Dokumentasi kegiatan Hari ke-3

Materi

Examine Microsoft Azure Security, Privacy, compliance, and trust

Kelompok 1

Kevin Sundriansyah 535180130

Jeremy Leonardo 535200077

Jeremy Reinhart 535200083

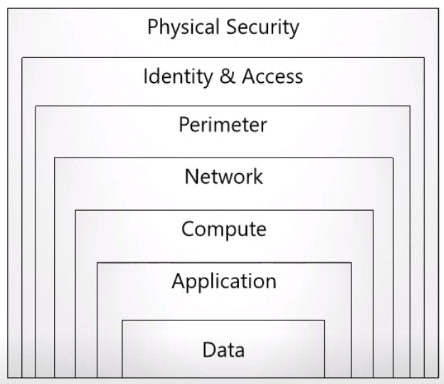
Ruben Eliezer 535200081

Nicko Kurniawan 535200065

* Networking
* Azure Identity
* Security Tools
* Azure Governance, Compliance, and Monitoring

Explore Defense in depth

Sistem security berlaku secara umum menggunakan strategi pertahanan yang berlapis yaitu kita tidak hanya mengandalkan satu sistem pertahanan/benteng jadi dalam setiap layer aplikasi seperti beberapa perusahaan menggunakan internet firewall karena itu sudah cukup untuk mengamankan data-data. Walaupun ada beberapa ancaman kita dapat menerapkan sistem pertahanan seperti ini.



Serangan terhadap keamanan sistem informasi (security attack) dewasa ini seringkali terjadi. Kejahatan computer (cyber crime) pada dunia maya seringkali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan. Ada beberapa kemungkinan tipe dari serangan yang dilakukan oleh penyerang yaitu:

1. *Interception* yaitu pihak yang tidak mempunyai wewenang telah berhasil mendapatkan hak akses informasi
2. *Interruption* yaitu penyerang telah dapat menguasai sistem, tetapi tidak keseluruhan. Admin asli masih bisa login.
3. *Fabrication* yaitu penyerang telah menyisipkan objek palsu ke dalam sistem target
4. *Modification* yaitu penyerang telah merusak sistem dan telah mengubah secara keseluruhan.

Firewall juga dapat memantau informasi keadaan koneksi untuk menentukan apakah ia hendak mengizinkan lalu lintas jaringan. Umumnya hal ini dilakukan dengan memelihara sebuah tabel keadaan koneksi (dalam istilah firewall: state table) yang memantau keadaan semua komunikasi yang melewati firewall. Secara umum Fungsi Firewall adalah untuk:

1. Mengatur dan mengontrol lalu lintas.
2. Melakukan autentikasi terhadap akses.
3. Melindungi sumber daya dalam jaringan privat.
4. Mencatat semua kejadian, dan melaporkan kepada administrator

Jenis Firewall dapat dikelompokan menjadi empat yakni:

1. *Personal Firewall* didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. Firewall jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total misalnya: Microsoft Windows Firewall
2. *Network Firewall* didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server. Misalnya : Internet Security and Acceleration Server (ISA Server), Cisco PIX
3. *IP Filtering Firewall*: Sebuah IP Filtering firewall bekerja pada level paket
4. *Proxy Server*: Cara kerja proxy server, terlihat saat user terhubung dengan proxy server dengan perangkat lunak client, proxy server akan menduplikasi komunikasi tersebut.

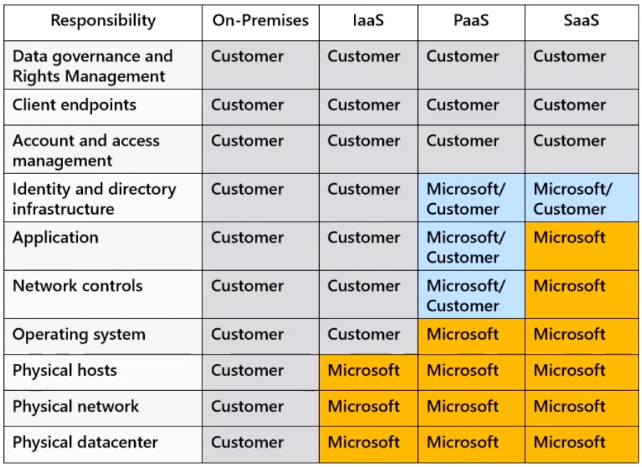
Define Shared security

Penyedia layanan cloud mematuhi model tanggung jawab keamanan bersama, yang berarti tim keamanan kita mempertahankan beberapa tanggung jawab untuk keamanan saat akan memindahkan aplikasi, data, kontainer, dan beban kerja ke cloud, sementara penyedia bertanggung jawab, tetapi tidak semua.

