenis: String

Pola: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Wajib: Tidak

StartTime

Nilai waktu dalam format angka waktu mulai pekerjaan.

Nilai ini adalah waktu dalam format Unix, Coordinated Universal Time (UTC), dan akurat hingga milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

State

Nilai ini adalah jumlah pekerjaan untuk pekerjaan dengan status yang ditentukan.

Jenis: String

Nilai yang Valid: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForCreate

Layanan: AWS Backup

Ini berisi metadata tentang rencana pengujian pemulihan.

Daftar Isi

RecoveryPointSelection

`RecoveryPointSelection`memiliki lima parameter (tiga diperlukan dan dua opsional). Nilai yang Anda tentukan menentukan titik pemulihan mana yang termasuk dalam tes pemulihan. Anda harus menunjukkan dengan `Algorithm` apakah Anda menginginkan titik pemulihan terbaru di dalam Anda `SelectionWindowDays` atau jika Anda menginginkan titik pemulihan acak, dan Anda harus menunjukkan melalui `IncludeVaults` brankas mana titik pemulihan dapat dipilih.

`Algorithm`(wajib) Nilai yang valid: "`LATEST_WITHIN_WINDOW`" atau "`RANDOM_WITHIN_WINDOW`".

`Recovery point types`(wajib) Nilai yang valid: "`SNAPSHOT`" dan/atau "`CONTINUOUS`". Sertakan `SNAPSHOT` untuk memulihkan hanya titik pemulihan snapshot; termasuk `CONTINUOUS` untuk memulihkan titik pemulihan berkelanjutan (point in time restore /PITR); gunakan keduanya untuk memulihkan snapshot atau titik pemulihan berkelanjutan. Titik pemulihan akan ditentukan oleh nilai untuk`Algorithm`.

`IncludeVaults`(diperlukan). Anda harus menyertakan satu atau lebih brankas cadangan. Gunakan wildcard ["*"] atau ARN tertentu.

`SelectionWindowDays`(opsional) Nilai harus berupa bilangan bulat (dalam hari) dari 1 hingga 365. Jika tidak disertakan, nilai default ke. `30`

`ExcludeVaults`(opsional). Anda dapat memilih untuk memasukkan satu atau lebih ARN vault cadangan khusus untuk mengecualikan konten vault tersebut dari kelayakan pemulihan. Atau, Anda dapat menyertakan daftar pemilih. Jika parameter ini dan nilainya tidak termasuk, default ke daftar kosong.

Tipe: Objek RestoreTestingRecoveryPointSelection

Wajib: Ya

RestoreTestingPlanName

RestoreTestingPlanName Ini adalah string unik yang merupakan nama dari rencana pengujian pemulihan. Ini tidak dapat diubah setelah pembuatan, dan harus hanya terdiri dari karakter alfanumerik dan garis bawah.

Tipe: String

Diperlukan: Ya

ScheduleExpression

Ekspresi CRON di zona waktu tertentu saat rencana pengujian pemulihan dijalankan.

Tipe: String

Diperlukan: Ya

ScheduleExpressionTimezone

Tidak wajib. Ini adalah zona waktu di mana ekspresi jadwal diatur. Secara default, ScheduleExpressions ada di UTC. Anda dapat memodifikasi ini ke zona waktu tertentu.

Tipe: String

Wajib: Tidak

StartWindowHours

Default hingga 24 jam.

Nilai dalam beberapa jam setelah tes pemulihan dijadwalkan sebelum pekerjaan akan dibatalkan jika tidak berhasil dimulai. Nilai ini bersifat opsional. Jika nilai ini disertakan, parameter ini memiliki nilai maksimum 168 jam (satu minggu).

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForGet

Layanan: AWS Backup

Ini berisi metadata tentang rencana pengujian pemulihan.

Daftar Isi

CreationTime

Tanggal dan waktu rencana pengujian pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Ya

RecoveryPointSelection

Kriteria yang ditentukan untuk menetapkan satu set sumber daya, seperti jenis titik pemulihan atau brankas cadangan.

Tipe: Objek RestoreTestingRecoveryPointSelection

Wajib: Ya

RestoreTestingPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana pengujian pemulihan.

Tipe: String

Diperlukan: Ya

RestoreTestingPlanName

Nama rencana pengujian pemulihan.

Tipe: String

Diperlukan: Ya

ScheduleExpression

Ekspresi CRON di zona waktu tertentu saat rencana pengujian pemulihan dijalankan.

Tipe: String

Diperlukan: Ya

CreatorRequestId

Ini mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Jika permintaan menyertakan `CreatorRequestId` yang cocok dengan rencana cadangan yang ada, paket tersebut dikembalikan. Parameter ini bersifat opsional.

Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

LastExecutionTime

Terakhir kali pengujian pemulihan dijalankan dengan rencana pengujian pemulihan yang ditentukan. Tanggal dan waktu, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastExecutionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

LastUpdateTime

Tanggal dan waktu rencana pengujian pemulihan diperbarui. Pembaruan ini dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastUpdateTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

ScheduleExpressionTimezone

Tidak wajib. Ini adalah zona waktu di mana ekspresi jadwal diatur. Secara default, ScheduleExpressions ada di UTC. Anda dapat memodifikasi ini ke zona waktu tertentu.

Tipe: String

Wajib: Tidak

StartWindowHours

Default hingga 24 jam.

Nilai dalam beberapa jam setelah tes pemulihan dijadwalkan sebelum pekerjaan akan dibatalkan jika tidak berhasil dimulai. Nilai ini bersifat opsional. Jika nilai ini disertakan, parameter ini memiliki nilai maksimum 168 jam (satu minggu).

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForList

Layanan: AWS Backup

Ini berisi metadata tentang rencana pengujian pemulihan.

Daftar Isi

CreationTime

Tanggal dan waktu rencana pengujian pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Ya

RestoreTestingPlanArn

Nama Sumber Daya Amazon (ARN) yang secara unik mengidentifikasi rencana pengujian pemulihan.

Tipe: String

Diperlukan: Ya

RestoreTestingPlanName

Nama rencana pengujian pemulihan.

Tipe: String

Diperlukan: Ya

ScheduleExpression

Ekspresi CRON dalam zona waktu tertentu ketika rencana pengujian pemulihan dijalankan.

Tipe: String

Diperlukan: Ya

LastExecutionTime

Terakhir kali pengujian pemulihan dijalankan dengan rencana pengujian pemulihan yang ditentukan. Tanggal dan waktu, dalam format Unix dan Coordinated Universal Time (UTC). Nilai

akurat `LastExecutionDate` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

LastUpdateTime

Tanggal dan waktu rencana pengujian pemulihan diperbarui. Pembaruan ini dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `LastUpdateTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 2018 12:11:30.087.

Tipe: Timestamp

Wajib: Tidak

ScheduleExpressionTimezone

Tidak wajib. Ini adalah zona waktu di mana ekspresi jadwal diatur. Secara default, ScheduleExpressions ada di UTC. Anda dapat memodifikasi ini ke zona waktu tertentu.

Tipe: String

Wajib: Tidak

StartWindowHours

Default hingga 24 jam.

Nilai dalam beberapa jam setelah tes pemulihan dijadwalkan sebelum pekerjaan akan dibatalkan jika tidak berhasil dimulai. Nilai ini bersifat opsional. Jika nilai ini disertakan, parameter ini memiliki nilai maksimum 168 jam (satu minggu).

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForUpdate

Layanan: AWS Backup

Ini berisi metadata tentang rencana pengujian pemulihan.

Daftar Isi

RecoveryPointSelection

Diperlukan: `AlgorithmRecoveryPointTypes`;; `IncludeVaults` (satu atau lebih).

Opsional: SelectionWindowDays('30' jika tidak ditentukan); `ExcludeVaults` (default ke daftar kosong jika tidak terdaftar).

Tipe: Objek RestoreTestingRecoveryPointSelection

Wajib: Tidak

ScheduleExpression

Ekspresi CRON dalam zona waktu tertentu ketika rencana pengujian pemulihan dijalankan.

Tipe: String

Wajib: Tidak

ScheduleExpressionTimezone

Tidak wajib. Ini adalah zona waktu di mana ekspresi jadwal diatur. Secara default, ScheduleExpressions ada di UTC. Anda dapat memodifikasi ini ke zona waktu tertentu.

Tipe: String

Wajib: Tidak

StartWindowHours

Default hingga 24 jam.

Nilai dalam beberapa jam setelah tes pemulihan dijadwalkan sebelum pekerjaan akan dibatalkan jika tidak berhasil dimulai. Nilai ini bersifat opsional. Jika nilai ini disertakan, parameter ini memiliki nilai maksimum 168 jam (satu minggu).

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingRecoveryPointSelection

Layanan: AWS Backup

`RecoveryPointSelection`memiliki lima parameter (tiga diperlukan dan dua opsional). Nilai yang Anda tentukan menentukan titik pemulihan mana yang termasuk dalam tes pemulihan. Anda harus menunjukkan dengan `Algorithm` apakah Anda menginginkan titik pemulihan terbaru di dalam Anda `SelectionWindowDays` atau jika Anda menginginkan titik pemulihan acak, dan Anda harus menunjukkan melalui `IncludeVaults` brankas mana titik pemulihan dapat dipilih.

`Algorithm`(wajib) Nilai yang valid: "`LATEST_WITHIN_WINDOW`" atau "`RANDOM_WITHIN_WINDOW`".

`Recovery point types`(wajib) Nilai yang valid: "`SNAPSHOT`" dan/atau "`CONTINUOUS`". Sertakan `SNAPSHOT` untuk memulihkan hanya titik pemulihan snapshot; termasuk `CONTINUOUS` untuk memulihkan titik pemulihan berkelanjutan (point in time restore /PITR); gunakan keduanya untuk memulihkan snapshot atau titik pemulihan berkelanjutan. Titik pemulihan akan ditentukan oleh nilai untuk`Algorithm`.

`IncludeVaults`(diperlukan). Anda harus menyertakan satu atau lebih brankas cadangan. Gunakan wildcard ["*"] atau ARN tertentu.

`SelectionWindowDays`(opsional) Nilai harus berupa bilangan bulat (dalam hari) dari 1 hingga 365. Jika tidak disertakan, nilai defaultnya. `30`

`ExcludeVaults`(opsional). Anda dapat memilih untuk memasukkan satu atau lebih ARN vault cadangan khusus untuk mengecualikan konten vault tersebut dari kelayakan pemulihan. Atau, Anda dapat menyertakan daftar pemilih. Jika parameter ini dan nilainya tidak termasuk, default ke daftar kosong.

