



Strategi pemulihan bencana untuk database AWS

AWS Panduan Preskriptif



AWS Panduan Preskriptif: Strategi pemulihan bencana untuk database AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Pengantar	1
Hasil bisnis yang ditargetkan	4
Mengatasi kerugian finansial	4
Mengurangi dampak terhadap proses bisnis yang kritis	4
Kurangi koordinasi manual selama acara nyata (otomatisasi)	4
Pertahankan pelanggan Anda	4
Tingkatkan keamanan	4
Meningkatkan produktivitas karyawan	5
Mendefinisikan strategi DR Anda	6
Memilih layanan database	10
Mendorong adopsi strategi DR Anda	14
Mengotomatiskan strategi DR Anda	15
Deteksi peristiwa bencana	15
Failover	15
Pengujian untuk mencapai kepercayaan	17
Pertimbangan-pertimbangan	17
Frekuensi pengujian	17
Deteksi penyimpangan	18
Observabilitas	18
Langkah dan sumber daya selanjutnya	19
Riwayat dokumen	20
.....	xxi

Strategi pemulihan bencana untuk database AWS

Oliver Francis, Balaji Desikachari, Jitendra Kumar, dan Suhas Basavaraj, Amazon Web Services

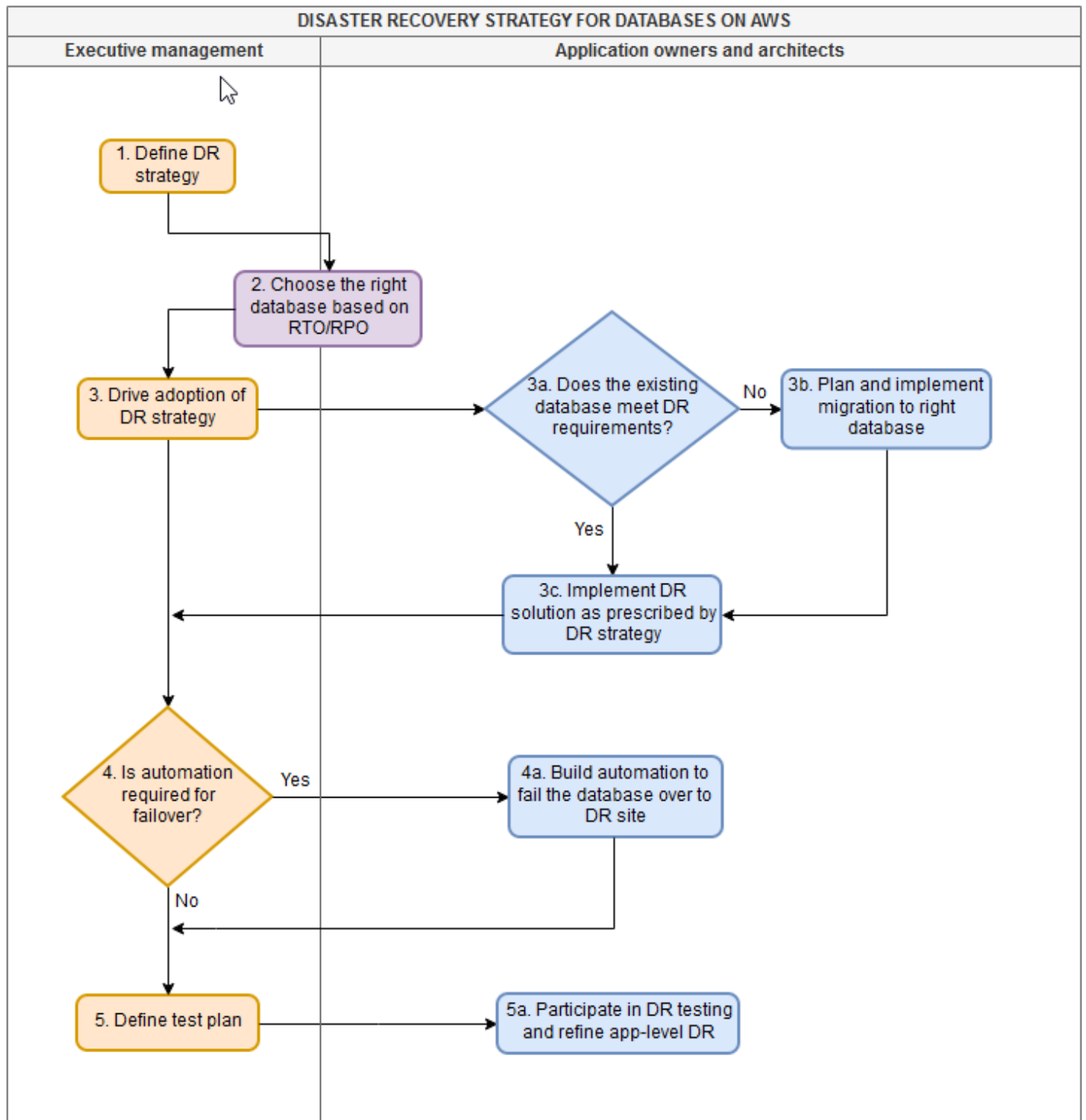
Pada Oktober 2021, Dewan Teknologi Forbes menerbitkan artikel berjudul [Mengapa Pemulihan Bencana Tidak Lagi Opsional Untuk Bisnis Saat Ini](#). Artikel tersebut mengutip a U.S. Studi Federal Emergency Management Agency (FEMA) yang menyatakan bahwa 40 persen usaha kecil dan menengah di Amerika Serikat keluar dari bisnis setelah bencana. Selain itu, 25 persen dari bisnis yang dibuka kembali ditutup kembali dalam waktu satu tahun. Mengingat beratnya subjek, rencana kelangsungan bisnis yang dipersiapkan dengan baik yang mencakup strategi pemulihan bencana (DR) untuk aset TI sangat penting untuk memastikan pertumbuhan jangka panjang dan kesuksesan bisnis Anda. Komputasi awan telah membuat pemulihan bencana layak bahkan untuk usaha kecil dan menengah dengan menurunkan penghalang untuk masuk. Mengingat risiko yang ditimbulkan oleh kurangnya solusi yang memadai dalam kasus bencana, rencana kelangsungan bisnis yang mencakup strategi DR harus berada di urutan teratas daftar prioritas Anda sebagai pemimpin bisnis.