Menentukan batas antara tanggung jawab Anda dan tanggung jawab penyedia Anda sangat penting untuk mengurangi risiko memperkenalkan kerentanan ke lingkungan publik, hybrid, dan multi-cloud Anda.

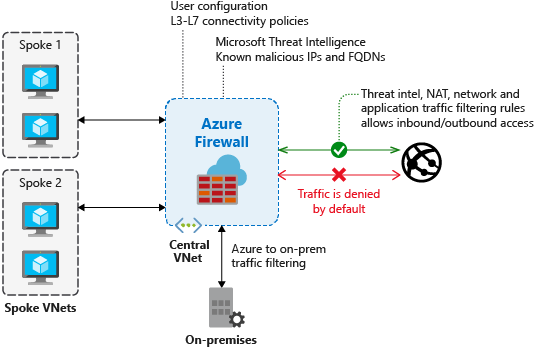
Migrasi dari pusat data yang dikendalikan pelanggan ke pusat data berbasis cloud mengalihkan tanggung jawab atas keamanan. keamanan menjadi perhatian bersama antara penyedia cloud dan pelanggan.

Untuk permasalahan keamanan juga terdapat pembagian antara penyedia layanan(Azure) dan juga pengguna layanan(customer). Yang dapat dilihat sebagai berikut:



Firewall Azure

Azure Firewall adalah layanan keamanan jaringan berbasis cloud terkelola yang melindungi sumber daya Azure Virtual Network Anda. Ini adalah layanan firewall stateful penuh yang dilengkapi dengan ketersediaan tinggi bawaan dan skalabilitas cloud tanpa batas.



Anda dapat membuat, menerapkan, dan mencatat kebijakan konektivitas jaringan dan aplikasi secara terpusat di seluruh langganan dan jaringan virtual. Azure Firewall memberikan alamat IP publik statis untuk sumber daya jaringan virtual Anda, memungkinkan firewall luar mengidentifikasi lalu lintas yang berasal dari jaringan virtual Anda. Layanan terintegrasi penuh dengan Azure Monitor untuk logging dan analitik.

Compare Authentication and authorization

**Authentication** merupakan proses untuk memastikan suatu pengenalan atau memastikan suatu pengakuan. Jadi pada authentication ini akan memastikan siapakah sebenarnya yang telah berinteraksi dengan sistem.

Proses authentication bisa meliputi:

1. Misalnya password

Seseorang yang login dengan suatu username dan password yang hanya dia yang tahu maka dapat dipastikan bahwa orang itu benar-benar login ke sistem

1. kartu akses atas nama dia

Pada suatu perusahaan mungkin dibuatkan suatu kartu akses yang dapat membuka pintu. Jika pintu terbuka maka log mengenai kartu tersebut akan terekam, dan pemiliknya akan disebut sebagai karyawan yang menbuka pintu tersebut

1. Biometric misalnya sidik jari

Setiap karyawan yang yang datang ke kantor pagi hari akan melakukan presensi dengan sidik jari



Sedangkan **Authorization** adalah proses selanjutnya setelah authentication berhasil. Sistem akan memberikan akses sesuai kebijakan yang sudah ditentukan sebelumnya. Di sini sistem akan memberikan batasan akses yang akan diberikan kepada karyawan yang sudah login tersebut. Tentu saja sebelumnya sudah ada rancangan pembatasan akses untuk mencegah terjadinya fraud atau kecurangan dalam perusahaan.

Contoh authorization ini adalah ada karyawan yang login dan dia hanya bisa mengajukan pembayaran kepada vendor. Ada karyawan lain yang login dan dia hanya bisa melakukan persetujuan pembayaran ke vendor. Kemudian ada karyawan yang lain juga yang hanya dapat melakukan pengajuan pembayaran dan karyawan lain yang melakukan pembayaran sesuai pengajuan tadi.

Explore Azure Active Directory (AD)

Layanan manajemen akses dan identitas berbasis cloud Microsoft, yang membantu karyawan Anda masuk dan mengakses sumber daya di: Sumber daya eksternal, seperti Microsoft 365, portal Microsoft Azure, dan ribuan aplikasi SaaS lainnya.

* Autentikasi (employees sign-in untuk mengakses resources)
* Single sign-on (SSO)
* Application management
* Business to Business (B2B)
* Business to Customur (B2C) identity services
* Devices management

Explore Azure Multi-Factor Authentication

multi-factor authentication adalah metode otentikasi atau proses verifikasi pengguna yang hendak mengakses suatu perangkat maupun server. Jika suatu akun dilindungi dengan multi-factor authentication, penggunanya harus memberikan dua atau lebih bukti bahwa ia memang pemilik akun tersebut.

