10 praktik terbaik keamanan teratas untuk mengamankan cadangan AWS

AWS Panduan Preskriptif

AWS Panduan Preskriptif: 10 praktik terbaik keamanan teratas untuk mengamankan cadangan AWS

Table of Contents

10 praktik terbaik keamanan teratas untuk mengamankan cadangan AWS

Ibukun (IB) Oyewumi, Amazon Web Services ()AWS

Mei 2022 (riwayat dokumen)

Keamanan adalah tanggung jawab bersama antara Amazon Web Services (AWS) dan pelanggan. Pelanggan telah meminta cara untuk mengamankan cadangan mereka. AWS Karena praktik keamanan terus berkembang untuk mengurangi risiko baru, penting bagi Anda untuk melakukan penilaian risiko secara teratur untuk menentukan penerapan kontrol keamanan, dan menerapkan beberapa lapisan kontrol untuk mengurangi risiko pada data Anda.

Dokumen ini akan memandu Anda melalui daftar kurasi dari 10 praktik terbaik keamanan teratas untuk mengamankan data dan operasi cadangan Anda. AWS Meskipun panduan ini berfokus pada data cadangan dan operasi menggunakan AWS Backuplayanan, praktik terbaik keamanan yang direkomendasikan ini dapat digunakan dengan solusi pencadangan lainnya, seperti alat cadangan dari AWS Marketplace.

Praktik terbaik

Saat Anda mengamankan cadangan AWS, sebaiknya gunakan pendekatan berikut:

Topik

Langkah 1. Menerapkan strategi cadangan

Strategi pencadangan yang komprehensif adalah bagian penting dari rencana perlindungan data organisasi untuk menahan, memulihkan, dan mengurangi dampak apa pun yang mungkin dipertahankan karena peristiwa keamanan. Buat strategi pencadangan ekstensif yang menentukan data mana yang harus dicadangkan, seberapa sering data harus dicadangkan, dan bagaimana tugas pencadangan dan pemulihan akan dipantau.

Ketika Anda mengembangkan strategi komprehensif untuk membuat cadangan dan memulihkan data, pertama-tama identifikasi gangguan yang mungkin terjadi, dan potensi dampak bisnisnya.

Tujuan Anda adalah untuk membangun strategi pemulihan yang membawa beban kerja Anda kembali atau menghindari downtime dalam tujuan pemulihan yang dapat diterima, Recovery Time Objective (RTO) dan Recovery Point Objective (RPO). RTO adalah keterlambatan yang dapat diterima antara gangguan layanan dan pemulihan layanan. RPO adalah jumlah waktu yang dapat diterima sejak titik pemulihan data terakhir. Pertimbangkan strategi cadangan granular yang mencakup semua hal berikut:

- Irama cadangan berkelanjutan
- Point-in-Time Pemulihan (PITR)
- Pemulihan tingkat file
- Pemulihan tingkat data aplikasi
- Pemulihan tingkat volume
- Pemulihan tingkat instans

Ransomware

Strategi pencadangan yang dirancang dengan baik harus mencakup tindakan yang dapat melindungi dan memulihkan sumber daya Anda dari ransomware, dengan persyaratan pemulihan terperinci untuk aplikasi Anda dan dependensi datanya. Misalnya, saat Anda membuat kontrol preventif dan detektif untuk mengurangi risiko ransomware, pastikan bahwa Anda juga merancang tingkat perincian yang sesuai untuk pola penyalinan dan pemulihan lintas Wilayah AWS atau lintas akun, untuk memastikan bahwa administrator tidak memulihkan data cadangan yang rusak setelah peristiwa keamanan.

Persyaratan retensi

Di beberapa industri, saat mengembangkan strategi cadangan, Anda juga harus mempertimbangkan peraturan untuk persyaratan penyimpanan data. Pastikan bahwa strategi cadangan Anda dirancang dengan persyaratan retensi yang cukup untuk memenuhi kebutuhan peraturan Anda untuk setiap tingkat klasifikasi data dan jenis sumber daya.