Daftar Isi

Algorithm

Nilai yang dapat diterima termasuk “LATEST_WITHIN_WINDOW” atau “RANDOM_WITHIN_WINDOW”

Jenis: String

Nilai yang Valid: `LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW`

Wajib: Tidak

ExcludeVaults

Nilai yang diterima termasuk ARN tertentu atau daftar pemilih. Default ke daftar kosong jika tidak terdaftar.

Tipe: Array string

Wajib: Tidak

IncludeVaults

Nilai yang diterima termasuk wildcard ["*"] atau dengan ARN tertentu atau penggantian wilcard ARN ["arn:aws:backup: us-west- 2:123456789012: backup-vault: asdf",...] ["arn:aws:backup: *:*:backup-vault:asdf-*",...]

Tipe: Array string

Wajib: Tidak

RecoveryPointTypes

Ini adalah jenis titik pemulihan.

Sertakan `SNAPSHOT` untuk memulihkan hanya titik pemulihan snapshot; termasuk `CONTINUOUS` untuk memulihkan titik pemulihan berkelanjutan (point in time restore /PITR); gunakan keduanya untuk memulihkan snapshot atau titik pemulihan berkelanjutan. Titik pemulihan akan ditentukan oleh nilai untuk`Algorithm`.

Tipe: Array string

Nilai yang Valid: `CONTINUOUS | SNAPSHOT`

Wajib: Tidak

SelectionWindowDays

Nilai yang diterima adalah bilangan bulat dari 1 hingga 365.

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForCreate

Layanan: AWS Backup

Ini berisi metadata tentang pilihan pengujian pemulihan tertentu.

ProtectedResourceType diperlukan, seperti Amazon EBS atau Amazon EC2.

Ini terdiri dari`RestoreTestingSelectionName`,`ProtectedResourceType`, dan salah satu dari yang berikut:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Setiap jenis sumber daya yang dilindungi dapat memiliki satu nilai tunggal.

Pilihan pengujian pemulihan dapat menyertakan nilai wildcard (“*”) untuk `ProtectedResourceArns` bersama dengan`ProtectedResourceConditions`. Atau, Anda dapat menyertakan hingga 30 ARN sumber daya terlindungi tertentu di`ProtectedResourceArns`.

`ProtectedResourceConditions`Contohnya termasuk sebagai `StringEquals` dan`StringNotEquals`.

Daftar Isi

IamRoleArn

Nama Sumber Daya Amazon (ARN) dari peran IAM yang AWS Backup digunakan untuk membuat sumber daya target; misalnya:. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Diperlukan: Ya

ProtectedResourceType

Jenis AWS sumber daya yang disertakan dalam pilihan pengujian pemulihan; misalnya, volume Amazon EBS atau database Amazon RDS.

Jenis sumber daya yang didukung diterima meliputi:

- `Aurora`untuk Amazon Aurora
- `DocumentDB`untuk Amazon DocumentDB (dengan kompatibilitas MongoDB)

- `DynamoDB`untuk Amazon DynamoDB
- `EBS`untuk Amazon Elastic Block Store
- `EC2`untuk Amazon Elastic Compute Cloud
- `EFS`untuk Amazon Elastic File System
- `FSx`untuk Amazon FSx
- `Neptune`untuk Amazon Neptunus
- `RDS`untuk Amazon Relational Database Service
- `S3` untuk Amazon S3

Tipe: String

Diperlukan: Ya

RestoreTestingSelectionName

Nama unik dari pilihan pengujian pemulihan yang termasuk dalam rencana pengujian pemulihan terkait.

Tipe: String

Diperlukan: Ya

ProtectedResourceArns

Setiap sumber daya yang dilindungi dapat difilter oleh ARN spesifiknya, seperti `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` atau oleh wildcard:`ProtectedResourceArns: ["*"]`, tetapi tidak keduanya.

Tipe: Array string

Wajib: Tidak

ProtectedResourceConditions

Jika Anda telah menyertakan wildcard ProtectedResourceArns, Anda dapat menyertakan kondisi sumber daya, seperti`ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]`.

Tipe: Objek ProtectedResourceConditions

Wajib: Tidak

RestoreMetadataOverrides

Anda dapat mengganti kunci metadata pemulihan tertentu dengan memasukkan parameter `RestoreMetadataOverrides` di badan. `RestoreTestingSelection` Nilai kunci tidak peka huruf besar/kecil.

Lihat daftar lengkap metadata yang disimpulkan dari pengujian pemulihan.

Tipe: Peta antar string

Wajib: Tidak

ValidationWindowHours

Ini adalah jumlah jam (1 hingga 168) yang tersedia untuk menjalankan skrip validasi pada data. Data akan dihapus setelah selesainya skrip validasi atau akhir periode retensi yang ditentukan, mana yang lebih dulu.

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForGet

Layanan: AWS Backup

Ini berisi metadata tentang pilihan pengujian pemulihan.

Daftar Isi

CreationTime

Tanggal dan waktu pemilihan pengujian pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili Jumat, 26 Januari 201812:11:30.087 AM.

Tipe: Timestamp

Wajib: Ya

IamRoleArn

Nama Sumber Daya Amazon (ARN) dari peran IAM yang AWS Backup digunakan untuk membuat sumber daya target; misalnya:. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Diperlukan: Ya

ProtectedResourceType

Jenis AWS sumber daya yang disertakan dalam pemilihan pengujian sumber daya; misalnya, volume Amazon EBS atau database Amazon RDS.

Tipe: String

Diperlukan: Ya

RestoreTestingPlanName

RestoreTestingPlanName Ini adalah string unik yang merupakan nama dari rencana pengujian pemulihan.

Tipe: String

Diperlukan: Ya

RestoreTestingSelectionName

Nama unik dari pilihan pengujian pemulihan yang termasuk dalam rencana pengujian pemulihan terkait.

Tipe: String

Diperlukan: Ya

CreatorRequestId

Ini mengidentifikasi permintaan dan memungkinkan permintaan yang gagal untuk dicoba ulang tanpa risiko menjalankan operasi dua kali. Jika permintaan menyertakan `CreatorRequestId` yang cocok dengan rencana cadangan yang ada, paket tersebut dikembalikan. Parameter ini bersifat opsional.

Jika digunakan, parameter ini harus berisi 1 sampai 50 alfanumerik atau '-_.' karakter.

Tipe: String

Wajib: Tidak

ProtectedResourceArns

Anda dapat menyertakan ARN tertentu, seperti `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` atau Anda dapat menyertakan wildcard:`ProtectedResourceArns: ["*"]`, tetapi tidak keduanya.

Tipe: Array string

Wajib: Tidak

ProtectedResourceConditions

Dalam pemilihan pengujian sumber daya, parameter ini menyaring berdasarkan kondisi tertentu seperti `StringEquals` atau`StringNotEquals`.

Tipe: Objek ProtectedResourceConditions

Wajib: Tidak

RestoreMetadataOverrides

Anda dapat mengganti kunci metadata pemulihan tertentu dengan memasukkan parameter `RestoreMetadataOverrides` di badan. `RestoreTestingSelection` Nilai kunci tidak peka huruf besar/kecil.

Lihat daftar lengkap metadata yang disimpulkan dari pengujian pemulihan.

Tipe: Peta antar string

Wajib: Tidak

ValidationWindowHours

Ini adalah jumlah jam (1 hingga 168) yang tersedia untuk menjalankan skrip validasi pada data. Data akan dihapus setelah selesainya skrip validasi atau akhir periode retensi yang ditentukan, mana yang lebih dulu.

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForList

Layanan: AWS Backup

Ini berisi metadata tentang pilihan pengujian pemulihan.

Daftar Isi

CreationTime

Tanggal dan waktu pemilihan pengujian pemulihan dibuat, dalam format Unix dan Coordinated Universal Time (UTC). Nilai akurat `CreationTime` untuk milidetik. Misalnya, nilai 1516925490.087 mewakili hari Jumat, 26 Januari 2018 12:11:30,087.

Tipe: Timestamp

Wajib: Ya

IamRoleArn

Nama Sumber Daya Amazon (ARN) dari peran IAM yang AWS Backup digunakan untuk membuat sumber daya target; misalnya:. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Diperlukan: Ya

ProtectedResourceType

Jenis AWS sumber daya yang disertakan dalam pilihan pengujian pemulihan; misalnya, volume Amazon EBS atau database Amazon RDS.

Tipe: String

Diperlukan: Ya

RestoreTestingPlanName

String unik yang merupakan nama dari rencana pengujian pemulihan.

Nama tidak dapat diubah setelah penciptaan. Nama harus terdiri dari hanya karakter alfanumerik dan garis bawah. Panjang maksimum adalah 50.

Tipe: String

Diperlukan: Ya

RestoreTestingSelectionName

Nama unik dari pilihan pengujian pemulihan.

Tipe: String

Diperlukan: Ya

ValidationWindowHours

Nilai ini mewakili waktu, dalam jam, data dipertahankan setelah tes pemulihan sehingga validasi opsional dapat diselesaikan.

Nilai yang diterima adalah bilangan bulat antara 0 dan 168 (setara per jam tujuh hari).

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForUpdate

Layanan: AWS Backup

Ini berisi metadata tentang pilihan pengujian pemulihan.

Daftar Isi

IamRoleArn

Nama Sumber Daya Amazon (ARN) dari peran IAM yang AWS Backup digunakan untuk membuat sumber daya target; misalnya:. `arn:aws:iam::123456789012:role/S3Access`

Tipe: String

Wajib: Tidak

ProtectedResourceArns

Anda dapat menyertakan daftar ARN tertentu, seperti `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` atau Anda dapat menyertakan wildcard:`ProtectedResourceArns: ["*"]`, tetapi tidak keduanya.

Tipe: Array string

Wajib: Tidak

ProtectedResourceConditions

Kondisi yang Anda tentukan untuk sumber daya dalam rencana pengujian pemulihan menggunakan tag.

Misalnya, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Operator kondisi peka huruf besar/kecil.

Tipe: Objek ProtectedResourceConditions

Wajib: Tidak

RestoreMetadataOverrides

Anda dapat mengganti kunci metadata pemulihan tertentu dengan memasukkan parameter `RestoreMetadataOverrides` di badan. `RestoreTestingSelection` Nilai kunci tidak peka huruf besar/kecil.

Lihat daftar lengkap metadata yang disimpulkan dari pengujian pemulihan.