Hanya dengan cara itulah seorang pengguna bisa mendapat akses masuk ke dalam sebuah akun. Bukti untuk memverifikasi dirinya ini bisa berupa macam-macam informasi. Hal itu misalnya nomor HP, alamat email, atau jawaban security question yang biasanya bersifat pribadi dan hanya diketahui oleh pengguna saja sebagai pemilik akun.

Multi-factor authentication tidak hanya muncul ketika akan masuk ke dalam suatu akun, tetapi juga biasanya diminta jika kita terus-menerus gagal untuk menyertakan informasi login yang tepat. Dengan perlindungan ekstra ini, kita bisa lebih tenang dan yakin bahwa akun kita tidak mudah dimasuki oleh orang lain dengan mudah.

Explore Azure Key Vault

Azure Key Vault adalah layanan cloud untuk menyimpan dan mengakses rahasia dengan aman. Rahasia adalah apa pun yang ingin Anda kontrol dengan ketat aksesnya, seperti kunci API, kata sandi, sertifikat, atau kunci kriptografi. Layanan Key Vault mendukung dua jenis kontainer: vault dan kumpulan modul keamanan perangkat keras terkelola (HSM). Vault mendukung penyimpanan perangkat lunak dan kunci, rahasia, dan sertifikat yang didukung HSM. Kumpulan HSM terkelola hanya mendukung kunci yang didukung HSM.

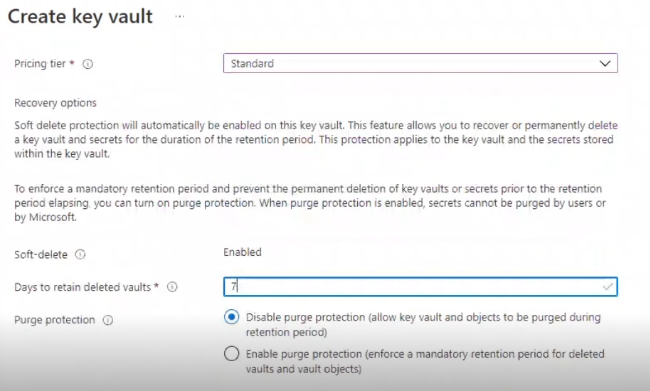
* Secret management
* Key management
* Certificate management
* Storing secrets backed by hardware security modules (HSMs)

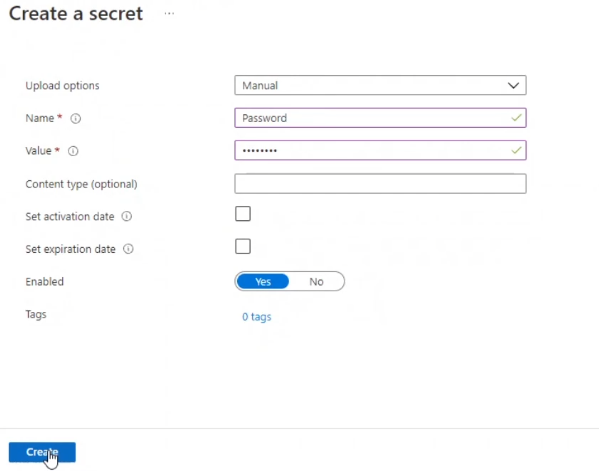
Symmetric Key Encryption:

Enkripsi adalah proses untuk mengubah bentuk pesan apa pun untuk melindunginya agar tidak dibaca oleh siapa pun. Dalam enkripsi kunci-simetris, pesan dienkripsi dengan menggunakan kunci dan kunci yang sama digunakan untuk mendekripsi pesan yang membuatnya mudah digunakan tetapi kurang aman. Ini juga membutuhkan metode yang aman untuk mentransfer kunci dari satu pihak ke pihak lain.

Asymmetric Key Encryption:

Enkripsi Kunci Asimetris didasarkan pada teknik enkripsi kunci publik dan pribadi. Ini menggunakan dua kunci yang berbeda untuk mengenkripsi dan mendekripsi pesan. Ini lebih aman daripada teknik enkripsi kunci simetris tetapi jauh lebih lambat.





Define Azure Information Protection (API)

Azure Information Protection merupakan solusi berbasis cloud yang bertugas mengklasifikasikan dan melindungi dokumen serta email yang tersimpan dalam SharePoint dan Outlook. Azure Information Protection akan mengelompokkan, melabel, dan melindungi data berdasarkan sensitivitasnya. Anda bisa leluasa mengatur dan menetapkan batasan terhadap dokumen maupun tindakan pengguna.