Jika beban kerja Anda berjalan AWS, tidak diragukan lagi sebagian besar data Anda berada di AWS database. Apakah itu data yang disimpan dalam sistem database relasional (RDBMS) seperti Amazon Aurora MySQL-Compatible Edition atau database NoSQL seperti Amazon DynamoDB, data ini berharga untuk bisnis Anda. Mengembangkan strategi DR yang khusus untuk database AWS membantu Anda memahami apa yang AWS ditawarkan dalam hal pemulihan bencana untuk database Anda dan bagaimana Anda dapat memanfaatkan informasi ini dalam rencana DR Anda untuk AWS Cloud

Diagram jalur renang berikut menyajikan tugas tingkat tinggi yang terkait dengan mendefinisikan dan menerapkan strategi DR. Dua kolom menunjukkan tugas yang dimiliki oleh tim manajemen eksekutif dan tugas yang dimiliki oleh pemilik aplikasi dan arsitek. Tim manajemen eksekutif memiliki pengambilan keputusan. Tim ini mendefinisikan strategi DR yang akan diikuti oleh organisasi, mendorong adopsi DR di seluruh organisasi, memutuskan apakah otomatisasi akan diperlukan untuk mencapai tujuan DR, dan mendefinisikan rencana pengujian DR.

Ketika strategi DR diterapkan, tim manajemen eksekutif bekerja dengan pemilik aplikasi dan arsitek untuk memilih database yang tepat yang sesuai dengan tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO) harapan yang berasal dari strategi DR. Ketika tim manajemen eksekutif mendorong adopsi strategi DR, pemilik aplikasi dan arsitek mengevaluasi database yang digunakan dalam aplikasi mereka dan bermigrasi ke database yang tepat jika yang saat ini tidak mencapai RTO dan RPO yang ditetapkan untuk aplikasi mereka. Pemilik aplikasi dan arsitek juga membangun

otomatisasi jika diperlukan dan berpartisipasi dalam pengujian DR untuk menyempurnakan dan meningkatkan DR.