Kepatuhan

Konsultasikan dengan tim kepatuhan keamanan Anda untuk memvalidasi apakah sumber daya dan operasi cadangan Anda harus disertakan atau tersegmentasi dari ruang lingkup program kepatuhan Anda. Menyertakan pencadangan dan pemulihan sebagai bagian penting dari program keamanan Anda akan membantu Anda memahami di mana data berada di seluruh lingkungan Anda dan menentukan cakupan kepatuhan dengan tepat.

Untuk praktik terbaik arsitektur dalam merancang dan mengoperasikan beban kerja yang andal, aman, efisien, dan hemat biaya di cloud, lihat Pendekatan Backup and recovery using AWS and Reliability Pillar — AWS Well-Architected Framework.

Langkah 2. Memasukkan cadangan di DR dan BCP

Disaster recovery (DR) adalah proses mempersiapkan, menanggapi, dan memulihkan diri dari bencana. Bagian penting dari strategi ketahanan Anda, rencana DR menyangkut bagaimana beban kerja Anda merespons ketika bencana melanda. Bencana bisa berupa kegagalan teknis, tindakan manusia, atau peristiwa alam. Business Continuity Plan (BCP) menguraikan bagaimana organisasi bermaksud untuk melanjutkan operasi bisnis normal selama gangguan yang tidak direncanakan.

Rencana DR Anda harus menjadi bagian dari BCP organisasi Anda. BCP juga harus mencakup AWS Backup prosedur. Misalnya, peristiwa keamanan yang memengaruhi data produksi mungkin mengharuskan Anda untuk menjalankan rencana DR yang digunakan AWS Backup untuk gagal untuk mencadangkan data dari yang lain Wilayah AWS. Pastikan karyawan Anda terbiasa dan telah berlatih menggunakan AWS Backup prosedur organisasi Anda, sehingga jika terjadi bencana, organisasi Anda dapat melanjutkan operasi normalnya dengan sedikit atau tanpa gangguan layanan. Informasi lebih lanjut tentang penggunaan AWS Backup disediakan di bagian lain dalam panduan ini.

Langkah 3. Mengotomatiskan operasi pencadangan

Rencana cadangan dan penetapan sumber daya organisasi Anda harus dikonfigurasi untuk mencerminkan kebijakan perlindungan data perusahaan Anda. Dengan mengotomatiskan dan menerapkan kebijakan cadangan atau rencana pencadangan di seluruh organisasi, Anda dapat menstandarisasi dan menskalakan strategi pencadangan Anda. Anda dapat menggunakan AWS Organizationsuntuk mengotomatiskan kebijakan pencadangan secara terpusat untuk menerapkan, mengonfigurasi, mengelola, dan mengatur aktivitas pencadangan di seluruh AWS Backup sumber daya yang didukung dengan menjadwalkan operasi pencadangan.

Untuk meningkatkan produktivitas dan mengatur operasi infrastruktur di lingkungan multi-akun, pertimbangkan untuk menerapkan infrastruktur sebagai kode (IAc) dan arsitektur berbasis peristiwa sebagai bagian penting dari transformasi digital dan strategi pencadangan Anda. Mengotomatiskan cadangan memberikan manfaat berikut:

- Mengurangi overhead manual dari konfigurasi backup yang memakan waktu
- Meminimalkan risiko kesalahan
- Memberikan visibilitas pada deteksi drift
- Meningkatkan kepatuhan kebijakan cadangan di beberapa AWS beban kerja atau akun

Menerapkan kebijakan pencadangan sebagai kode dapat membantu Anda memenuhi peraturan perlindungan data dengan melakukan hal berikut:

- Mengkonfigurasi persyaratan yang berbeda untuk jenis sumber daya Anda
- Menskalakan strategi perlindungan data perusahaan Anda
- Menerapkan aturan siklus hidup untuk menentukan berapa lama sebelum titik pemulihan transisi ke penyimpanan dingin atau dihapus, yang dapat membantu mengoptimalkan biaya Anda

Saat mengotomatiskan operasi pencadangan, Anda dapat menskalakan opsi penetapan sumber daya dengan menggunakan AWS tag dan sumber daya IDs untuk secara otomatis mengidentifikasi AWS sumber daya yang menyimpan data untuk aplikasi penting bisnis Anda dan melindungi data Anda menggunakan cadangan yang tidak dapat diubah. Ini dapat membantu Anda memprioritaskan kontrol keamanan, seperti izin akses dan rencana atau kebijakan cadangan.