Pengaturan tersebut dapat dilakukan lewat dua cara, yaitu:

* Otomatis, melalui administrator sistem yang sudah menetapkan aturan tertentu sesuai kebutuhan
* Manual, pengaturan dilakukan oleh pengguna sendiri
* Kombinasi dari aplikasi pengguna secara manual dan otomasi dari administrator.

Dengan Azure Information Protection, Anda bisa memilih siapa saja pengguna internal dan eksternal yang memperoleh akses untuk melihat, mencetak, menyalin, serta mengirim dokumen. Azure Information Protection juga memfasilitasi kebutuhan Anda dalam mencabut akses ke suatu dokumen setelah pemberian izin diberlakukan. Tindakan ini dapat dilakukan terjadwal atau manual.

keberadaan AIP akan membantu dalam memahami lebih dalam kapan perlu mendistribusikan suatu konten dan bagaimana menggunakan konten tersebut. Tingkat visibilitas ini akan memudahkan dalam beberapa hal, yaitu:

* Mencegah tindakan modifikasi, penyimpanan, dan distribusi data bisnis penting secara ilegal
* Menghilangkan kemungkinan pengguna tidak terdaftar secara sah dalam sistem untuk melihat konten sensitif
* Mengendalikan seluruh informasi yang ada lewat tindakan pemantauan pengguna, termasuk siapa saja yang berhak mengakses konten dan bagaimana mereka bisa menggunakannya
* Memenuhi standar perlindungan dan kepatuhan regulasi data.

Singkatnya, Azure Information Protection mempermudah Anda melakukan manajemen informasi dalam bisnis. AIP memberikan Anda kontrol besar atas keamanan dan kepatuhan informasi bisnis. Tepatnya lewat tindakan perlindungan yang kuat dengan model klasifikasi dan enkripsi sehingga pengguna tidak perlu repot mengerjakan tugas keamanan yang rumit.

Semua proses izin bisa dibuat otomatis dalam SharePoint. Azure Information Protection dapat memastikan informasi tersebut telah diamankan lewat cara terstruktur dan dapat diprediksi secara otomatis. Pengguna pun bebas membuat, menyimpan, mengatur interaksi, dan mendistribusikan konten secara mudah tanpa perlu pusing dengan isu keamanan.

Define Azure Advanced Threat Protection (Azure ATP)

Advanced Threat Protection menyediakan lapisan keamanan baru, yang memungkinkan pelanggan mendeteksi dan merespons potensi ancaman saat terjadi dengan memberikan peringatan keamanan pada aktivitas anomali. Pengguna menerima peringatan tentang aktivitas basis data yang mencurigakan, potensi kerentanan, dan serangan injeksi SQL, serta akses basis data yang tidak wajar dan pola kueri. Advanced Threat Protection mengintegrasikan peringatan dengan Azure Security Center, yang mencakup detail aktivitas mencurigakan dan merekomendasikan tindakan tentang cara menyelidiki dan mengurangi ancaman. Advanced Threat Protection memudahkan untuk mengatasi potensi ancaman ke database tanpa perlu menjadi ahli keamanan atau mengelola sistem pemantauan keamanan tingkat lanjut.

solusi keamanan berbasis cloud untuk mengidentifikasi, mendeteksi, dan menyelidiki ancaman tingkat lanjut, identitas yang disusupi, dan tindakan orang dalam yang berbahaya.

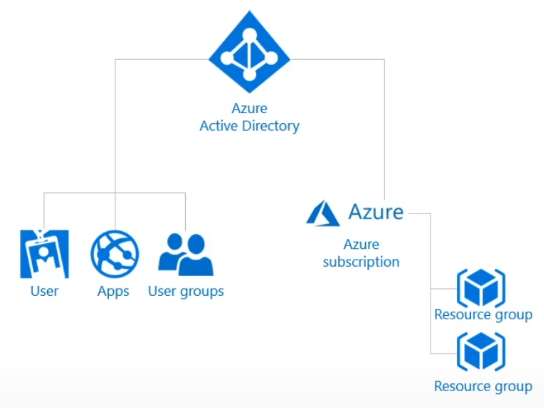
* portal khusus untuk memantau dan menanggapi aktivitas mencurigakan
* sensor dipasang langsung ke pengontrol domain anda
* layanan cloud berjalan di Azure infrastructure

Explore Role-based access control (RBAC)

Dalam RBAC ini kita akan membuat Role untuk masing-masing tingkatan user. Dalam setiap Role ini terdapat berbagai menu yang diberikan kepada Role ini lengkap dengan permissionnya.

Misal Role Admin Purchasing akan mendapatkan menu Purchase Order dengan permission Create. Kemudian Role Purchasing Manager akan mendapatkan menu Purchase Order dan Purchase Request masing-masing dengan permission Approve.