Artikel ini menjelaskan langkah-langkah ini pada tingkat tinggi untuk para pemimpin bisnis dan pengambil keputusan yang ingin merumuskan strategi DR lintas wilayah yang membantu memenuhi

tujuan bisnis mereka. Artikel ini mengasumsikan beberapa pengetahuan teknis dan keakraban dengan terminologi pemulihan bencana tetapi tidak memiliki keahlian. AWS

Hasil bisnis yang ditargetkan

Bagian ini membahas hasil yang diharapkan terkait dengan mendefinisikan dan membangun rencana pemulihan bencana (DR) untuk basis data Anda. AWS

Mengatasi kerugian finansial

Jika Anda memiliki solusi DR yang dirancang dengan baik untuk database yang menyimpan data aplikasi Anda, Anda dapat pulih dari peristiwa bencana lebih cepat dan dengan kehilangan data minimal atau tanpa. Ini meminimalkan kerugian finansial yang berpotensi diakibatkan oleh aplikasi Anda yang tidak tersedia untuk waktu yang lama, atau, dalam kasus terburuk, dari kehilangan data Anda secara permanen.

Mengurangi dampak terhadap proses bisnis yang kritis

Ketika Anda mengidentifikasi layanan dan proses tingkat 0 Anda, dan merencanakan strategi DR Anda untuk memulihkannya dengan cepat, Anda akan dapat mengurangi dampak signifikan terhadap layanan dan proses ini, dan menangani pemulihan proses dependen juga.

Kurangi koordinasi manual selama acara nyata (otomatisasi)

Jika Anda memilih untuk mengotomatiskan solusi DR Anda, Anda dapat mengurangi koordinasi manual yang diperlukan untuk menjalankan solusi DR ketika ada acara. Otomasi bermanfaat bahkan ketika Anda menguji [rencana kontinuitas bisnis \(BCP\)](#) Anda, yang menentukan bagaimana Anda mempertahankan operasi bisnis standar selama gangguan yang tidak direncanakan.

Pertahankan pelanggan Anda

Di pasar yang kompetitif, strategi DR Anda memengaruhi cara Anda mendapatkan loyalitas pelanggan dan mempertahankan pelanggan. Jika organisasi Anda memiliki kemampuan untuk pulih dengan cepat dari bencana, Anda dapat membangun kepercayaan diri dengan pelanggan Anda.

Tingkatkan keamanan

Strategi DR lintas wilayah yang terencana dengan baik dapat membantu membatasi dampak serangan ransomware ke satu Wilayah AWS dan memungkinkan Anda untuk menggunakan data Anda di Wilayah lain secara bebas tanpa kehilangan data Anda.

Meningkatkan produktivitas karyawan

Jika karyawan Anda memahami proses DR dengan baik dan merasa nyaman dengannya, acara DR tidak akan menimbulkan kepanikan. Anda dapat mengikuti runbook yang terdefinisi dengan baik untuk menerapkan solusi DR, dan karyawan Anda dapat memanfaatkan waktu mereka sebaik mungkin untuk mengembalikan bisnis Anda ke normal.

Mendefinisikan strategi pemulihan bencana Anda

Bergantung pada seberapa penting aplikasi dalam organisasi Anda untuk bisnis Anda, Anda dapat memutuskan strategi yang seragam untuk semua aplikasi atau mengembangkan strategi DR yang lebih kompleks berdasarkan kekritisannya setiap aplikasi. Organisasi Anda mungkin mentolerir downtime beberapa jam sebelum semua aplikasi dimunculkan di situs DR. Dalam hal ini, Anda dapat memilih strategi DR yang hemat biaya berdasarkan pencadangan dan pemulihan untuk semua database. Di sisi lain, bisnis organisasi Anda mungkin bergantung pada beberapa layanan atau aplikasi penting yang tersedia dengan cepat, dengan persyaratan RPO dan RTO yang lebih agresif, sedangkan aplikasi lain mungkin mentolerir kebutuhan RPO dan RTO yang kurang ketat. Dalam hal ini, Anda perlu menetapkan strategi DR yang tepat untuk setiap tingkatan aplikasi dan database.