Langkah 4. Menerapkan mekanisme kontrol akses

Saat memikirkan keamanan di cloud, strategi dasar Anda harus dimulai dengan fondasi identitas yang kuat untuk memastikan pengguna memiliki izin yang tepat untuk mengakses data. Otentikasi dan otorisasi yang tepat dapat mengurangi risiko kejadian keamanan. Model tanggung jawab bersama mengharuskan AWS pelanggan untuk menerapkan kebijakan kontrol akses. Untuk membuat dan mengelola kebijakan akses dalam skala besar, Anda dapat menggunakan AWS Identity and Access Management (IAM).

Saat mengonfigurasi hak akses dan izin, terapkan prinsip hak istimewa terkecil dengan memastikan setiap pengguna atau sistem yang mengakses data cadangan atau brankas Anda hanya diberikan izin yang diperlukan untuk memenuhi tugas pekerjaan mereka. Gunakan AWS Backup untuk menetapkan kebijakan akses pada brankas cadangan untuk melindungi beban kerja cloud Anda.

Misalnya, dengan menerapkan kebijakan kontrol akses, Anda dapat memberi pengguna akses untuk membuat paket cadangan dan cadangan sesuai permintaan sambil membatasi kemampuan mereka untuk menghapus titik pemulihan. Dengan menggunakan kebijakan akses vault, Anda dapat membagikan brankas cadangan tujuan dengan peran sumber Akun AWS atau IAM, seperti yang dipersyaratkan oleh kebutuhan bisnis Anda. Anda juga dapat menggunakan kebijakan akses untuk berbagi brankas cadangan dengan satu atau beberapa akun, atau dengan seluruh organisasi Anda. AWS Organizations Lihat informasi yang lebih lengkap dalam dokumentasi AWS Backup.

Saat Anda menskalakan beban kerja atau bermigrasi AWS, Anda mungkin perlu mengelola izin secara terpusat ke brankas dan operasi cadangan Anda. Gunakan kebijakan kontrol layanan (SCPs) untuk menerapkan kontrol terpusat atas izin maksimum yang tersedia untuk semua akun di organisasi Anda. SCPs menawarkan pertahanan secara mendalam, dan mereka memastikan bahwa pengguna Anda tetap dalam pedoman kontrol akses yang ditentukan. Untuk informasi selengkapnya, lihat Mengelola akses ke cadangan menggunakan kebijakan kontrol layanan dengan. AWS Backup

Untuk mengurangi risiko keamanan seperti akses yang tidak diinginkan ke sumber daya dan data cadangan Anda, gunakan IAM Access Analyzer untuk mengidentifikasi peran IAM apa pun yang dibagikan dengan yang AWS Backup berikut:

- Entitas eksternal seperti Akun AWS
- Pengguna root
- Pengguna atau peran IAM
- Pengguna gabungan
- Sebuah Layanan AWS
- Pengguna anonim
- Entitas lain yang dapat digunakan untuk membuat filter

Langkah 5. Enkripsi data cadangan dan brankas

Organizations semakin perlu meningkatkan strategi keamanan data mereka, dan mereka mungkin diminta untuk memenuhi peraturan perlindungan data saat mereka menskalakan di cloud. Implementasi metode enkripsi yang benar dapat memberikan lapisan perlindungan tambahan di atas mekanisme kontrol akses dasar. Lapisan tambahan ini memberikan mitigasi jika kebijakan kontrol akses utama Anda gagal.

Misalnya, jika Anda mengonfigurasi kebijakan kontrol akses yang terlalu permisif pada AWS Backup data Anda, sistem atau proses manajemen kunci Anda dapat mengurangi dampak maksimum dari peristiwa keamanan. Ini karena ada mekanisme otorisasi terpisah untuk mengakses data dan kunci enkripsi Anda, yang berarti bahwa data cadangan hanya dapat dilihat sebagai teks sandi.