Tipe: Peta antar string

Wajib: Tidak

ValidationWindowHours

Nilai ini mewakili waktu, dalam jam, data dipertahankan setelah tes pemulihan sehingga validasi opsional dapat diselesaikan.

Nilai yang diterima adalah bilangan bulat antara 0 dan 168 (setara per jam tujuh hari).

Tipe: Integer

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AWS Backup gateway

tipe data berikut didukungAWS Backup gateway:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine

- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

Layanan: AWS Backup gateway

Menjelaskan interval batas laju bandwidth untuk gateway. Jadwal batas tingkat bandwidth terdiri dari satu atau lebih interval batas laju bandwidth. Interval batas tingkat bandwidth mendefinisikan periode waktu pada satu hari atau lebih dalam seminggu, di mana batas tingkat bandwidth ditentukan untuk mengunggah, mengunduh, atau keduanya.

Daftar Isi

DaysOfWeek

Komponen hari dalam seminggu dari interval batas laju bandwidth, direpresentasikan sebagai angka urut dari 0 hingga 6, di mana 0 mewakili hari Minggu dan 6 mewakili hari Sabtu.

Tipe: Array bilangan bulat

Anggota Array: Jumlah minimum 1 item. Jumlah maksimum 7 item.

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 6.

Wajib: Ya

EndHourOfDay

Jam dalam sehari untuk mengakhiri interval batas laju bandwidth.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 23.

Wajib: Ya

EndMinuteOfHour

Menit jam untuk mengakhiri interval batas laju bandwidth.

> **Important**
>
> Interval batas laju bandwidth berakhir pada akhir menit. Untuk mengakhiri interval pada akhir jam, gunakan nilainya`59`.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 59.

Wajib: Ya

StartHourOfDay

Jam dalam sehari untuk memulai interval batas laju bandwidth.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 23.

Wajib: Ya

StartMinuteOfHour

Menit jam untuk memulai interval batas laju bandwidth. Interval dimulai pada awal menit itu. Untuk memulai interval tepat di awal jam, gunakan nilainya`0`.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 59.

Wajib: Ya

AverageUploadRateLimitInBitsPerSec

Komponen batas kecepatan unggah rata-rata dari interval batas laju bandwidth, dalam bit per detik. Bidang ini tidak muncul dalam respons jika batas kecepatan unggahan tidak ditetapkan.

Tipe: Long

Rentang Valid: Nilai minimum 51200. Nilai maksimum 8000000000000.

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Gateway

Layanan: AWS Backup gateway

Gateway adalah alat AWS Backup Gateway yang berjalan di jaringan pelanggan untuk menyediakan konektivitas tanpa batas ke penyimpanan cadangan di AWS Cloud.

Daftar Isi

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway. Gunakan `ListGateways` operasi untuk mengembalikan daftar gateway untuk akun Anda dan. Wilayah AWS

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Tidak

GatewayDisplayName

Nama tampilan gateway.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

GatewayType

Jenis gateway.

Jenis: String

Nilai yang Valid: `BACKUP_VM`

Wajib: Tidak

HypervisorId

ID hypervisor dari gateway.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Wajib: Tidak

LastSeenTime

AWS Backup Gateway terakhir kali berkomunikasi dengan gateway, dalam format Unix dan waktu UTC.

Tipe: Timestamp

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

GatewayDetails

Layanan: AWS Backup gateway

Rincian gateway.

Daftar Isi

GatewayArn

Nama Sumber Daya Amazon (ARN) dari gateway. Gunakan `ListGateways` operasi untuk mengembalikan daftar gateway untuk akun Anda dan. Wilayah AWS

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 180.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Tidak

GatewayDisplayName

Nama tampilan gateway.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

GatewayType

Jenis tipe gateway.

Jenis: String

Nilai yang Valid: `BACKUP_VM`

Wajib: Tidak

HypervisorId

ID hypervisor dari gateway.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Wajib: Tidak

LastSeenTime

Detail yang menunjukkan AWS Backup gateway terakhir kali dikomunikasikan dengan cloud, dalam format Unix dan waktu UTC.

Tipe: Timestamp

Wajib: Tidak

MaintenanceStartTime

Mengembalikan waktu mulai pemeliharaan mingguan gateway Anda termasuk hari dan waktu dalam seminggu. Perhatikan bahwa nilai dalam hal zona waktu gateway. Bisa mingguan atau bulanan.

Tipe: Objek MaintenanceStartTime

Wajib: Tidak

NextUpdateAvailabilityTime

Detail yang menunjukkan waktu ketersediaan pembaruan gateway berikutnya.

Tipe: Timestamp

Wajib: Tidak

VpcEndpoint

Nama DNS untuk titik akhir virtual private cloud (VPC) yang digunakan gateway untuk terhubung ke cloud untuk gateway cadangan.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum sebesar 255.

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Hypervisor

Layanan: AWS Backup gateway

Merupakan izin hypervisor yang akan terhubung dengan gateway.

Hypervisor adalah perangkat keras, perangkat lunak, atau firmware yang membuat dan mengelola mesin virtual, dan mengalokasikan sumber daya untuk mereka.

Daftar Isi

Host

Host server hypervisor. Ini bisa berupa alamat IP atau nama domain yang sepenuhnya memenuhi syarat (FQDN).

Jenis: String

Batasan Panjang: Panjang minimum 3. Panjang maksimum 128.

Pola: `^.+$`

Wajib: Tidak

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Tidak

KmsKeyArn

Nama Sumber Daya Amazon (ARN) yang AWS Key Management Service digunakan untuk mengenkripsi hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Wajib: Tidak

Name

Nama hypervisor.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

State

Keadaan hypervisor.

Jenis: String

Nilai yang Valid: `PENDING | ONLINE | OFFLINE | ERROR`

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

HypervisorDetails

Layanan: AWS Backup gateway

Ini adalah detail dari hypervisor yang ditentukan. Hypervisor adalah perangkat keras, perangkat lunak, atau firmware yang membuat dan mengelola mesin virtual, dan mengalokasikan sumber daya untuk mereka.

Daftar Isi

Host

Host server hypervisor. Ini bisa berupa alamat IP atau nama domain yang sepenuhnya memenuhi syarat (FQDN).

Jenis: String

Batasan Panjang: Panjang minimum 3. Panjang maksimum 128.

Pola: `^.+$`

Wajib: Tidak

HypervisorArn

Nama Sumber Daya Amazon (ARN) dari hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Tidak

KmsKeyArn

Nama Sumber Daya Amazon (ARN) yang AWS KMS digunakan untuk mengenkripsi hypervisor.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Wajib: Tidak

LastSuccessfulMetadataSyncTime

Ini adalah waktu ketika sinkronisasi metadata sukses terbaru terjadi.

Tipe: Timestamp

Wajib: Tidak

LatestMetadataSyncStatus

Ini adalah status terbaru untuk sinkronisasi metadata yang ditunjukkan.

Jenis: String

Nilai yang Valid: `CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED`

Wajib: Tidak

LatestMetadataSyncStatusMessage

Ini adalah status terbaru untuk sinkronisasi metadata yang ditunjukkan.

Tipe: String

Wajib: Tidak

LogGroupArn

Nama Sumber Daya Amazon (ARN) dari grup gateway dalam log yang diminta.

Jenis: String

Batasan Panjang: Panjang minimum sebesar 0. Panjang maksimum 2048.

Pola: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Wajib: Tidak

Name

Ini adalah nama hypervisor yang ditentukan.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

State

Ini adalah keadaan hypervisor yang ditentukan saat ini.

Negara-negara yang mungkin adalah `PENDINGONLINE`,`OFFLINE`,, atau`ERROR`.

Jenis: String

Nilai yang Valid: `PENDING | ONLINE | OFFLINE | ERROR`

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MaintenanceStartTime

Layanan: AWS Backup gateway

Ini adalah waktu mulai pemeliharaan mingguan gateway Anda termasuk hari dan waktu dalam seminggu. Perhatikan bahwa nilai dalam hal zona waktu gateway. Bisa mingguan atau bulanan.

Daftar Isi

HourOfDay

Komponen jam dari waktu mulai pemeliharaan direpresentasikan sebagai hh, di mana hh adalah jam (0 hingga 23). Jam dalam sehari berada di zona waktu gerbang.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 23.

Wajib: Ya

MinuteOfHour

Komponen menit dari waktu mulai pemeliharaan direpresentasikan sebagai mm, di mana mm adalah menit (0 hingga 59). Menit jam berada di zona waktu gerbang.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 59.

Wajib: Ya

DayOfMonth

Komponen hari bulan dari waktu mulai pemeliharaan direpresentasikan sebagai nomor urut dari 1 hingga 28, di mana 1 mewakili hari pertama bulan itu dan 28 mewakili hari terakhir bulan tersebut.

Jenis: Integer

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 31.

Wajib: Tidak

DayOfWeek

Nomor urut antara 0 dan 6 yang mewakili hari dalam seminggu, di mana 0 mewakili hari Minggu dan 6 mewakili hari Sabtu. Hari dalam seminggu berada di zona waktu gateway.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 0. Nilai maksimum 6.

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

Layanan: AWS Backup gateway

Pasangan nilai kunci yang dapat Anda gunakan untuk mengelola, memfilter, dan mencari sumber daya Anda. Karakter yang diizinkan termasuk huruf UTF-8, angka, spasi, dan karakter berikut: + - =. _: /.

Daftar Isi

Key

Bagian kunci dari pasangan nilai kunci tag. Kunci tidak dapat diawali dengan `aws:`.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 128.

Pola: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Wajib: Ya

Value

Bagian nilai dari pasangan nilai kunci tag.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 256.

Pola: `^[^\x00]*$`

Diperlukan: Ya

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VirtualMachine

Layanan: AWS Backup gateway

Mesin virtual yang ada di hypervisor.

Daftar Isi

HostName

Nama host dari mesin virtual.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

HypervisorId

ID hypervisor mesin virtual.

Tipe: String

Wajib: Tidak

LastBackupDate

Tanggal terbaru mesin virtual dicadangkan, dalam format Unix dan waktu UTC.

Tipe: Timestamp

Wajib: Tidak

Name

Nama mesin virtual.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

Path

Jalur mesin virtual.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 4096.

Pola: `^[^\x00]+$`

Wajib: Tidak

ResourceArn

Nama Sumber Daya Amazon (ARN) dari mesin virtual. Sebagai contoh, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Diperlukan: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VirtualMachineDetails

Layanan: AWS Backup gateway

`VirtualMachine`Objek Anda, diurutkan berdasarkan Nama Sumber Daya Amazon (ARN) mereka.