Tabel berikut menjelaskan empat opsi DR untuk beban kerja yang berjalan di AWS Cloud, untuk membantu Anda menentukan dan menentukan strategi DR organisasi Anda. RPO dan RTO yang didokumentasikan dalam tabel ini adalah untuk tumpukan penuh yang mencakup komponen aplikasi dan database. Untuk informasi selengkapnya, lihat [Opsi pemulihan bencana di cloud](#) dalam dokumentasi AWS Well-Architected Framework. Bagian selanjutnya mencakup opsi RPO dan RTO yang khusus untuk database.

Opsi pemulihan	RPO	RTO	Tugas infrastruktur di Wilayah DR	Biaya
Pencadangan dan pemulihan	Jam	Kurang dari 24 jam	Menyediakan semua sumber daya aplikasi yang diperlukan di Wilayah DR dan memulihkan database dari snapshot yang disalin.	Rendah
Pilot light	Puluhan menit	Puluhan menit	Berikan salinan infrastruktur aplikasi Anda dan matikan	Sedang

sumber daya
di tumpukan
aplikasi.
Replikasi data
Anda dari
satu Wilayah
ke Wilayah
lainnya. Jaga
agar database
selalu aktif dan
disinkronkan
dengan basis
data utama.
Menyediakan
sumber daya
sesuai perminta
n selama
peristiwa failover
dan pengujian
. Anda juga
perlu menerapka
n perubahan
infrastruktur
dan perubahan
aplikasi ke kedua
Wilayah secara
bersamaan
. Anda dapat
menyederh
anakan ini
dengan
membangun
jaringan pipa
otomatisasi yang
dapat menyinkro
nkan kode dan

			infrastruktur di Wilayah primer dan DR.	
Warm standby	Menit	Menit	Menyediakan salinan seluruh infrastruktur aplikasi di Wilayah DR, tetapi tetap memperkecil salinannya dibandingkan dengan Wilayah utama. Wilayah DR akan dapat menerima lalu lintas pada volume yang lebih kecil dibandingkan dengan Wilayah utama.	Tinggi

Multi-site atau active/active	Dekat nol	Nol atau mendekati nol	Berikan salinan lengkap infrastruktur Anda ke Wilayah DR. Semua sumber daya di Wilayah DR akan setara dengan sumber daya di Wilayah primer dan akan dapat melayani lalu lintas pada skala yang sama dengan Wilayah utama. Karena tidak ada jeda dalam arus lalu lintas, opsi ini tidak memerlukan tugas failover sebagai bagian dari rencana DR Anda.	Lebih tinggi
-------------------------------	-----------	------------------------	---	--------------

Memilih database yang tepat untuk persyaratan RTO dan RPO Anda

Ketika Anda telah menentukan strategi DR untuk organisasi Anda berdasarkan tabel di bagian sebelumnya, pilih database yang sesuai dengan persyaratan RPO dan RTO Anda. Secara default, semua layanan AWS database menyediakan fungsionalitas pencadangan dan pemulihan. Gunakan tabel berikut untuk memahami fitur DR yang lebih canggih yang disediakan oleh layanan AWS database dan memetakannya ke persyaratan DR Anda.