Untuk mendapatkan hasil maksimal dari AWS Cloud enkripsi, enkripsi data baik dalam perjalanan maupun saat istirahat. Untuk melindungi data dalam perjalanan, AWS gunakan panggilan API yang dipublikasikan untuk mengakses AWS Backup melalui jaringan menggunakan protokol TLS untuk

menyediakan enkripsi antara Anda, aplikasi Anda, dan AWS Backup layanan. Untuk melindungi data saat istirahat, Anda dapat menggunakan AWS cloud-native AWS Key Management Service(AWS KMS) atau. AWS CloudHSM Model keamanan perangkat keras berbasis cloud (HSM), AWS CloudHSM menggunakan Advanced Encryption Standard (AES) dengan kunci 256-bit (AES-256), algoritma yang diadopsi industri yang kuat untuk mengenkripsi data. Evaluasi tata kelola data dan persyaratan peraturan Anda, dan pilih layanan enkripsi yang sesuai untuk mengenkripsi data cloud dan brankas cadangan Anda.

Konfigurasi enkripsi berbeda tergantung pada jenis sumber daya dan operasi cadangan di seluruh akun atau Wilayah. Jenis sumber daya tertentu mendukung kemampuan untuk mengenkripsi cadangan Anda menggunakan kunci enkripsi terpisah dari kunci yang digunakan untuk mengenkripsi sumber daya sumber. Karena Anda bertanggung jawab untuk mengelola kontrol akses untuk menentukan siapa yang dapat mengakses AWS Backup data atau kunci enkripsi vault Anda dan dalam kondisi apa, gunakan bahasa kebijakan yang ditawarkan oleh AWS KMS untuk menentukan kontrol akses pada kunci. Anda juga dapat menggunakan AWS Backup Audit Manager untuk mengonfirmasi bahwa cadangan Anda dienkripsi dengan benar. Untuk informasi selengkapnya, lihat Enkripsi untuk cadangan di. AWS Backup

Anda dapat menggunakan tombol AWS KMSMulti-region untuk mereplikasi kunci dari satu Wilayah ke Wilayah lainnya. Kunci Multi-Region dirancang untuk menyederhanakan manajemen enkripsi ketika data terenkripsi Anda harus disalin ke Wilayah lain untuk pemulihan bencana. Evaluasi kebutuhan untuk menerapkan AWS KMS kunci Multi-region sebagai bagian dari strategi pencadangan Anda secara keseluruhan.

Langkah 6. Lindungi cadangan menggunakan penyimpanan yang tidak dapat diubah

Organizations dapat menggunakan immutable storage untuk menulis data dalam status Write Once Read Many (WORM). Sementara dalam keadaan WORM, data dapat ditulis satu kali, dan dibaca dan digunakan sesering yang diperlukan setelah dilakukan atau ditulis ke media penyimpanan. Penyimpanan yang tidak dapat diubah membantu memastikan bahwa integritas data dipertahankan. Ini juga memberikan perlindungan terhadap hal-hal berikut:

- Menghapus
- Menimpa
- Akses yang tidak disengaja dan tidak sah

- Kompromi ransomware

Penyimpanan yang tidak dapat diubah menawarkan mekanisme yang efisien untuk mengatasi potensi peristiwa keamanan yang mungkin berdampak nyata pada operasi bisnis Anda.

Anda dapat menggunakan penyimpanan yang tidak dapat diubah untuk tata kelola yang lebih baik saat dipasangkan dengan pembatasan SCP yang kuat. Anda juga dapat menggunakan penyimpanan yang tidak dapat diubah dalam mode WORM kepatuhan ketika surat hukum (seperti penahanan hukum) memerlukan akses ke data yang tidak dapat diubah.

Untuk menjaga ketersediaan dan integritas data, Anda dapat menggunakan AWS Backup Vault Lock untuk melindungi cadangan Anda. Saat Anda menggunakan AWS Backup Vault Lock, entitas yang tidak berwenang tidak dapat menghapus, mengubah, atau merusak data pelanggan atau bisnis Anda selama periode penyimpanan yang diperlukan. AWS Backup Vault Lock membantu Anda memenuhi kebijakan perlindungan data organisasi dengan mencegah hal berikut:

- Penghapusan oleh pengguna istimewa (termasuk pengguna root) Akun AWS
- Perubahan pada setelan siklus hidup cadangan Anda
- Pembaruan yang mengubah periode retensi yang ditentukan

AWS Backup Vault Lock memastikan kekekalan dan menambahkan lapisan pertahanan tambahan yang melindungi cadangan (titik pemulihan) di brankas cadangan Anda. Ini sangat berguna dalam industri yang sangat diatur yang memiliki kebutuhan integritas yang ketat untuk cadangan dan arsip. AWS Backup Vault Lock memastikan data Anda disimpan bersama dengan cadangan untuk dipulihkan jika terjadi tindakan yang tidak diinginkan atau berbahaya.