Daftar Isi

HostName

Nama host dari mesin virtual.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

HypervisorId

ID hypervisor mesin virtual.

Tipe: String

Wajib: Tidak

LastBackupDate

Tanggal terbaru mesin virtual dicadangkan, dalam format Unix dan waktu UTC.

Tipe: Timestamp

Wajib: Tidak

Name

Nama mesin virtual.

Jenis: String

Panjang Batasan: Panjang minimum 1. Panjang maksimum 100.

Pola: `^[a-zA-Z0-9-]*$`

Wajib: Tidak

Path

Jalur mesin virtual.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 4096.

Pola: `^[^\x00]+$`

Wajib: Tidak

ResourceArn

Nama Sumber Daya Amazon (ARN) dari mesin virtual. Sebagai contoh, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Jenis: String

Kendala Panjang: Panjang minimum 50. Panjang maksimum 500.

Pola: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Wajib: Tidak

VmwareTags

Ini adalah rincian tag VMware yang terkait dengan mesin virtual yang ditentukan.

Tipe: Array objek VmwareTag

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VmwareTag

Layanan: AWS Backup gateway

Tag VMware adalah tag yang dilampirkan ke mesin virtual tertentu. Tag adalah pasangan kunci-nilai yang dapat Anda gunakan untuk mengelola, memfilter, dan mencari sumber daya Anda.

Isi tag VMware dapat dicocokkan dengan tag. AWS

Daftar Isi

VmwareCategory

Ini adalah kategori VMware.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 80.

Wajib: Tidak

VmwareTagDescription

Ini adalah deskripsi yang ditentukan pengguna dari tag VMware.

Tipe: String

Wajib: Tidak

VmwareTagName

Ini adalah nama yang ditentukan pengguna dari tag VMware.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 80.

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

VmwareToAwsTagMapping

Layanan: AWS Backup gateway

Ini menampilkan pemetaan tag VMware ke tag yang sesuai. AWS

Daftar Isi

AwsTagKey

Bagian kunci dari pasangan nilai kunci AWS tag.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 128.

Pola: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Wajib: Ya

AwsTagValue

Bagian nilai dari pasangan nilai kunci AWS tag.

Jenis: String

Batasan Panjang: Panjang minimum 0. Panjang maksimum 256.

Pola: `^[^\x00]*$`

Wajib: Ya

VmwareCategory

Ini adalah kategori VMware.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 80.

Wajib: Ya

VmwareTagName

Ini adalah nama yang ditentukan pengguna dari tag VMware.

Jenis: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 80.

Wajib: Ya

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu AWS SDK khusus bahasa, lihat berikut ini:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Parameter Umum

Daftar berikut berisi parameter yang digunakan semua tindakan untuk menandatangani permintaan Tanda Tangan Versi 4 dengan string kueri. Setiap parameter khusus tindakan tercantum dalam topik untuk tindakan tersebut. Untuk informasi selengkapnya tentang Signature Versi 4, lihat Menandatangani permintaanAWS API di Panduan Pengguna IAM.

Action

Tindakan yang harus dilakukan.

Tipe: string

Wajib: Ya

Version

Versi API yang ditulis dalam permintaan, dinyatakan dalam format HH-BB-TTTT.

Tipe: string

Wajib: Ya

X-Amz-Algorithm

Algoritme hash yang Anda gunakan untuk membuat tanda tangan permintaan.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Nilai yang Valid: `AWS4-HMAC-SHA256`

Diperlukan: Kondisional

X-Amz-Credential

Nilai lingkup kredensial, yang merupakan string yang menyertakan access key Anda, tanggal, wilayah yang Anda targetkan, layanan yang Anda minta, dan string penghentian ("aws4_request"). Nilai dinyatakan dalam format berikut: access_key/HHBBTTTT/wilayah/layanan/aws4_request.

Untuk informasi selengkapnya, lihat Membuat permintaanAWS API yang ditandatangani di Panduan Pengguna IAM.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Diperlukan: Kondisional

X-Amz-Date

Tanggal yang digunakan untuk membuat tanda tangan. Format harus berupa format dasar ISO 8601 (YYYYMMDD'T'HMMSS'Z'). Misalnya, waktu tanggal berikut adalah nilai X-Amz-Date yang valid: `20120325T120000Z`.

Syarat: X-Amz-Date bersifat opsional untuk semua permintaan; nilai ini dapat digunakan untuk mengganti tanggal yang digunakan untuk menandatangani permintaan. Jika header Tanggal ditentukan dalam format dasar ISO 8601, X-Amz-Date tidak diperlukan. Ketika X-Amz-Date digunakan, ia selalu mengganti nilai header Tanggal. Untuk informasi selengkapnya, lihat Elemen tanda tangan permintaanAWS API di Panduan Pengguna IAM.

Tipe: string

Diperlukan: Kondisional

X-Amz-Security-Token

Token keamanan sementara yang diperoleh melalui panggilan keAWS Security Token Service (AWS STS). Untuk daftar layanan yang mendukung kredensi keamanan sementara dariAWS STS, lihat Layanan AWSbahwa bekerja dengan IAM dalam Panduan Pengguna IAM.

Syarat: Jika Anda menggunakan kredensi keamanan sementara dariAWS STS, Anda harus menyertakan token keamanan.

Tipe: string

Diperlukan: Kondisional

X-Amz-Signature

Menentukan tanda tangan yang dikodekan oleh hex yang dihitung dari string to sign dan kunci penandatanganan turunan.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Diperlukan: Kondisional

X-Amz-SignedHeaders

Menentukan semua header HTTP yang disertakan sebagai bagian dari permintaan kanonik. Untuk informasi selengkapnya tentang menentukan header yang ditandatangani, lihat Membuat permintaanAWS API yang ditandatangani di Panduan Pengguna IAM.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Diperlukan: Kondisional

Kesalahan Umum

Bagian ini berisi daftar kesalahan yang umum terjadi pada tindakan API dari semua layanan AWS. Untuk kesalahan khusus pada tindakan API untuk layanan ini, lihat topik untuk tindakan API tersebut.

AccessDeniedException

Anda tidak memiliki akses yang memadai untuk melakukan tindakan ini.

Kode Status HTTP: 400

IncompleteSignature

Tanda tangan permintaan tidak sesuai dengan standar AWS.

Kode Status HTTP: 400

InternalFailure

Pemrosesan permintaan telah gagal karena kesalahan yang tidak diketahui, pengecualian atau kegagalan.

Kode Status HTTP: 500

InvalidAction

Tindakan atau operasi yang diminta tidak valid. Verifikasi bahwa tindakan diketik dengan benar.

Kode Status HTTP: 400

InvalidClientTokenId

Sertifikat X.509 atau access key ID AWS yang diberikan tidak ada dalam catatan kami.

Kode Status HTTP: 403

NotAuthorized

Anda tidak memiliki izin untuk melakukan tindakan ini.

Kode Status HTTP: 400

OptInRequired

Access key ID AWS membutuhkan berlangganan untuk layanan.

Kode Status HTTP: 403

RequestExpired

Permintaan menjangkau layanan lebih dari 15 menit setelah stempel tanggal pada permintaan atau lebih dari 15 menit setelah tanggal kedaluwarsa permintaan (seperti untuk URL pre-signed), atau stempel tanggal pada permintaan lebih dari 15 menit di masa mendatang.

Kode Status HTTP: 400

ServiceUnavailable

Permintaan telah gagal karena kegagalan sementara server.

Kode Status HTTP: 503

ThrottlingException

Permintaan ditolak karena throttling permintaan.

Kode Status HTTP: 400

ValidationError

Input gagal untuk memenuhi batasan yang ditentukan oleh layanan AWS.

Kode Status HTTP: 400

Riwayat dokumen untuk AWS Backup

- Versi API: 6 Desember 2023
- Pembaruan dokumentasi terbaru: 3 Juni 2024

Tabel berikut mencantumkan semua AWS Backup peluncuran sejak peluncuran layanan pada Januari 2019 hingga sekarang. Untuk pemberitahuan tentang pembaruan dokumentasi ini, Anda dapat berlangganan umpan RSS di atas.

Perubahan	Deskripsi	Tanggal
AWS Backup fitur Ekspansi regional	AWS Backup dukungan tingkat arsip snapshot Amazon EBS sekarang tersedia di Wilayah berikut: • China (Beijing) • China (Ningxia) • AWS GovCloud (AS-Barat) • AWS GovCloud (AS-Timur)	3 Juni 2024
Kebijakan AWS terkelola yang diperbarui	AWS Backup menambahkan izin `backup:TagResource` ke kebijakan terkelola berikut: • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup Untuk informasi selengkapnya, lihat Pembaruan kebijakan.	17 Mei 2024

Perubahan	Deskripsi	Tanggal
AWS Backup sekarang tersedia di Canada West (Calgary) Region	Backup dan restore untuk banyak jenis sumber daya sekarang tersedia di Wilayah AWS Canada West (Calgary). Untuk fitur pencadangan yang kompatibel, lihat Ketersediaan fitur menurut Wilayah AWS. Untuk jenis sumber daya yang didukung, lihat Layanan yang didukung oleh Wilayah AWS.	Maret 14, 2024
Menambahkan izin ke kebijakan terkelola	AWS Backup memperbarui kebijakan AWSServiceRolePolicyForBackupRestoreTestingdengan menambahkan izin untuk mendukung jenis sumber daya tambahan dalam fitur pengujian pemulihan. Untuk informasi selengkapnya tentang izin tertentu yang ditambahkan, lihat Pembaruan kebijakan.	Februari 14, 2024
Cadangkan dan pulihkan dukungan untuk FSx untuk volume ONTAP FlexGroup	AWS Backup sekarang mendukung pencadangan dan pemulihan FSx untuk FlexGroup volume ONTAP di sebagian besar. Wilayah AWS Untuk informasi selengkapnya, lihat Memulihkan sistem file Amazon FSx .	10 Januari 2024

Perubahan	Deskripsi	Tanggal
Support untuk backup dan restore SAP HANA HA	AWS Backup sekarang menawarkan dukungan SAP HANA database Ketersediaan Tinggi di Amazon EC2 backup dan restore. Untuk informasi selengkapnya, lihat SAP HANA di Amazon EC2 backup dan Restoring a SAP HANA High Availability system	21 Desember 2023
AWS Backup Kontrol Audit Manager untuk pengujian pemulihan	AWS Backup Audit Manager sekarang menawarkan waktu Pemulihan kontrol untuk sumber daya yang memenuhi target untuk membantu memantau waktu pemulihan. Kontrol ini memeriksa apakah waktu pemulihan sumber daya memenuhi durasi target. Untuk informasi selengkapnya, lihat Kontrol dan remediasi dan Pengujian pemulihan audit.	18 Desember 2023