* fine-grained access management
* pisahkan tugas dalam tim Anda dan berikan hanya jumlah akses kepada pengguna yang mereka butuhkan untuk melakukan pekerjaan mereka
* memungkinkan atau melarang akses ke portal Azure dan mengontrol akses ke sumber daya



Define Azure Policy

Azure Policy menetapkan konvensi untuk sumber daya. Definisi kebijakan menjelaskan kondisi kepatuhan sumber daya dan efek yang harus diambil jika kondisi terpenuhi. Kondisi membandingkan bidang properti sumber daya atau nilai dengan nilai yang diperlukan. Bidang properti sumber daya diakses menggunakan alias. Saat bidang properti sumber daya adalah array, alias array khusus dapat digunakan untuk memilih nilai dari semua anggota array dan menerapkan kondisi ke masing-masing array. Pelajari selengkapnya tentang kondisi.

Dengan mendefinisikan konvensi, Anda dapat mengontrol biaya dan mengelola sumber daya Anda dengan lebih mudah. Misalnya, Anda dapat menentukan bahwa hanya jenis komputer virtual tertentu yang diizinkan. Atau, Anda dapat mengharuskan sumber daya untuk memiliki tag tertentu. Penetapan kebijakan diwariskan oleh sumber daya anak. Jika penetapan kebijakan diterapkan ke grup sumber daya, kebijakan tersebut berlaku untuk semua sumber daya dalam grup sumber daya tersebut.

Anda menggunakan JSON untuk membuat definisi kebijakan. Definisi kebijakan berisi elemen untuk:

* nama tampilan
* description
* mode
* metadata
* parameter
* aturan kebijakan
* evaluasi logika
* efek

Azure Policy mengevaluasi sumber daya di Azure dengan membandingkan properti sumber daya tersebut dengan aturan bisnis. Aturan bisnis ini, yang dijelaskan dalam format JSON, dikenal sebagai definisi kebijakan. Untuk menyederhanakan manajemen, beberapa aturan bisnis dapat dikelompokkan bersama untuk membentuk inisiatif kebijakan (kadang-kadang disebut sebagai policySet). Setelah aturan bisnis Anda terbentuk, definisi atau inisiatif kebijakan ditetapkan ke cakupan sumber daya apa pun yang didukung Azure, seperti grup manajemen, langganan, grup sumber daya, atau sumber daya individu. Penugasan berlaku untuk semua sumber daya dalam Cakupan Resource Manager dari penugasan tersebut.

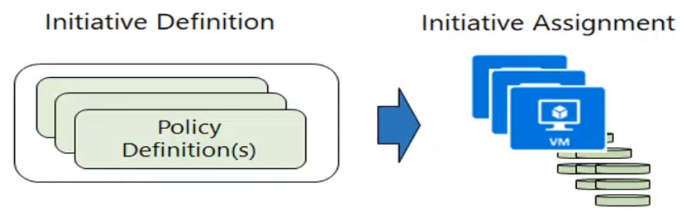
Jadi Azure Policy adalah layanan untuk membuat, menetapkan, dan mengelola kebijakan. kebijakan ini memberlakukan aturan dan efek yang berbeda atas sumber daya Anda, sehingga sumber daya tersebut tetap sesuai dengan standar perusahaan dan perjanjian tingkat layanan (SLAs) Anda

Implementing Azure Policy



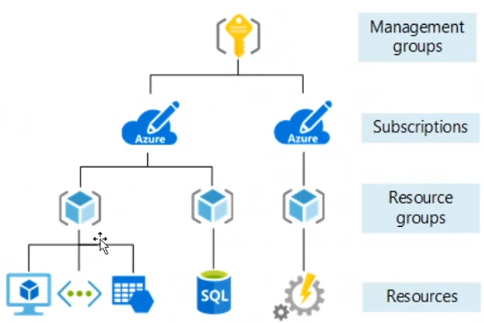
definisi kebijakan mengungkapkan apa yang harus dievaluasi dan tindakan apa yang harus diambil. menerapkan definisi kebijakan Anda dengan menetapkannya ke sekelompok sumber daya. meninjau hasilnya. hasilnya sesuai atau tidak sesuai.