⚠ Important

- AWS Backup Vault Lock belum dinilai sesuai dengan aturan Securities and Exchange Commission (SEC) 17a-4 (f) dan Commodity Futures Trading Commission (CFTC) dalam peraturan 17 C.F.R. 1.31 (b) - (c).
- AWS Backup Vault Lock segera berlaku. Ini memberi Anda periode pendinginan minimum tiga hari (72 jam) untuk menghapus atau memperbarui konfigurasinya sebelum mengunci brankas Anda secara permanen. Anda dapat secara opsional memperpanjang durasi periode pendinginan ini. Gunakan periode pendinginan ini untuk menguji AWS Backup Vault Lock terhadap beban kerja dan kasus penggunaan Anda. Setelah periode

pendinginan Anda berakhir, Anda maupun tidak AWS Dukungan dapat menghapus atau mengubah AWS Backup Vault Lock atau konten brankas Anda yang terkunci. Untuk informasi selengkapnya, lihat dokumentasi tentang AWS Backup Vault Lock.

Langkah 7. Menerapkan pemantauan dan peringatan cadangan

Pekerjaan Backup bisa gagal. Pekerjaan yang gagal, seperti tugas pencadangan, pemulihan, atau penyalinan, dapat berdampak pada langkah selanjutnya dalam suatu proses. Ketika pekerjaan pencadangan awal gagal, ada kemungkinan besar bahwa tugas lain yang berhasil juga akan gagal. Dalam skenario seperti itu, Anda dapat memahami jalannya peristiwa dengan baik melalui pemantauan dan pemberitahuan. Pemantauan dan peringatan dapat memberikan kesadaran organisasi untuk pekerjaan cadangan Anda, yang membantu Anda menanggapi kegagalan cadangan.

Mengaktifkan dan mengonfigurasi notifikasi untuk memantau AWS Backup pekerjaan memberikan manfaat berikut:

- Memberi Anda kesadaran akan aktivitas pencadangan Anda
- Membantu memastikan bahwa Anda memenuhi perjanjian tingkat layanan kritis () SLAs
- Meningkatkan pemantauan Anda business-as-usual
- Membantu Anda memenuhi kewajiban kepatuhan

Anda dapat menerapkan pemantauan cadangan untuk beban kerja Anda AWS Backup dengan mengintegrasikan dengan sistem lain Layanan AWS dan tiket untuk melakukan investigasi otomatis dan alur eskalasi. Misalnya, Anda dapat melakukan hal berikut:

- Gunakan Amazon CloudWatch untuk melacak metrik, membuat alarm, dan melihat dasbor.
- Gunakan Amazon EventBridge untuk memantau AWS Backup proses dan peristiwa.
- Gunakan AWS CloudTrailuntuk memantau panggilan AWS Backup API dengan informasi terperinci tentang waktu, IP sumber, pengguna, dan akun yang melakukan panggilan tersebut.
- Gunakan Amazon Simple Notification Service (Amazon SNS) untuk berlangganan topik AWS Backup terkait seperti backup, restore, dan copy event.

Anda dapat menggunakan AWS Backup Audit Manager untuk secara otomatis menghasilkan bukti laporan audit cadangan harian Anda untuk setiap akun dan Wilayah. Anda juga dapat menskalakan pemantauan cadangan di beberapa akun dengan menggunakan serangkaian templat dan dasbor otomatisasi (dikenal sebagai solusi pengamat cadangan) untuk mendapatkan pelaporan multi-wilayah lintas akun harian agregat. AWS Backup

Langkah 8. Konfigurasi cadangan audit

Untuk memastikan bahwa program cadangan berjalan sebagaimana mestinya dan untuk mengidentifikasi dan memperbaiki anomali apa pun dari proses pencadangan, audit kepatuhan AWS Backup kebijakan terhadap kontrol yang ditentukan seperti frekuensi cadangan yang ditentukan. Untuk menemukan dan menyelidiki operasi cadangan atau sumber daya yang tidak sesuai dengan kebutuhan bisnis Anda, terus dan secara otomatis melacak aktivitas pencadangan Anda dan menghasilkan laporan otomatis.