Perubahan	Deskripsi	Tanggal
Support untuk penyimpanan dingin Amazon EBS	AWS Backup sekarang mendukung transisi cadangan EBS dari penyimpanan hangat ke penyimpanan dingin. Untuk informasi selengkapnya, silakan lihat • Tingkat Arsip Amazon EBS untuk penyimpanan dingin • Siklus hidup dan tingkatan penyimpanan • Membuat rencana cadangan	27 November 2023
Memperkenalkan pengujian pemulihan	AWS Backup memperken alkan pengujian pemulihan , yang membawa evaluasi kelayakan pemulihan secara otomatis dan berkala, serta kemampuan untuk memantau waktu durasi pekerjaan pemulihan. Untuk informasi selengkap nya, lihat Mengembalikan pengujian.	27 November 2023

Perubahan	Deskripsi	Tanggal
Kebijakan AWS terkelola yang diperbarui	AWS Backup menambahkan izin `ec2:DescribeSnapshotTierStatus` dan kebijakan `ec2:ModifySnapshotTier` terkelola `AWSBackupServiceRolePolicyForBackups` dan`AWSBackupServiceLinkedRolePolicyForBackup` . AWS Backup juga menambahkan izin `ec2:DescribeSnapshotTierStatus` dan kebijakan `ec2:RestoreSnapshotTier` `AWSBackupServiceRolePolicyForRestores` terkelola. Izin ini diperlukan bagi pengguna untuk memiliki opsi untuk mentransisikan sumber daya Amazon EBS yang disimpan AWS Backup ke penyimpanan arsip dan memulihkan sumber daya dari tingkat penyimpanan arsip. Untuk informasi selengkapnya, lihat Pembaruan kebijakan.	27 November 2023

Perubahan	Deskripsi	Tanggal
Menambahkan izin peran lulus untuk mendukung pengujian pemulihan.	AWS Backup ditambahkan `restore-testing.backup.amazonaws.com` ke `IamPassRolePermissions` dan `IamCreateServiceLinkedRolePermissions`. Penambahan ini diperlukan AWS Backup untuk melakukan tes pemulihan atas nama pelanggan.	27 November 2023

Perubahan	Deskripsi	Tanggal
Menambahkan peran terkait layanan baru	AWS Backup telah menambahkan peran terkait layanan baru bernama `AWSServiceRoleForBackupRestoreTesting`, yang menyediakan izin cadangan untuk melakukan pengujian pemulihan. Peran terkait layanan baru ini menyediakan izin AWS Backup yang diperlukan untuk melakukan pengujian pemulihan. Izin termasuk tindakan `list, read, and write` untuk layanan berikut yang akan disertakan dalam tes pemulihan: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx for Lustre, fsX untuk Windows File Server, fsX untuk ONTAP, FSx untuk OpenZx FS, Amazon Neptunus, Amazon RDS, dan Amazon S3.	27 November 2023

Perubahan	Deskripsi	Tanggal
Dasbor metrik pekerjaan baru di AWS Backup konsol	AWS Backup Konsol sekarang menampilkan dasbor pekerjaan, menyederhanakan pemantauan kesehatan cadangan dalam skala besar dengan antarmuka pengguna visual baru dan metrik pencadangan, salin, dan pemulihan gabungan untuk layanan yang didukung oleh. AWS Backup Dasbor pekerjaan tersedia di semua Wilayah di mana AWS Backup Audit Manager tersedia. Wilayah yang tidak terdaftar masih dapat mengakses CloudWatch dasbor. Untuk informasi selengkapnya, lihat dasbor AWS Backup konsol.	15 November 2023

Perubahan	Deskripsi	Tanggal
Support untuk cadangan tumpukan bersarang	AWS Backup telah memperluas dukungannya untuk cadangan sumber daya. AWS CloudFormation Tumpukan CloudFormation aplikasi Anda yang memiliki tumpukan bersarang di dalamnya dapat disertakan dalam cadangan Anda. Untuk informasi selengkapnya, lihat CloudFormation stack backup.	8 November 2023
Support untuk Amazon S3 di China (Beijing) dan China (Ningxia).	AWS Backup dukungan untuk Amazon S3 sekarang tersedia di Wilayah China (Beijing) dan China (Ningxia). Untuk informasi selengkapnya, lihat Ketersediaan fitur menurut Wilayah.	26 Oktober 2023
Dukungan untuk backup berkelanjutan Amazon Aurora dan pemulihan P oint-in-time	AWS Backup sekarang mendukung backup dan point-in-time restore berkelanjutan (PITR) untuk sumber daya Aurora. Untuk informasi selengkapnya, lihat Pencadangan berkelanjutan dan pemulihan P oint-in-time .	7 September 2023

Perubahan	Deskripsi	Tanggal
AWS CloudFormation tumpukan mendukung pengecualian sumber daya	AWS Backup sekarang mendukung opsi untuk mengecualikan sumber daya yang dipilih dari AWS CloudFormation tumpukan Anda. Untuk informasi selengkapnya, lihat AWS CloudFormation stack backup.	September 6, 2023
Aturan rencana Backup memperkenalkan fleksibilitas zona waktu	AWS Backup aturan rencana sekarang dapat memiliki zona waktu tertentu untuk jendela cadangan. Untuk informasi selengkap nya, lihat Mengelola paket cadangan.	28 Agustus 2023
AWS Backup sekarang tersedia di Wilayah Israel (Tel Aviv)	Banyak AWS Backup fitur sekarang tersedia di Wilayah Israel (Tel Aviv) yang baru. Untuk melihat sumber daya apa yang didukung, kunjungi Ketersediaan fitur oleh Wilayah AWS.	22 Agustus 2023

Perubahan	Deskripsi	Tanggal
AWS Backup Audit Manager sekarang mendukung akun administrator yang didelegas ikan	AWS Backup Pembuatan laporan Audit Manager sekarang dapat diakses oleh akun administrator yang didelegasikan. Untuk informasi selengkapnya, silakan lihat • Audit backup dan buat laporan dengan AWS Backup Audit Manager • Bekerja dengan laporan audit • Administrator yang didelegasikan	16 Agustus 2023
Pratinjau brankas cadangan yang memiliki lubang udara secara logis	AWS Backup sekarang menawarkan pratinjau jenis baru brankas cadangan untuk membantu melengkapi operasi perlindungan data. Untuk informasi selengkap nya, lihat Logically air-gapped vaults (pratinjau).	8 Agustus 2023
AWS Backup meningkatkan cadangan Amazon S3	AWS Backup telah meningkat kan kinerja, ukuran, dan kemampuan kecepatan untuk cadangan bucket S3. Untuk informasi selengkapnya, lihat cadangan Amazon S3.	1 Agustus 2023

Perubahan	Deskripsi	Tanggal
Fitur Tag on restore sekarang tersedia di Wilayah China	Tag yang merupakan bagian dari cadangan sekarang dapat disalin saat Anda membuat pekerjaan pemulihan di Wilayah China (Beijing) atau China (Ningxia). Untuk informasi selengkap nya, lihat Menyalin tag selama pemulihan.	Juli 17, 2023
AWS Backup sekarang mendukung Amazon S3 di Wilayah tambahan	AWS Backup Dukungan untuk Amazon S3 sekarang tersedia di Eropa (Spanyol) , Eropa (Zurich), Asia Pasifik (Hyderabad), dan Asia Pasifik (Melbourne). Untuk informasi selengkap nya, lihat Ketersediaan fitur menurut Wilayah.	6 Juli 2023

Perubahan	Deskripsi	Tanggal
Salinan lintas akun diperluas ke Wilayah tambahan	AWS Backup sekarang mendukung salinan cadangan lintas akun dari sebagian besar sumber daya di Wilayah berikut: Asia Pasifik (Jakarta) , Timur Tengah (Bahrain), Asia Pasifik (Hong Kong), Afrika (Cape Town), Eropa (Milan), Asia Pasifik (Osaka), Timur Tengah (UEA), Eropa (Spanyol), Eropa (Zurich), Asia Pasifik (Hyderabad), dan Asia Pasifik (Melbourne). Untuk informasi selengkap nya, lihat Ketersediaan fitur menurut Wilayah	5 Juli 2023
Backup Audit Manager tersedia di GovCloud Wilayah	AWS Backup telah memperlua s AWS Backup Audit Manager ke AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat). Untuk informasi selengkap nya, lihat Ketersediaan fitur menurut Wilayah	29 Juni 2023

Perubahan	Deskripsi	Tanggal
Manajemen lintas akun sekarang tersedia di Wilayah GovCloud	AWS Backup sekarang mendukung pengelolaan sumber daya lintas akun di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat). Untuk informasi selengkapnya, lihat Mengelola AWS Backup sumber daya di beberapa AWS akun.	29 Juni 2023
Support untuk salinan Lintas wilayah Amazon Aurora di Wilayah tambahan	AWS Backup sekarang mendukung salinan cadangan lintas wilayah untuk cluster Aurora ke dalam dan dari Wilayah berikut: Asia Pasifik (Jakarta), Timur Tengah (Bahrain), Asia Pasifik (Hong Kong), Afrika (Cape Town), Eropa (Milan), Timur Tengah (UEA), Eropa (Spanyol), Eropa (Zurich), Asia Pasifik (Hyderabad), dan Asia Pasifik (Melbourne).	Juni 5, 2023
Salin tag saat memulihkan	Tag yang merupakan bagian dari cadangan sekarang dapat disalin saat Anda membuat pekerjaan pemulihan. Untuk informasi selengkap nya, lihat Menyalin tag selama pemulihan.	22 Mei 2023

Perubahan	Deskripsi	Tanggal
AWS Backup terintegrasi dengan Pemberitahuan AWS Pengguna	Sekarang Anda dapat memilih untuk menerima notifikasi terkait pencadangan, penyalinan, dan pemulihan peristiwa melalui konsol Pemberitahuan AWS Pengguna. Untuk informasi selengkapnya, lihat Memulai Pemberitahuan AWS Pengguna.	10 Mei 2023
Cadangan Lintas Wilayah tersedia di empat Wilayah baru	AWS Backup sekarang mendukung cadangan Lintas wilayah di Wilayah Timur Tengah (UEA), Wilayah Eropa (Spanyol), Wilayah Eropa (Zurich), dan Wilayah Asia Pasifik (Hyderabad).	28 April 2023
Dukungan AWS Backup salinan lintas wilayah yang diperluas	Pencadangan lintas wilayah Amazon EFS, VMware, dan DynamoDB sekarang dapat dilakukan dalam Wilayah berikut: Asia Pasifik (Jakarta), Timur Tengah (Bahrain), Asia Pasifik (Hong Kong), Afrika (Cape Town), dan Eropa (Milan).	28 April 2023