AWS layanan basis data	Metode replikasi ke Wilayah DR	Klasifikasi siaga yang mungkin	RTO	RPO
Amazon RDS for MySQL	Cross-Region baca replika	1. Lampu pilot 2. Siaga hangat dengan kemampuan untuk membaca lalu lintas	Biasanya menit. Otomatisasi dapat meminimalkan penundaan.	Biasanya di bawah 1 detik
Amazon RDS untuk PostgreSQL	Cross-Region baca replika	1. Lampu pilot 2. Siaga hangat dengan kemampuan untuk membaca lalu lintas	Biasanya menit. Otomatisasi dapat meminimalkan penundaan.	Biasanya di bawah 1 detik
Amazon RDS for MariaDB	Cross-Region baca replika	1. Lampu pilot 2. Siaga hangat dengan kemampuan untuk membaca lalu lintas	Biasanya menit. Otomatisasi dapat meminimalkan penundaan.	Biasanya di bawah 1 detik
Edisi Amazon Aurora MySQL-Compatible	Database global memiliki klaster sekunder di	1. Siaga panas dengan kemampuan	Biasanya di bawah 1 menit.	Biasanya di bawah 1 detik

	Wilayah yang berbeda	untuk mendukung lalu lintas baca 2. Siaga hangat dengan kemampuan untuk mendukung lalu lintas baca		
Edisi Amazon Aurora PostgreSQL-Compatible	Database global memiliki kluster sekunder di Wilayah yang berbeda	1. Siaga panas dengan kemampuan untuk mendukung lalu lintas baca 2. Siaga hangat dengan kemampuan untuk mendukung lalu lintas baca	Biasanya di bawah 1 menit.	Biasanya di bawah 1 detik
Amazon DocumentDB (dengan kompatibilitas MongoDB)	Cluster global memiliki cluster sekunder di Wilayah yang berbeda	1. Siaga panas dengan kemampuan untuk mendukung lalu lintas baca 2. Siaga hangat dengan kemampuan untuk mendukung lalu lintas baca	Biasanya di bawah 1 menit.	Dalam hitungan detik

Amazon ElastiCache (Redis OSS)	Datastore global memiliki cluster sekunder di Wilayah yang berbeda	1. Siaga panas dengan kemampuan untuk mendukung lalu lintas baca 2. Siaga hangat dengan kemampuan untuk mendukung lalu lintas baca	Biasanya menit. Otomatisasi dapat meminimal kan penundaan.	Dalam hitungan detik
Amazon DynamoDB	Tabel global DynamoDB	Active/active konfigurasi menerima operasi tulis di Wilayah sekunder	Nol atau mendekati nol.	Sub-second
Amazon RDS for Oracle	Baca promosi replika di seluruh Wilayah (Oracle Enterprise Edition dan Active Data Guard)	1. Lampu pilot 2. Siaga hangat dengan kemampuan untuk membaca lalu lintas	Biasanya menit.	Biasanya di bawah 1 detik
Amazon RDS for Oracle (alternatif)	Promosi replika baca yang dipasang di seluruh Wilayah (Oracle Enterpris e Edition)	1. Lampu pilot 2. Siaga hangat (tidak mengizink an kueri baca)	Biasanya menit.	Biasanya di bawah 1 detik

Amazon RDS for SQL Server	Cross-Region baca replika (Microsoft SQL Server Enterprise Edition 2016-2022)	1. Lampu pilot 2. Siaga hangat dengan kemampuan untuk membaca lalu lintas	Biasanya menit. Otomatisasi dapat meminimalkan penundaan.	Biasanya di bawah 1 detik
Amazon Neptune	Database global memiliki cluster sekunder di Wilayah yang berbeda	1. Siaga panas dengan kemampuan untuk mendukung lalu lintas baca 2. Siaga hangat dengan kemampuan untuk mendukung lalu lintas baca	Biasanya di bawah 1 menit.	Biasanya 1 detik
Amazon RDS untuk Db2	Cross-Region baca replika (Amazon RDS untuk Db2 11.5.9 dan 12.1.4)	1. Lampu pilot 2. Siaga hangat dengan kemampuan untuk membaca lalu lintas	Biasanya menit. Otomatisasi dapat meminimalkan penundaan.	Biasanya di bawah 1 detik
Amazon MemoryDB Multi-Region	Multi-Region cluster dengan replikasi aktif-aktif	Active/active konfigurasi menerima operasi tulis di Wilayah sekunder	Nol atau mendekati nol.	Biasanya di bawah 1 detik

Mendorong adopsi strategi pemulihan bencana Anda

Ketika strategi DR Anda sudah ada, Anda dapat mendorong adopsi strategi di seluruh organisasi Anda. Ketika strategi Anda mencapai adopsi 100 persen, semua aplikasi dan database mereka akan berada dalam posisi untuk menangani peristiwa DR yang merugikan dan dapat mengejar kematangan DR melalui pengujian.