AWS Backup Audit Manager menyediakan kontrol kepatuhan bawaan yang dapat disesuaikan yang selaras dengan kepatuhan bisnis dan persyaratan peraturan Anda. Anda dapat menggunakan kontrol bawaan dan dapat disesuaikan sebagai kerangka kerja audit untuk mengevaluasi praktik Anda. AWS Backup Kontrol meliputi:

- Sumber daya cadangan dilindungi oleh rencana cadangan
- Frekuensi minimum dan retensi minimum rencana pencadangan
- Titik pemulihan cadangan dienkripsi
- Penghapusan manual titik pemulihan cadangan
- Retensi minimum titik pemulihan cadangan
- Salinan Lintas Wilayah
- Salinan lintas akun
- Kunci Brankas Cadangan

Untuk otomatisasi infrastruktur as-kode (IAc), Anda dapat menggunakan AWS Backup Audit Manager dengan. AWS CloudFormation

AWS Security Hub CSPMmemberi Anda pandangan komprehensif tentang keadaan keamanan Anda di AWS. Ini juga membantu Anda memeriksa lingkungan Anda terhadap praktik terbaik keamanan dan standar industri seperti kontrol Praktik Terbaik Keamanan AWS Dasar. Jika Anda menggunakan

Security Hub CSPM dalam lingkungan cloud Anda, kami sarankan Anda mengaktifkan standar Praktik Terbaik Keamanan AWS Dasar, karena ini mencakup kontrol detektif yang dapat membantu mengamankan cadangan. AWSSebagian besar kontrol detektif di AWS Backup Audit Manager dan Security Hub CSPM juga tersedia sebagai AWS Config aturan terkelola.

Langkah 9. Menguji kemampuan pemulihan data

Strategi pencadangan Anda harus mencakup pengujian cadangan Anda. Strategi pencadangan tidak efektif jika data yang dicadangkan tidak dapat dipulihkan. Uji kemampuan Anda secara teratur untuk menemukan titik pemulihan tertentu dan mengembalikannya.

Meskipun AWS Backup secara otomatis menyalin tag dari sumber daya yang dilindunginya ke titik pemulihan, tag tidak secara default disalin dari titik pemulihan ke sumber daya yang dipulihkan sesuai. Untuk menskalakan manajemen inventaris Anda dan menemukan titik pemulihan, pertimbangkan untuk menggunakan AWS Backup peristiwa untuk memulai proses replikasi tag pada sumber daya yang dibuat dengan AWS Backup memulihkan pekerjaan.

Anda dapat memulai alur kerja pemulihan data Anda dengan menetapkan pola pemulihan data dan kemudian secara teratur mengujinya. Untuk meningkatkan kepercayaan pada kemampuan Anda memulihkan data cadangan, buat proses dasar yang dapat diulang untuk melakukan pengujian pemulihan data berkelanjutan. Misalnya, Anda dapat membuat pola untuk menguji operasi pemulihan lintas akun lintas wilayah dari brankas cadangan DR pusat yang dienkripsi dengan kunci yang dikelola pelanggan ke brankas cadangan akun sumber yang dienkripsi dengan AWS KMS kunci yang dikelola pelanggan yang berbeda. AWS KMS

Jika Anda tidak sering menguji operasi pemulihan seperti itu, Anda mungkin menemukan bahwa asumsi Anda tentang AWS KMS enkripsi untuk operasi lintas akun, lintas wilayah salah. Seringkali, satu-satunya pola pemulihan cadangan yang benar-benar berfungsi adalah jalur yang sering Anda uji. Melalui pengujian rutin jenis sumber daya cadangan yang didukung, Anda dapat melihat peringatan dini yang berpotensi menyebabkan gangguan di masa depan dan hilangnya data penting. Jika memungkinkan, pertahankan jalur dan pola pemulihan dalam jumlah terbatas namun layak untuk mencegah ruang penyimpanan yang terbuang, mengoptimalkan biaya, dan menghemat waktu. Memperbaiki masalah ketika tes pemulihan gagal lebih mudah daripada kehilangan data berharga atau penting.