Perubahan	Deskripsi	Tanggal
Pencadangan dan pemulihan Amazon S3 di Wilayah Amerika Selatan (São Paulo)	AWS Backup dukungan untuk Amazon S3 (Amazon Simple Storage Service) sekarang tersedia di Wilayah Amerika Selatan (São Paulo). Untuk informasi selengkapnya, lihat cadangan Amazon S3.	20 April 2023
AWS Backup Memperlua s ke Wilayah Asia Pasifik (Melbourne)	AWS Backup sekarang tersedia di Wilayah Asia Pasifik (Melbourne). Untuk informasi selengkap nya, lihat Ketersediaan fitur menurut AWS Wilayah.	20 April 2023
Dukungan Regional yang diperluas untuk Amazon S3	AWS Backup dukungan untuk Amazon S3 (Amazon Simple Storage Service) sekarang tersedia di Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat) Untuk informasi selengkapnya, lihat cadangan Amazon S3.	19 April 2023

Perubahan	Deskripsi	Tanggal
Cadangkan dan pulihkan database SAP HANA di instans Amazon EC2	AWS Backup sekarang menawarkan kemampuan untuk mencadangkan dan memulihkan database SAP HANA yang berjalan pada instans Amazon EC2 di sebagian besar Wilayah. Untuk informasi selengkapnya, lihat database SAP HANA di cadangan instans Amazon EC2.	17 April 2023
AWS Backup sekarang tersedia di Wilayah Eropa (Spanyol), Eropa (Zurich), dan Asia Pasifik (Hyderabad)	AWS Backup dukungan telah diperluas ke Wilayah baru, termasuk Eropa (Spanyol) , Eropa (Zurich), dan Asia Pasifik (Hyderabad). Sumber daya yang didukung dapat dicadangkan dan dipulihkan dalam Wilayah ini. Untuk informasi selengkap nya, lihat Ketersediaan fitur menurut AWS Wilayah.	13 April 2023

Perubahan	Deskripsi	Tanggal
Kebijakan AWS terkelola yang diperbarui `AWSBackup AuditAccess`	Kebijakan AWS terkelola yang diperbarui AWSBackup AuditAccess. AWS Backup mengganti pemilihan sumber daya dalam API `config:De scribeComplianceBy ConfigRule` dengan sumber daya wildcard. Untuk informasi selengkapnya lihat Pembaruan kebijakan untuk AWS Backup.	11 April 2023
Hypervisor dengan Log Amazon CloudWatch	AWS Backup pengguna gateway sekarang dapat mengintegrasikan hyperviso r dengan CloudWatch Log untuk memelihara log. Untuk informasi selengkapnya, lihat Mengedit konfigurasi hypervisor dan CloudWatch Log.	29 Maret 2023
Dukungan Regional yang diperluas untuk Amazon S3	AWS Backup Dukungan untuk Amazon S3 sekarang tersedia di Wilayah Asia Pasifik (Jakarta) dan Timur Tengah (UEA).	22 Maret 2023

Perubahan	Deskripsi	Tanggal
Peningkatan cadangan inkremental mesin virtual	Pencadangan VMware VM (mesin virtual) yang mengalami masalah data CBT (Changed Block Tracking) sekarang berisi informasi tambahan untuk membantu memperbaiki dan memecahkan masalah. Untuk informasi selengkapnya, lihat Pencadangan VM tambahan dan Memecahkan Masalah mesin virtual Anda.	15 Maret 2023
AWS Backup dukungan untuk beberapa adapter jaringan	AWS Backup gateway sekarang mendukung konfigurasi beberapa adapter jaringan Untuk informasi selengkapnya tentang mengonfigurasi adaptor jaringan, lihat Mengkonfigurasi gateway Anda untuk beberapa NIC di VMware di Panduan Pengembang.AWS Backup	8 Maret 2023

Perubahan	Deskripsi	Tanggal
AWS Backup dukungan untuk vSphere 8	AWS Backup sekarang mendukung backup dan restore mesin virtual yang berjalan pada VMware vSphere 8. Untuk informasi selengkap nya tentang opsi VMware yang didukung, lihat VM yang didukung di Panduan Pengembang.AWS Backup	8 Maret 2023
AWS Backup Audit Manager mendukung backup Amazon RDS Multi-AZ	Backup Audit Manager sekarang menawarkan dukungan untuk backup Zona Multi-Availability Zone Amazon Relational Database Service. Untuk informasi selengkapnya, lihat cara mengaudit cadangan dan membuat laporan dengan AWS Backup Audit Manager.	1 Februari 2023

Perubahan	Deskripsi	Tanggal
AWS Backup menawarkan cadangan tambahan untuk tabel Amazon Timestream	AWS Backup sekarang menawarkan kemampuan cadangan yang diperluas untuk cadangan Timestream. Paket Backup sekarang dapat mengambil backup tambahan untuk mengurangi waktu yang diperlukan untuk backup sumber daya Timestream dan menurunkan biaya penyimpan an. Untuk informasi selengkapnya, lihat pencadangan Amazon Timestream.	23 Januari 2023
AWS Backup sekarang tersedia di Dubai	AWS Backup telah diperluas ke Wilayah Timur Tengah (UEA). Sumber daya yang didukung dapat dicadangkan dan dipulihkan dalam Wilayah ini.	Januari 17, 2023

Perubahan	Deskripsi	Tanggal
Penyalinan Lintas Wilayah tersedia di Wilayah tambahan	AWS Backup Saat ini menawarkan backup lintas wilayah di Wilayah Asia Pasifik (Jakarta), Wilayah Timur Tengah (Bahrain), Wilayah Asia Pasifik (Hong Kong), Wilayah Afrika (Cape Town), dan Wilayah Eropa (Milan) untuk sebagian besar sumber daya. Untuk informasi selengkap nya, lihat Membuat salinan cadangan di seluruh Wilayah AWS.	21 Desember 2022
Backup Gateway Batas Bandwidth dan Throttling	AWS Backup Gateway sekarang memungkinkan batasan pada throughput upload dari gateway AWS Backup untuk mengontrol jumlah bandwidth jaringan yang digunakan oleh gateway. Untuk mendukung fitur ini, AWS Backup telah membuat dan memperbarui kebijakan terkelola, termasuk `AWSBackupFullAccess` dan`AWSBackupOperatorAccess` . Untuk informasi selengkap nya, lihat Backup Gateway bandwidth throttling.	Desember 15, 2022

Perubahan	Deskripsi	Tanggal
Backup Gateway dukungan tag VMware	AWS Backup Gateway sekarang mendukung tag VMware. Pengguna memiliki fleksibilitas tambahan untuk membuat AWS tag yang cocok dengan tag yang digunakan untuk mesin virtual. Untuk mendukung fitur ini, AWS Backup telah membuat dan memperbar ui kebijakan terkelola , termasuk`AWSBackup GatewayServiceRole PolicyForVirtualMa chineMeta dataSync` ,`AWSBackup FullAccess` , dan`AWSBackupOperatorA ccess` . Untuk informasi selengkapnya, lihat tag VMware.	Desember 15, 2022
AWS Backup dukungan untuk Amazon Timestream	AWS Backup sekarang mendukung pencadang an dan pemulihan tabel Amazon Timestream. Untuk informasi selengkapnya, lihat Pencadangan Amazon Timestream.	13 Desember 2022

Perubahan	Deskripsi	Tanggal
AWS Backup menawarkan Legal Hold	AWS Backup memperken alkan alat baru untuk membantu melindungi titik pemulihan melalui penahanan hukum. Untuk informasi lebih lanjut, lihat Penahanan hukum.	27 November 2022
AWS Backup Audit Manager Pelaporan lintas wilayah dan lintas akun	AWS Backup Audit Manager menghadirkan fungsionalitas tambahan untuk kepatuhan dan laporan pekerjaan. Pengguna dapat membuat laporan yang menggabun gkan beberapa Wilayah dan beberapa akun. Untuk informasi selengkapnya, lihat Bekerja dengan laporan audit.	27 November 2022
AWS Backup mendukung Amazon Redshift	AWS Backup sekarang menawarkan dukungan untuk cadangan cluster Amazon Redshift dan untuk memulihka n cluster dan tabel Amazon Redshift. Untuk informasi selengkapnya, lihat cadangan Amazon Redshift.	27 November 2022

Perubahan	Deskripsi	Tanggal
AWS Backup menawarkan dukungan untuk cadangan tumpukan AWS CloudFormation aplikasi	AWS Backup menyediakan kemampuan untuk membuat cadangan CloudFormation dan memulihkan aplikasi yang berisi banyak sumber daya dengan membuat cadangan tumpukan dan memulihkan sumber daya di dalamnya. Untuk informasi selengkapnya, lihat Backup tumpukan aplikasi.	27 November 2022
AWS Backup menawarkan akun administrator yang didelegasikan dan delegasi kebijakan cadangan	AWS Backup akun yang terdaftar AWS Organizations dapat menunjuk akun anggota sebagai akun administrator yang didelegasikan. Untuk informasi selengkapnya, lihat Mengelola beberapa akun dengan AWS Organizations.	November 27,2022

Perubahan	Deskripsi	Tanggal
Pratinjau Publik SAP HANA di Amazon EC2 Instans backup dan restore	AWS Backup dan AWS Backint menawarkan pratinjau fungsionalitas publik terintegrasi untuk mencadangkan dan memulihkan database SAP HANA pada instans EC2. Untuk informasi selengkapnya, lihat Pratinjau Publik SAP HANA di instans Amazon EC2. Untuk mendukung pratinjau ini, AWS Backup telah menyediakan pembaruan kebijakan dan Kebijakan AWS Terkelola baru untuk fitur-fitur ini.	November 20, 2022
Kembalikan instans VMware ke Amazon EC2	AWS Backup sekarang menawarkan kemampuan untuk mengembalikan mesin virtual ke instans Amazon EC2, selain kemampuan untuk mengembalikan mesin ke EBS, VMware, VMware Cloud on, dan VMware Cloud on. AWS AWS Outposts Untuk informasi selengkapnya, lihat dokumentasi tentang cara Menggunakan AWS Backup konsol untuk memulihkan titik pemulihan mesin virtual.	9 November 2022