Anda dapat bekerja dengan pemilik aplikasi dan arsitek untuk mendorong adopsi dengan mengkomunikasikan strategi DR di seluruh organisasi Anda dan meminta karyawan untuk mengevaluasi database AWS saat ini yang digunakan dalam aplikasi mereka. Ini memastikan bahwa semua database yang digunakan saat ini dapat memenuhi harapan yang ditetapkan dalam strategi DR. Jika pemilik aplikasi dan arsitek menentukan bahwa database yang mereka pilih untuk aplikasi mereka tidak dapat memenuhi persyaratan strategi DR, mereka harus merencanakan migrasi ke AWS database yang sesuai yang dapat mencapai harapan RTO dan RPO yang dipilih. Misalnya, jika aplikasi penting dalam bisnis Anda yang memerlukan RPO dalam hitungan detik dan RTO dalam hitungan menit saat ini menggunakan instans Amazon RDS for Oracle DB, Amazon RDS tidak akan dapat memenuhi harapan ini. Dalam hal ini, Anda dapat mempertimbangkan untuk memigrasikan beban kerja ke [Amazon PostgreSQL-Compatible](#) Aurora dan menggunakan database global untuk memenuhi harapan yang ditetapkan oleh strategi DR Anda.

Mengotomatiskan strategi pemulihan bencana Anda

Anda dapat memilih untuk menerapkan otomatisasi penuh atau sebagian untuk mendapatkan kontrol yang lebih baik dari pemulihan bencana. Jika Anda menggunakan opsi pencadangan dan pemulihan DR, Anda dapat mengotomatiskan pencadangan dengan menggunakan [AWS Backup](#), yang mendukung semua database Amazon RDS serta tabel DynamoDB, Amazon DocumentDB, dan Amazon Neptune.

Deteksi peristiwa bencana

Untuk mempersingkat waktu pemulihan, Anda dapat mempertimbangkan untuk mengotomatiskan deteksi peristiwa Regionwide, yang kemudian dapat memulai failover ke Wilayah DR. Untuk menerapkan deteksi otomatis untuk mencapai RTO agresif, Anda dapat membangun solusi berdasarkan [pemeriksaan kesehatan](#). Pemeriksaan kesehatan ini tidak berhenti pada detak jantung (yang memeriksa apakah bidang kontrol dan modul bidang data dalam jaringan dapat berkomunikasi satu sama lain), tetapi lebih dalam untuk mengevaluasi sifat komponen aplikasi yang saling terkait untuk mencapai prediksi yang akurat. Namun, solusi otomatis dapat membawa risiko alarm palsu, yang dapat menyebabkan kegagalan yang tidak perlu. Anda harus berhati-hati dalam kasus ini, karena kegagalan yang tidak perlu menimbulkan masalah ketersediaan untuk bisnis Anda. Anda juga dapat membuat penggantian manual dalam alur kerja untuk mengonfirmasi bahwa failover telah dilakukan. Anda dapat berlangganan feed RSS [Service Health Dashboard](#) untuk tetap mendapat informasi tentang gangguan tingkat layanan. Selain itu, Anda dapat menggunakan [AWS Health Dasbor](#) (memerlukan Akun AWS) di Wilayah dan akun utama Anda untuk tetap mengetahui peristiwa yang dapat memengaruhi akun Anda. Ini dapat membantu Anda membuat keputusan berdasarkan informasi untuk gagal dalam kasus suatu Region-wide peristiwa.