Define Polity Initiatives

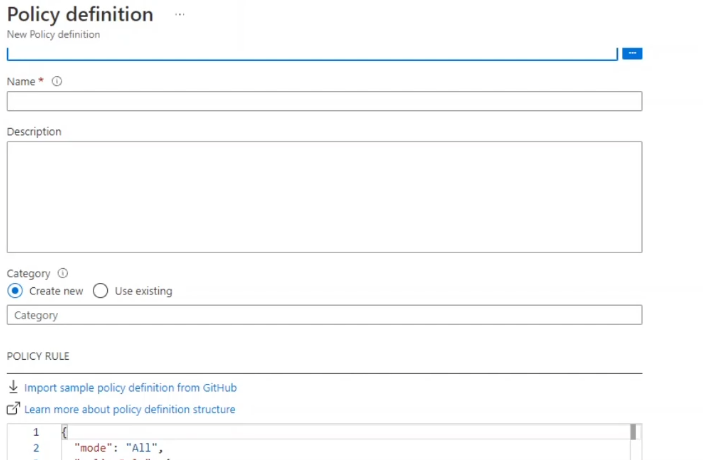


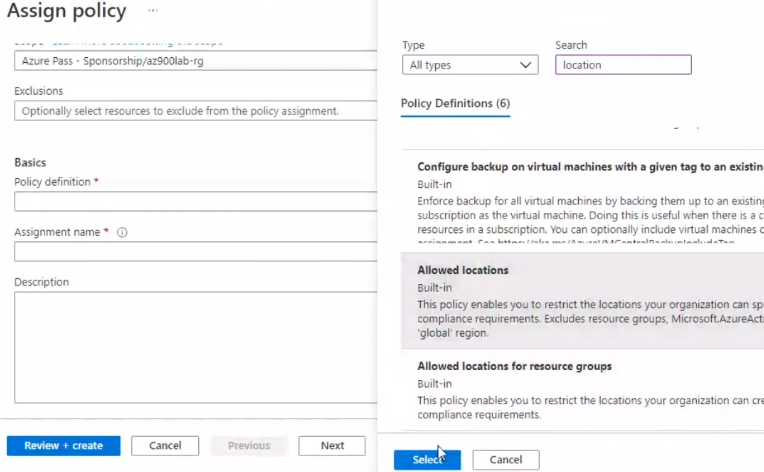
Policy Initiatives work with Azure Policies

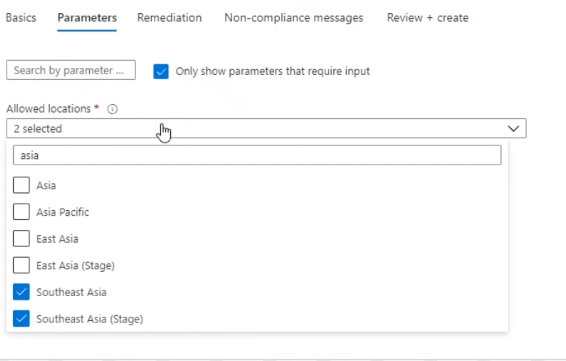
* **Initiative definitions** mengelompokkan beberapa definisi kebijakan ke dalam satu unit, untuk melacak kepatuhan pada cakupan yang lebih tinggi. misalnya, satu inisiatif dapat memantau semua Anda
* **Initiative assignments** ditugaskan ke ruang lingkup sosial dan mengurangi kebutuhan untuk membuat definisi inisiatif untuk setiap ruang lingkup.



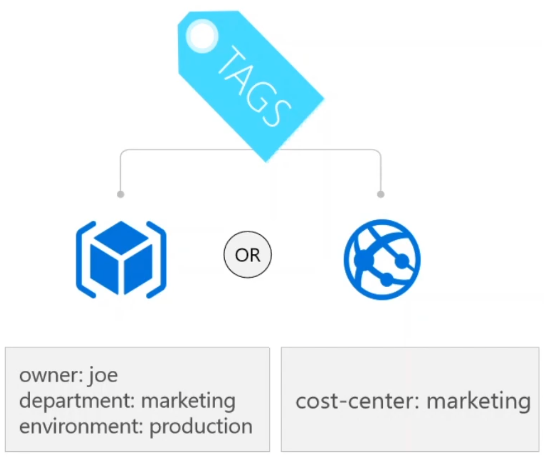
Mengimplemen policy







Explore Tags



* menyediakan metadata untuk Azure resources anda
* secara logis mengatur sumber daya menjadi taksonomi
* terdiri dari pasangan nama-nilai
* sangat berguna untuk menggulung informasi penagihan