Perubahan	Deskripsi	Tanggal
AWS Backup Fungsionalitas Vault Lock yang diperluas	AWS Backup Vault Lock sekarang dapat dibuat dalam mode tata kelola untuk perlindungan IAM tambahan atau dalam mode kepatuhan untuk memastikan kekekalan. Pelajari lebih lanjut di AWS Backup Vault Lock.	4 Oktober 2022
AWS Backup Audit Manager sekarang tersedia di Wilayah Afrika (Cape Town) dan Wilayah Eropa (Milan)	AWS Backup Audit Manager telah diperluas ke Wilayah Afrika (Cape Town) dan Wilayah Eropa (Milan). Untuk informasi selengkap nya tentang Backup Audit Manager, lihat Audit backup dan buat laporan dengan AWS Backup Audit Manager.	14 September 2022
AWS Backup membawa CloudWatch metrik Amazon ke dasbor konsol Backup	AWS Backup menyempur nakan dasbor konsol Cadangan untuk menampilkan CloudWatch metrik Amazon terintegrasi untuk pencadang an dan pemulihan pekerjaan untuk kemampuan pemantaua n dan fleksibilitas tambahan.	8 September 2022
Support untuk fleksibil itas enkripsi Amazon EBS tambahan selama pemulihan	AWS Backup sekarang menawarkan pilihan enkripsi tambahan selama pemulihan snapshot Amazon EBS.	September 1, 2022

Perubahan	Deskripsi	Tanggal
AWS Backup mendukung penyalinan cadangan lintas akun Amazon S3 dan lintas wilayah	AWS Backup sekarang menawarkan penyalinan cadangan lintas wilayah dan lintas akun untuk cadangan Amazon S3. Untuk informasi lebih lanjut, lihat cadangan Amazon S3.	28 Juli 2022
AWS Backup Audit Manager menawarkan dukungan kontrol tambahan untuk FSx untuk ONTAP	AWS Backup Audit Manager sekarang menawarkan kontrol tambahan untuk mendukung pemantauan dan audit FSx untuk volume ONTAP, termasuk sumber daya Backup dilindungi oleh rencana cadangan dan titik pemulihan terakhir dibuat. Untuk informasi selengkapnya, lihat Kontrol dan remediasi AWS Backup Audit Manager.	22 Juli 2022
AWS Backup menambahkan dukungan untuk mencadangkan dan memulihkan cluster Amazon RDS Multi-AZ untuk cluster PostgreSQL dan MySQL	AWS Backup telah menambahkan opsi pencadangan dan pemulihan klaster Multi-Availability Zone dengan satu instance basis data siaga utama dan dua instance basis data siaga yang dapat dibaca. Untuk mempelajari lebih lanjut, lihat Pencadangan Amazon RDS Multi-AZ.	20 Juli 2022

Perubahan	Deskripsi	Tanggal
AWS Backup Audit Manager menambahkan kontrol baru untuk pembuatan titik pemulihan	AWS Backup Audit Manager menawarkan kontrol audit baru untuk meningkatkan dukungan kepatuhan. `Last recovery point created`adalah kontrol tambahan opsional untuk memastikan titik pemulihan dibuat dalam kerangka waktu yang ditentukan. Untuk mempelajari lebih lanjut, lihat Kontrol yang dibuat titik pemulihan terakhir.	Juni 29, 2022
Menambahkan AWS Backup sampel titik akhir Gateway	AWS Backup Gateway menyediakan contoh titik akhir untuk membantu pengguna terhubung ke VPN (Virtual Private Networks). Untuk informasi selengkapnya, lihat Membuat titik AWS Backup akhir VPC.	14 Juni 2022

Perubahan	Deskripsi	Tanggal
AWS Backup sekarang menawarkan titik akhir Amazon VPC untuk VMware	AWS Backup sekarang mendukung titik akhir Amazon VPC untuk VMware, memungkinkan Anda untuk menggunakan jaringan pribadi virtual antara lingkunga n VMware Anda dan menggunakan. AWS AWS PrivateLink Untuk informasi selengkap nya, lihat Membuat gateway dan AWS Backup dan AWS PrivateLink.	1 Juni 2022
AWS Backup Audit Manager menawarkan dukungan kontrol tambahan untuk Amazon S3	Backup Audit Manager sekarang menawarkan dukungan untuk kontrol kepatuhan Sumber daya Backup yang dilindungi oleh rencana cadangan untuk jenis sumber daya S3. Untuk informasi selengkapnya, lihat Kontrol dan remediasi AWS Backup Audit Manager.	25 Mei 2022

Perubahan	Deskripsi	Tanggal
AWS Backup Audit Manager menawarkan dukungan kontrol tambahan untuk Storage Gateway	Backup Audit Manager sekarang menawarkan dukungan untuk kontrol kepatuhan Sumber daya Backup yang dilindungi oleh rencana cadangan untuk jenis sumber daya Storage Gateway. Untuk informasi selengkapnya, lihat Kontrol dan remediasi AWS Backup Audit Manager.	25 Mei 2022
Support untuk Amazon FSx untuk OpenZFS	AWS Backup sekarang menawarkan manajemen tambahan perlindungan data untuk mencadangkan dan memulihkan ke FSx untuk sistem file OpenZFS.	Mei 18, 2022
AWS Backup Dukungan Audit Manager untuk VMware	AWS Backup sekarang menyediakan dukungan untuk mesin virtual dalam kontrol dan remediasi Backup Audit Manager. Untuk informasi selengkapnya, lihat Kontrol dan remediasi AWS Backup Audit Manager.	Mei 11, 2022
Amazon FSx sekarang didukung di Wilayah Asia Pasifik (Osaka)	AWS Backup sekarang menawarkan cadangan Amazon FSx di, dan salinan lintas wilayah ke dan dari, Wilayah Asia Pasifik (Osaka).	26 April 2022

Perubahan	Deskripsi	Tanggal
Dukungan untuk Amazon FSx for Lustre Persistent_2	AWS Backup sekarang menawarkan ketersediaan umum dukungan untuk Amazon FSx for Lustre, yang mendukung tingkat throughput per unit penyimpanan yang lebih tinggi dibandingkan dengan sistem file Persistent_1.	5 April 2022
Penyempurnaan VMware	AWS Backup sekarang menawarkan pemulihan ke Amazon EBS Volume, pemulihan level disk, dan dukungan untuk VMware aktif. AWS Outposts Untuk informasi selengkapnya, lihat Memulihkan mesin virtual.	31 Maret 2022
AWS Backup Ketersediaan untuk Asia Pasifik (Jakarta)	AWS Backup sekarang tersedia untuk pelanggan di Wilayah Asia Pasifik (Jakarta).	Maret 17, 2022
Kontrol Baru untuk AWS Backup Audit Manager	AWS Backup Audit Manager memperkenalkan tiga kontrol audit baru: Cross-Region copy, Cross-account copy, dan Backup Vault Lock. Untuk informasi selengkapnya, lihat Kontrol dan remediasi AWS Backup Audit Manager.	Maret 17, 2022

Perubahan	Deskripsi	Tanggal
Support untuk AWS PrivateLink	Dengan AWS PrivateLink for AWS Backup, Anda dapat terhubung langsung AWS Backup menggunakan titik akhir antarmuka di VPC Anda alih-alih terhubung melalui internet publik. Endpoint antarmuka dapat diakses langsung dari aplikasi yang ada di tempat atau di AWS Wilayah yang berbeda. Untuk informasi selengkapnya, lihat AWS Backup dan AWS PrivateLink.	28 Februari 2022
Dukungan untuk Amazon Simple Storage Service (Amazon S3)	Ketersediaan umum AWS Backup untuk Amazon S3 di semua Wilayah AWS tersedia kecuali untuk Wilayah China (Beijing), Wilayah China (Ningxia), (AS-Barat), dan AWS GovCloud AWS GovCloud (AS-Timur) Wilayah. Untuk informasi selengkapnya, lihat Bekerja dengan data Amazon S3.	14 Februari 2022
Dukungan untuk cadangan DynamoDB Tingkat Lanjut di Wilayah China AWS	Advanced DynamoDB backup sekarang tersedia di China (Beijing) Region dan China (Ningxia) Region. Untuk informasi selengkapnya, lihat Cadangan DynamoDB lanjutan.	18 Januari 2022

Perubahan	Deskripsi	Tanggal
Pratinjau publik dukungan untuk Amazon S3	AWS Backup menawarkan pratinjau publik cadangan Amazon S3. Untuk informasi selengkapnya, lihat Bekerja dengan data Amazon S3.	30 November 2021
Support untuk mesin virtual VMware (VM)	Anda sekarang dapat menggunakan AWS Backup untuk secara otomatis mencadangkan VMware VM. Untuk informasi selengkap nya, lihat Pencadangan mesin virtual.	30 November 2021
Support untuk cadangan DynamoDB tingkat lanjut	Anda sekarang dapat menggunakan fitur berikut AWS Backup untuk semua cadangan tabel DynamoDB baru yang Anda buat: tiering penyimpanan dingin, penandaan alokasi biaya, salinan lintas wilayah, salinan lintas akun, enkripsi indpendent, dan menyalin tag dari tabel DynamoDB sumber. Untuk informasi selengkapnya, lihat Cadangan DynamoDB tingkat lanjut di Panduan Pengembang Amazon DynamoDB dan Menggunakan AWS Backup dengan DynamoDB.	23 November 2021

Perubahan	Deskripsi	Tanggal
Dukungan untuk peningkatan penugasan AWS Backup sumber daya di Wilayah China AWS	AWS Backup peningkatan penugasan sumber daya sekarang tersedia di Wilayah China (Beijing) dan Wilayah China (Ningxia). Untuk informasi selengkapnya, lihat Menetapkan sumber daya ke paket cadangan.	November 16, 2021
Peluncuran AWS Backup peningkatan tugas sumber daya	Peningkatan penugasan sumber daya cadangan memberi Anda kontrol tambahan yang halus, serta proses baru yang disederhanakan untuk menerapkan rencana cadangan yang melindungi ratusan ribu sumber daya. AWS Gunakan fitur ini untuk meningkatkan kecepatan, fleksibilitas, dan presisi Anda saat melindungi data menggunakan AWS Backup. Untuk informasi selengkapnya, lihat Menetapkan sumber daya ke paket cadangan.	November 10, 2021
Dukungan untuk Amazon Neptunus	Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan cluster Amazon Neptunus. Untuk mempelajari selengkapnya, lihat Apa itu AWS Backup?	November 5, 2021