Failover

Terlepas dari strategi DR mana yang Anda pilih, Anda dapat membangun solusi otomatisasi DR khusus untuk melakukan failover ke Wilayah DR. Otomatisasi ini dapat meminimalkan kebutuhan akan intervensi manual dan memberikan kontrol yang lebih besar dalam menguji solusi DR Anda. Anda dapat memilih dari [API AWS layanan](#), yang AWS menyediakan dalam berbagai bahasa seperti JavaScript, Python, PHP, .NET, Ruby, Java, Go, Node.js dan C ++, berdasarkan preferensi organisasi Anda. Untuk membangun otomatisasi yang menggunakan API AWS layanan ini, Anda harus terlebih dahulu fokus mengubah infrastruktur database menjadi kode dalam bentuk AWS CloudFormation atau templat Terraform. Template ini dapat membantu Anda mengotomatiskan

failover beberapa database dan juga menjaga urutan aplikasi dan komponen database dibawa kembali di Wilayah DR.

Untuk tujuan DR, kami menyarankan Anda untuk fokus pada dua tujuan ini:

- [CloudFormation Tumpukan yang ada harus mengekspor](#) informasi terkait tentang database Anda, termasuk nama instance dan titik akhir. Proses otomatisasi Anda dapat merujuk ke nilai ekspor ini dalam suatu Wilayah dan melakukan operasi yang akan membantu operasi DR Anda.
- Jika Anda memiliki sumber daya yang sedang diproduksi tetapi tidak memiliki CloudFormation tumpukan terkait, Anda harus fokus pada pembuatan tumpukan untuk sumber daya tersebut. Juga pastikan bahwa tumpukan ini mencakup nilai ekspor yang tepat, seperti yang disebutkan pada poin sebelumnya.

Ketika Anda telah memenuhi dua tujuan ini, Anda dapat membangun solusi otomatisasi dalam bahasa pilihan organisasi Anda untuk memanfaatkan CloudFormation ekspor dan secara otomatis melakukan tindakan pemotongan yang diperlukan jika terjadi bencana. Misalnya, jika Anda memiliki datastore global ElastiCache (Redis OSS) yang digunakan sebagai CloudFormation template, kode otomatisasi memiliki akses ke CloudFormation ekspor yang memberikan rincian tentang datastore global. Jika terjadi bencana, kode dapat secara otomatis mempromosikan datastore sekunder ke datastore primer tanpa intervensi manual dengan menggunakan API layanan ElastiCache (Redis OSS).

Dalam skenario umum, otomatisasi harus dapat diskalakan untuk beberapa database dalam organisasi Anda. Anda dapat menskalakan solusi otomatisasi Anda untuk beberapa database dengan menggunakan [AWS Step Functions](#) atau [AWS Batch](#).

Pengujian untuk mencapai kepercayaan

Solusi DR terbaik untuk database adalah solusi yang sering diuji dan melewati pemeriksaan berikut:

- Pemulihan data yang tepat yang memenuhi harapan RPO untuk setiap database
- Pemulihan lengkap database yang berfungsi dalam kerangka waktu RTO yang diharapkan, yang memungkinkan aplikasi terhubung ke database dan melanjutkan fungsionalitas penuh

Pengujian DR harus menjadi bagian dari strategi bisnis Anda sehingga backup bekerja ketika mereka paling dibutuhkan. Pengujian DR juga harus mengatasi kasus di mana:

- Ukuran database tumbuh secara signifikan, dan strategi DR Anda saat ini tidak lagi memenuhi perjanjian tingkat layanan (SLA) untuk bisnis.
- File cadangan rusak, yang dapat menyebabkan masalah selama pemulihan.

Apa yang harus dipertimbangkan saat menguji strategi DR Anda

- Memiliki tujuan kelangsungan bisnis yang jelas mengenai RPO dan RTO, dan pastikan bahwa hasil tes selaras dengan tujuan Anda.
- Buat rencana pengujian DR terperinci yang memperhitungkan persyaratan keuangan dan sumber daya manusia untuk pengujian.
- Tetapkan sumber daya untuk mendokumentasikan potensi masalah dan pembelajaran.
- Perbarui strategi DR Anda berdasarkan pembelajaran, dan temukan solusi yang mendukung proses dan otomatisasi optimal yang sesuai untuk organisasi Anda.