Explore Azure Monitor

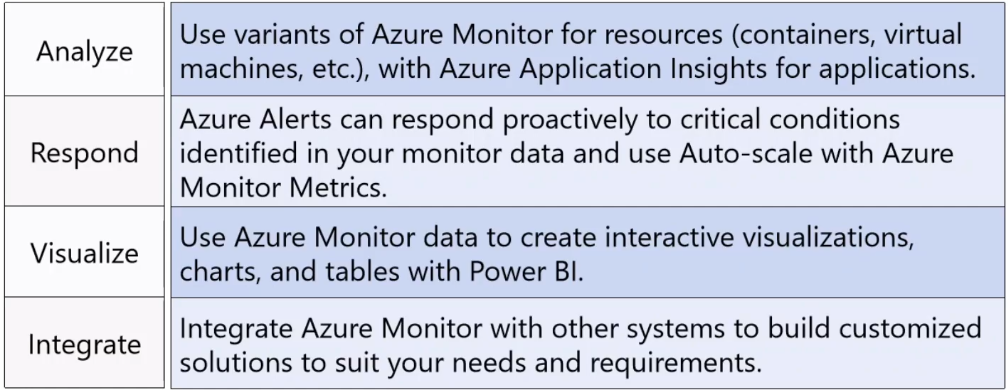
mengumpulkan, menganalisis, dan bertindak berdasarkan telemetri dari cloud dan lingkungan lokal, untuk memaksimalkan ketersediaan dan kinerja aplikasi Anda

Explore Azure Service Health

mengevaluasi dampak masalah layanan Azure dengan panduan dan dukungan yang dipersonalisasi, pemberitahuan, dan pembaruan resolusi masalah

Monitor applications and services

Proses monitoring yang sifat mengulang



Explore Trust Center

Tentang keamanan, privacy, compliance, plicies, fitur-fitur, dan practices across Microsoft’s cloud products

The Trust Center website provides:

* Informasi ahli yang mendalam
* Daftar sumber yang direkomendasikan, disusun berdasarkan topik
* informasi peran khusus untuk administrator orang lain di organisasi yang mungkin berperan dalam keamanan, privasi, dan kepatuhan. Orang-orang ini termasuk manajer bisnis, petugas penilaian risiko dan privasi, tim kepatuhan hukum, dll.

Explore Service Trust Portal (STP)

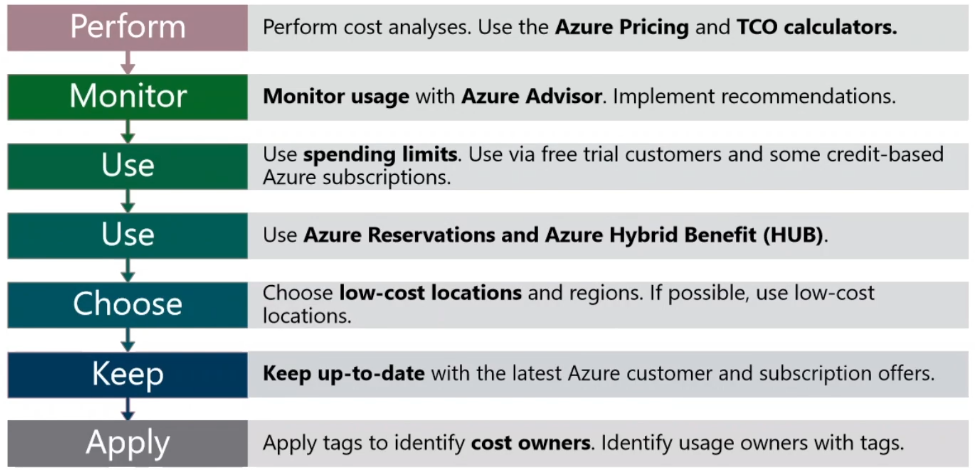
STP berisi detail tentang penerapan kontrol dan proses Microsoft yang melindungi layanan cloud kami dan data pelanggan di dalamnya. Untuk mengakses beberapa sumber daya di Portal Kepercayaan Layanan, Anda harus masuk sebagai pengguna yang diautentikasi dengan akun layanan cloud Microsoft Anda (akun organisasi Azure Active Directory atau Akun Microsoft) dan meninjau serta menerima Perjanjian Non-Disclosure Microsoft untuk Materi Kepatuhan.

STP untuk mengakses:

* Laporan audit di seluruh layanan cloud Microsoft
* Panduan untuk menggunakan layanan Microsoft Cloud untuk kepatuhan terhadap peraturan
* Publikasi tentang kepercayaan, dan bagaimana layanan Microsoft Cloud melindungi data Anda

Explore Minimizing costs

Minimisasi biaya adalah aturan dasar yang digunakan oleh produsen untuk menentukan campuran tenaga kerja dan modal apa yang menghasilkan output dengan biaya terendah. Dengan kata lain, apa metode pengiriman barang dan jasa yang paling hemat biaya dengan tetap mempertahankan tingkat kualitas yang diinginkan. Seperti di bawah:



Define Service Level Agreements (SLAs)

Service Level Agreement (SLA) merupakan bagian integral dari kontrak vendor mana pun. Selain mencantumkan ekspektasi kualitas dan jenis layanan, SLA menawarkan perbaikan ketika satu pihak gagal memenuhi semua persyaratan yang disebutkan.