Perubahan	Deskripsi	Tanggal
Dukungan untuk Amazon DocumentDB	Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan cluster Amazon DocumentDB. Untuk mempelajari selengkapnya, lihat Apa itu AWS Backup?	November 5, 2021
Support untuk AWS Backup Vault Lock di Wilayah AWS China	AWS Backup Vault Lock sekarang tersedia di Wilayah China (Beijing) dan Wilayah China (Ningxia). Untuk informasi selengkapnya, lihat Kunci Penyimpanan AWS Backup.	3 November 2021
Peluncuran AWS Backup Vault Lock	Dengan AWS Backup Vault Lock, Anda dapat mencegah penghapusan cadangan yang disimpan di brankas cadangan. AWS Backup Untuk informasi selengkapnya, lihat Kunci Penyimpanan AWS Backup.	7 Oktober 2021
Peluncuran laporan kepatuhan AWS Backup Audit Manager	Dengan laporan kepatuhan, Anda dapat membuat laporan harian tentang kepatuhan aktivitas pencadangan dan sumber daya terhadap kontrol yang Anda tetapkan dalam kerangka kerja AWS Backup Audit Manager. Untuk informasi selengkapnya, lihat Templat laporan kepatuhan.	5 Oktober 2021

Perubahan	Deskripsi	Tanggal
AWS CloudFormation dukungan untuk AWS Backup Audit Manager	Dengan AWS CloudFormation, Anda sekarang dapat menerapkan kerangka kerja, kontrol, dan rencana laporan AWS Backup Audit Manager dengan cara yang aman dan dapat diulang dalam skala besar. Untuk informasi selengkapnya, lihat Audit cadangan dan laporan dengan AWS Backup Audit Manager.	4 Oktober 2021
Peluncuran AWS Backup Audit Manager	Dengan AWS Backup Audit Manager, Anda sekarang dapat menentukan kontrol untuk aktivitas dan sumber daya pencadangan, serta mengidentifikasi aktivitas dan sumber daya yang tidak sesuai dengan kontrol Anda. Anda juga dapat menggunakan AWS Backup Audit Manager untuk menghasilkan laporan harian dan sesuai permintaan yang berfungsi sebagai bukti kepatuhan terhadap kontrol yang ditentukan dari waktu ke waktu. Untuk informasi selengkapnya, lihat Audit cadangan dan laporan dengan AWS Backup Audit Manager.	Agustus 24, 2021

Perubahan	Deskripsi	Tanggal
Support untuk operasi titik pemulihan asinkron baru	AWS Backup sekarang mengasumsikan peran terkait layanan untuk mengelola aturan siklus hidup cadangan jika Anda mengubah atau menghapus peran IAM asli Anda. Untuk informasi selengkapnya, lihat Menghapus cadangan.	23 Agustus 2021
Support untuk Amazon EBS multi-volume, backup yang konsisten dengan crash	Sekarang, saat Anda menggunakannya AWS Backup untuk melindung i instans Amazon EC2, AWS Backup mengambil pencadangan multi-volume dan konsisten crash dari semua volume Amazon EBS yang dilampirkan ke setiap instans Amazon EC2 secara default. Untuk informasi selengkapnya, lihat Membuat cadangan multi-volume Amazon EBS dan konsisten crash.	14 Juni 2021

Perubahan	Deskripsi	Tanggal
Support untuk Amazon FSx dalam tambahan Wilayah AWS	Anda sekarang dapat menggunakan AWS Backup untuk melindungi sistem file Amazon FSx Anda di Wilayah berikut: AWS GovCloud (US), Wilayah Eropa (Milan), Wilayah Afrika (Cape Town), dan Wilayah Timur Tengah (Bahrain). Untuk informasi lebih lanjut, lihat Titik akhir dan kuota AWS Backup di Referensi Umum AWS .	April 15, 2021
Dukungan untuk Amazon FSx Cross-region dan cross-acc ount backup	Anda sekarang dapat menggunakan AWS Backup untuk menyalin cadangan Amazon FSx di seluruh dan akun. Wilayah AWS Untuk informasi selengkapnya, lihat Membuat Salinan Cadangan. Jika Anda menggunakan kebijakan yang dikelola pelanggan, Anda harus menambahkan izin baru `fsx:CopyBackup` untuk mencegah pekerjaan cadangan yang ada gagal. Untuk izin tersebut, lihat pernyataan terakhir dalam kebijakan pencadangan Amazon FSx dalam kebijakan yang dikelola Pelanggan.	12 April 2021

Perubahan	Deskripsi	Tanggal
Support untuk tag alokasi biaya untuk backup Amazon EFS	Anda sekarang dapat menggunakan tag alokasi biaya untuk melacak biaya untuk cadangan Amazon EFS Anda pada tingkat terperinci, dan melihat serta memfilter tag tersebut. AWS Cost Explorer Untuk informasi selengkapnya, lihat Menggunakan Tag Alokasi Biaya.	7 April 2021
FedRAMP Otorisasi Tinggi	AWS Backup sekarang berwenang untuk mendukung beban kerja FedRAMP High. Untuk informasi selengkap nya, lihat AWS Layanan dalam Lingkup menurut Program Kepatuhan.	25 Maret 2021
Baru Wilayah AWS	AWS Backup sekarang tersedia di Wilayah Asia Pasifik (Osaka). Di Wilayah ini, AWS Backup saat ini tidak mendukung Storage Gateway, Amazon FSx, dan cadangan lintas akun di Wilayah ini. Untuk informasi lebih lanjut, lihat Titik akhir dan kuota AWS Backup di Referensi Umum AWS .	25 Maret 2021

Perubahan	Deskripsi	Tanggal
Support untuk operasi batch titik pemulihan	Anda sekarang dapat menggunakan AWS Backup konsol untuk mengotoma tiskan operasi batch untuk membersihkan titik pemulihan di brankas cadangan Anda. Untuk informasi selengkapnya, lihat Menghapus cadangan.	23 Maret 2021
Dukungan untuk pemulihan ke kelas penyimpanan Amazon EFS One Zone	Anda sekarang dapat memulihkan cadangan Amazon EFS Anda ke kelas penyimpanan Amazon EFS One Zone. Untuk informasi selengkapnya, lihat Memulihkan sistem file Amazon EFS.	12 Maret 2021
Support untuk pemulihan Amazon Relational Database point-in-time Service dan pencadangan berkelanjutan	Anda sekarang dapat menggunakan AWS Backup untuk mengotomatiskan backup berkelanjutan Amazon RDS dan melakukan point-in-time restore (PITR), selain mengatur cadangan snapshot Anda. Untuk informasi selengkapnya, lihat Memulihkan ke waktu tertentu menggunakan point-in-time pemulihan.	10 Maret 2021

Perubahan	Deskripsi	Tanggal
Support untuk Amazon CloudWatch	Anda sekarang dapat menggunakan CloudWatch untuk memantau AWS Backup metrik. Untuk informasi selengkapnya, lihat Memantau Peristiwa dan Metrik dengan Amazon CloudWatch dan Amazon EventBridge.	3 Februari 2021
Support untuk Amazon EventBridge	Anda sekarang dapat menggunakan EventBrid ge untuk memantau AWS Backup acara. Untuk informasi selengkapnya, lihat Memantau Peristiwa dan Metrik dengan Amazon CloudWatch dan Amazon EventBridge.	3 Februari 2021
Support untuk backup lintas akun	Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan sumber daya Anda di beberapa Akun AWS. Untuk informasi selengkapnya, lihat Membuat salinan cadangan di seluruh AWS akun.	18 November 2020
Dukungan untuk mencadang kan dan memulihkan sistem file Amazon FSx	Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan sistem file Amazon FSx. Untuk informasi selengkapnya, lihat Bekerja dengan sistem file Amazon FSx.	9 November 2020

Perubahan	Deskripsi	Tanggal
Baru Wilayah AWS	AWS Backup sekarang tersedia di Afrika (Cape Town) dan Eropa (Milan) Wilayah AWS. Untuk informasi lebih lanjut, lihat Titik akhir dan kuota AWS Backup di Referensi Umum AWS .	21 Oktober 2020
Support untuk cadangan Windows berkemampuan VSS	Anda sekarang dapat mencadangkan dan memulihkan aplikasi Windows berkemampuan VSS (Volume Shadow Copy Service) yang berjalan di instans Amazon EC2. Untuk informasi selengkapnya, lihat Membuat cadangan Windows VSS.	22 September 2020
Dukungan untuk cadangan otomatis Amazon EFS	Anda sekarang dapat menggunakan AWS Backup untuk secara otomatis mencadangkan sistem file Amazon EFS. Untuk informasi selengkapnya, lihat Memulai 4: Membuat cadangan otomatis Amazon EFS.	Juli 16, 2020
Baru Wilayah AWS	AWS Backup sekarang tersedia di AWS GovCloud (US) Region. Untuk informasi lebih lanjut, lihat Titik akhir dan kuota AWS Backup di Referensi Umum AWS .	24 Juni 2020

Perubahan	Deskripsi	Tanggal
Support untuk mengelola backup di beberapa Akun AWS	Anda sekarang dapat mengelola cadangan di beberapa Akun AWS dengan menggunakan. AWS Organizations Untuk informasi selengkapnya, lihat Cara Kerja Manajemen Lintas Akun.	24 Juni 2020
Support untuk Amazon Aurora ditambahkan ke AWS Backup	Anda sekarang dapat mengonfigurasi AWS Backup untuk mencadangkan sumber daya untuk Amazon Aurora. Untuk selengkapnya, lihat Ikhtisar Mencadangkan dan Memulihkan Cluster DB Aurora di Panduan Pengguna Amazon Aurora.	10 Juni 2020
Support untuk mengkonfi gurasi layanan untuk bekerja dengan AWS Backup	Anda sekarang dapat mengonfigurasi AWS Backup untuk mencadangkan sumber daya untuk AWS layanan tertentu. Untuk informasi selengkapnya, lihat Memilih untuk mengelola layanan dengan AWS Backup.	20 Mei 2020
Support untuk mencadang kan instans Amazon EC2 dan juga menambahkan dukungan untuk pencadangan lintas wilayah	Anda sekarang dapat mencadangkan seluruh instans Amazon EC2 dan juga menyalin sumber daya. Wilayah AWS Untuk informasi selengkapnya, lihat Membuat salinan cadangan di seluruh Wilayah AWS.	13 Januari 2020

Perubahan	Deskripsi	Tanggal
Panduan baru	AWS peluncuran AWS Backup dan Panduan AWS Backup Pengembang.	Januari 15, 2019

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.