Langkah 10. Masukkan cadangan dalam rencana respons insiden Anda

Security Incident Response Simulations (SIRS) adalah peristiwa internal yang memberikan kesempatan terstruktur untuk mempraktikkan rencana dan prosedur respons insiden Anda selama skenario realistis. Sangat berharga untuk menguji data cadangan dan operasi Anda dalam aktivitas SIRS kreatif untuk menguji diri Anda terhadap hal-hal yang tidak terduga. Ini membantu Anda memvalidasi kesiapan organisasi Anda dan mengembangkan kenyamanan dengan yang langka dan tak terduga. Simulasi Anda harus realistis, dan mereka harus melibatkan tim organisasi lintas fungsi yang diperlukan untuk menanggapi peristiwa.

Mulailah dengan latihan simulasi dasar, dan bekerjalah menuju acara yang lengkap dan kompleks. Misalnya, Anda dapat membuat model realistis yang terdiri dari virtual private cloud (VPC) dan sumber daya terkait yang mensimulasikan paparan informasi yang tidak disengaja atau potensi pelanggaran data yang disebabkan oleh perubahan kebijakan dan daftar kontrol akses. Untuk mengevaluasi seberapa baik rencana respons insiden Anda bekerja, dokumentasikan pelajaran yang dipetik, dan mengidentifikasi perbaikan yang perlu dilakukan pada prosedur respons masa depan.

Anda dapat menggunakannya AWS Backup untuk menyiapkan pencadangan tingkat instans otomatis sebagai Amazon Machine Images AMIs () dan pencadangan tingkat volume sebagai snapshot di beberapa foto. Akun AWS Ini dapat membantu tim respons insiden Anda meningkatkan proses forensik mereka, seperti pengumpulan disk forensik otomatis, dengan menyediakan titik pemulihan yang dapat mengurangi ruang lingkup dan dampak peristiwa keamanan potensial seperti ransomware.

Langkah selanjutnya

Panduan ini mencakup 10 praktik dan kontrol terbaik keamanan teratas untuk melindungi data cadangan Anda AWS. Sebaiknya gunakan praktik terbaik ini untuk merancang dan menerapkan strategi dan arsitektur pencadangan dan pemulihan, dengan beberapa lapisan kontrol, yang menskalakan dan mencapai kebutuhan bisnis Anda. Untuk informasi selengkapnya AWS Backup, lihat AWS Backup dokumentasi.

Jika Anda memiliki pertanyaan tentang panduan ini, mulailah utas baru di AWS Backupforum atau kontak AWS Dukungan.

Sumber daya

AWS Bimbingan Preskriptif

- Pendekatan Backup dan Recovery pada AWS (panduan)

AWS dokumentasi

- AWS Backup
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon EventBridge
- IAM
- AWS KMS
- AWS Organizations
- AWS Security Hub CSPM
- Amazon SNS

Unggahan blog

- Mengotomatiskan pencadangan terpusat pada skala di seluruh penggunaan Layanan AWSAWS Backup
- Arsitektur Pemulihan Bencana (DR) pada AWS, Bagian I: Strategi Pemulihan di Cloud
- Pentingnya enkripsi dan bagaimana AWS dapat membantu
- Tingkatkan postur keamanan cadangan Anda dengan AWS Backup Vault Lock
- Memantau, Mengevaluasi, dan Menunjukkan Kepatuhan Backup dengan AWS Backup Audit Manager
- Buat dan bagikan cadangan terenkripsi di seluruh akun dan Wilayah menggunakan AWS Backup

- Sederhanakan audit kebijakan perlindungan data Anda dengan AWS Backup Audit Manager
- Mengelola akses ke cadangan menggunakan kebijakan kontrol layanan dengan AWS Backup
- Dapatkan agregat pelaporan multi-wilayah lintas akun harian AWS Backup

GitHub repositori

Repositori kode berikut memberi Anda solusi manajemen dan penerapan untuk menerapkan pencadangan dan pemulihan dengan AWS Backup seluruh AWS Organizations organisasi Anda mencakup beberapa akun dan. Wilayah AWS

- Implementasikan AWS Backup menggunakan AWS
- Implementasikan AWS Backup menggunakan CI/CD Pipelines

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Mei 13, 2022

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