SLA adalah kontrak atau kesepakatan antara perusahaan dan penyedia layanannya yang menyatakan secara rinci harapan dan kewajiban hubungan tersebut. Ada beberapa keuntungan bekerja sama dengan penyedia layanan, tetapi untuk mendapatkan hasil maksimal dari jenis kemitraan ini, SLA harus diterapkan. SLA bertindak sebagai blueprint layanan yang disediakan vendor dan dapat melindungi aset dan reputasi perusahaan.

sebagian besar terdiri dari bagian serupa yang mencakup semua area hubungan client / mitra:

* Services

Bagian ini mencakup manfaat yang diberikan vendor. Misalnya, penyedia internet memberi pengguna akses ke ketersediaan internet dan layanan terhubung lainnya. Bagian layanan berisi spesifik dari semua layanan yang disediakan, kondisi ketersediaan layanan, tanggung jawab masing-masing pihak, prosedur eskalasi, standar (seperti jendela waktu untuk setiap tingkat layanan), dan pengorbanan biaya / layanan.

* Measurement

Bagian pengukuran digunakan untuk metrik yang mengukur komitmen layanan. Bagian pengukuran biasanya memiliki catatan yang menyoroti indikator kinerja utama, standar khusus, dan metode untuk mengukur kinerja, frekuensi, dan detail pelaporan.

* Intervals

Semua SLA harus memiliki bagian yang menguraikan lamanya waktu perjanjian diberlakukan dan interval di mana kontrak diaudit dan dinegosiasikan ulang.

* Obligations

Beberapa SLA memiliki kewajiban yang harus dipenuhi vendor dan pelanggan selama jangka waktu SLA agar perjanjian dapat diberlakukan. Ketika kewajiban ini tidak dipenuhi karena alasan apa pun, biasanya pelanggaran SLA akan diklaim, memungkinkan pelanggan untuk menggunakan hak mereka untuk menerima biaya penalti dari vendor.

* Penalties

Bagian hukuman menguraikan konsekuensi jika gagal mematuhi komponen kewajiban SLA.

Manfaat SLA (Service Level Agreement)

Berikut adalah beberapa manfaat yang dapat disediakan SLA untuk hubungan penyedia layanan baru dan berkelanjutan.

* Mereka menetapkan pedoman yang jelas. SLA penting untuk memastikan kedua belah pihak berada di halaman yang sama dalam hal standar dan layanan. Dengan membuat perjanjian tingkat layanan, vendor dan client memiliki metode yang terdokumentasi dengan jelas untuk bekerja melalui harapan bersama mereka. Membuat pedoman yang jelas dan terukur diperlukan karena menurunkan kemungkinan mengecewakan client dan menawarkan bantuan kepada klien jika kewajiban tidak dipenuhi. SLA menyediakan jalan lain untuk kewajiban yang terlewat. Jika vendor gagal memenuhi kewajibannya, harus ada konsekuensi. Dalam SLA, penalti dapat dan harus didefinisikan sebagai prosedur garis besar jika salah satu pihak gagal memenuhi standar kinerja. Hukuman moneter ini dapat membantu perusahaan Anda jika terjadi kerugian, dan juga melindungi kepentingan terbaik client dan vendor.
* Ini memberi ketenangan pikiran kepada client. Mereka memiliki kontrak yang dapat mereka rujuk yang memungkinkan mereka untuk meminta pertanggungjawaban vendor mereka. Ini juga merinci jenis layanan yang akan mereka dapatkan. Jika kebutuhan tidak terpenuhi, mereka dapat mengurangi beberapa dampak dengan memberikan kompensasi uang melalui penyedia mereka. Bagi banyak perusahaan, ini adalah jaminan yang mereka butuhkan untuk memulai hubungan dengan mitra yang belum pernah mereka tangani sebelumnya.
* SLA juga menciptakan peluang bisnis baru. Dalam banyak kasus, client akan meninggalkan vendor jika mereka merasa tidak mendapatkan perhatian pribadi yang cukup. Calon client sering kali mencari untuk memulai hubungan profesional baru karena mereka telah mengalami layanan buruk dari penyedia layanan lain dan sedang mencari mitra yang dapat memenuhi kebutuhan mereka dengan lebih baik. Akibatnya, memanfaatkan SLA bisnis dapat menjadi alat penjualan yang ampuh. Dengan mengatasi kesenjangan umum dalam perjanjian SLA dan menciptakan transparansi dalam hubungan, perusahaan jasa dapat dengan cepat mengatasi masalah umum client potensial dan secara jelas menguraikan bagaimana mereka akan memastikan standar layanan yang tinggi.

Memiliki SLA dapat saling menguntungkan bagi calon client yang mencari layanan dan penyedia terkelola.