Frekuensi pengujian untuk solusi DR

Tidak ada rekomendasi yang ditetapkan untuk siklus uji DR, kecuali jika secara eksplisit ditentukan oleh peraturan. Misalnya, audit kepatuhan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) mengharuskan organisasi untuk menguji rencana DR mereka setidaknya setahun sekali. (Lihat [Persyaratan Pemulihan Bencana PCI DSS](#) di situs web PCI DSS.)

Tim aplikasi juga dapat melakukan pengujian berkelanjutan terhadap solusi DR masing-masing ketika aplikasi atau infrastruktur mereka berubah.

Deteksi penyimpangan

Solusi DR Anda juga harus mengelola [deteksi drift](#). Ini akan memastikan bahwa Wilayah utama dan Wilayah DR berada pada tingkat sinkronisasi yang tepat dan akan memastikan kemajuan yang lancar selama pengujian. [AWS Config](#) menyediakan manajemen konfigurasi dan pelacakan riwayat konfigurasi di infrastruktur Anda, dan dapat membantu Anda mengelola drift secara efektif.

Observabilitas

Meningkatkan observabilitas berdampak positif pada persiapan Anda untuk pengujian. Semua solusi DR memindahkan data di Wilayah primer ke Wilayah sekunder (DR). Anda dapat mengatur peringatan untuk kelambatan replikasi dan pencadangan, atau menerapkan proses untuk melakukan pemeriksaan harian yang memastikan bahwa data Anda berhasil disalin ke Wilayah DR.

Langkah dan sumber daya selanjutnya

- Untuk informasi lebih lanjut tentang DR AWS, baca white paper [Disaster Recovery of Workloads on AWS: Recovery in the Cloud](#).
- Tinjau [pilar keandalan](#) dalam AWS Well-Architected Kerangka Kerja.
- Jelajahi [AWS Resilience Hub](#) untuk melacak dan memvalidasi ketahanan beban kerja Anda. AWS
- Tinjau sumber daya tambahan berikut:
 - [Menggunakan failover dalam database global Amazon Aurora](#) (dokumentasi Aurora)
 - [Replikasi di seluruh Wilayah AWS menggunakan datastores global](#) (dokumentasi ElastiCache Amazon (Redis OSS))
 - [Pemulihan Bencana dan Cluster Global Amazon DocumentDB](#) (dokumentasi Amazon DocumentDB)
 - [Bersiaplah untuk pemulihan bencana yang lebih cepat: Menyebarkan database global Amazon Aurora dengan Terraform \(Bagian 1\) \(posting blog\)](#) AWS
 - Tabel [global Amazon DynamoDB](#) (situs web) AWS
 - [Pemulihan Bencana aktif AWS, Cross-Region Replikasi](#) (lab Amazon RDS)
 - [Cross-Region pemulihan bencana Amazon RDS untuk SQL Server AWS](#) (posting blog)
 - [Pemulihan bencana terkelola dengan Amazon RDS for Oracle Cadangan otomatis lintas wilayah - Bagian 1 \(posting blog\)](#) AWS

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini.

Ubah	Deskripsi	Date
Detail yang diperbarui dalam tabel perbandingan	Memperbarui bagian Memilih database yang tepat untuk persyaratan RTO dan RPO Anda .	Juni 29, 2026
Detail yang diperbarui dalam tabel perbandingan	Di bagian Memilih database yang tepat untuk persyaratan RTO dan RPO Anda , memperbarui informasi tentang Amazon RDS untuk Db2, dan memperbaiki detail RPO untuk Amazon RDS for Oracle dan Amazon RDS for Oracle (alternatif).	Juni 11, 2025
Menambahkan Amazon RDS untuk Db2	Di bagian Memilih database yang tepat untuk persyaratan RTO dan RPO Anda , tambahkan informasi tentang Amazon RDS untuk Db2.	Maret 4, 2024
RTO/RPO Detail yang diperbarui	Di bagian Memilih database yang tepat untuk persyaratan RTO dan RPO Anda , memperbarui informasi tentang Amazon DocumentDB, Amazon (Redis OSS), dan ElastiCache Amazon RDS for SQL Server.	19 April 2023
Publikasi awal	—	26 Oktober 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.