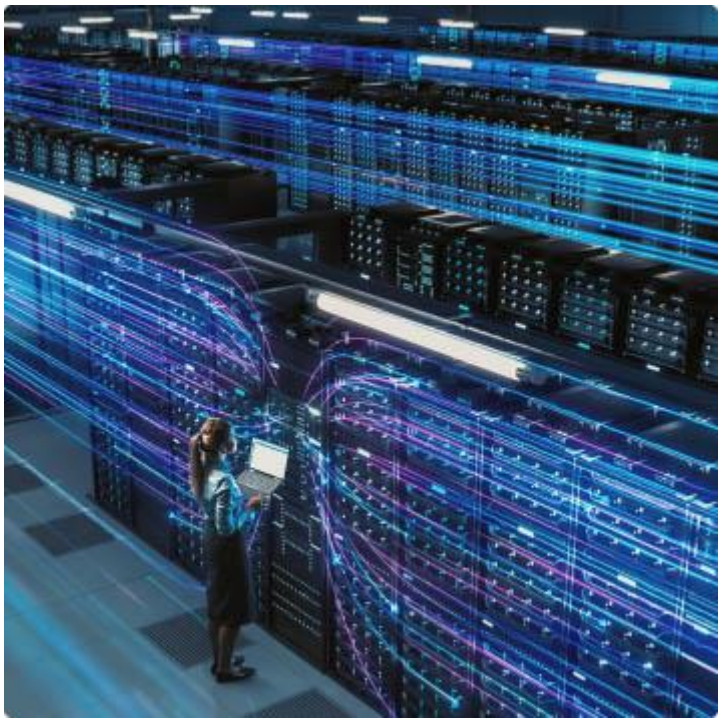
Serviço de Máquinas Virtuais

Já vimos, pela categorização atribuída pelo NIST para os tipos de serviços em nuvem, que infraestruturas, plataformas, softwares ou tecnologias acessadas pelos clientes a partir da internet, sem a necessidade de fazer download de nenhum outro software, podem ser considerados **serviços de computação em nuvem**. Veremos de forma mais específica alguns serviços associados às camadas de computação, armazenamento, rede, monitoramento e auditoria.



Falando sobre serviços em nuvem, especificamente para IaaS, o recurso mais comum e básico é a **computação**, que engloba desde as tradicionais máquinas virtuais (VMs), passando por bancos de dados gerenciados (executados nas VMs no back-end), até arquiteturas de computação mais modernas, conhecidas como **contêineres** e, eventualmente, arquiteturas que usam funções como serviço (abordagem conhecida como serverless).

Cada provedor na nuvem implementa as VMs de uma maneira diferente; porém, todas guardam a mesma ideia básica em comum com o cliente executando os passos a seguir.

1. Selecionar um tipo de máquina, normalmente caracterizada pelo tamanho, uma proporção entre a quantidade de CPU virtual (vCPU) e memória, de acordo com seus requisitos (uso geral, otimizado para computação, otimizado para memória e assim por diante).

2. Selecionar uma imagem pré-instalada de um sistema operacional (variando normalmente entre uma versão do Windows ou distribuições do Linux).
3. Configurar a parte de armazenamento (adicionando volumes adicionais, conectando-se a serviços de compartilhamento de arquivos e outros).
4. Definir as configurações de rede (desde controles de acesso à rede até microssegmentação de áreas dentro dela).
5. Configurar permissões para acessar cada um dos recursos da nuvem.
6. Implantar seus próprios aplicativos.
7. Ligar todos os serviços e começar a usar.
8. Fazer a manutenção contínua do sistema operacional, aplicando patches de atualização.

Serviço de Conteinerização

Vamos descrever brevemente o que é um contêiner. Podemos dizer que se trata de uma evolução da máquina virtual, devido às similaridades em termos de comportamento, porém, são extremamente mais enxutos e leves em termos de uso de recursos de computação. É uma abordagem de virtualização que busca implantar e executar aplicativos distribuídos.

Um contêiner contém tudo que é necessário para a execução da aplicação, como arquivos, variáveis de ambiente e bibliotecas próprias. Por meio dessa abordagem de virtualização, podem ser acionados vários contêineres (aplicativos distribuídos) em um único host, acessando um único kernel, ou seja, sem a necessidade de uma VM para cada aplicação. A leveza dessa abordagem propicia facilidades de escala, com os benefícios da computação em nuvem.

Em vez de precisar implantar um aplicativo rodando sobre um sistema operacional inteiro, você pode usar contêineres para implantar o aplicativo necessário, com apenas as bibliotecas e os binários mínimos do sistema operacional. Os contêineres têm os seguintes benefícios em relação às VMs:

Portabilidade

Um aplicativo pode ser desenvolvido dentro de um contêiner em uma máquina caseira e executado em grande escala em um ambiente de produção com centenas ou milhares de instâncias de contêiner.

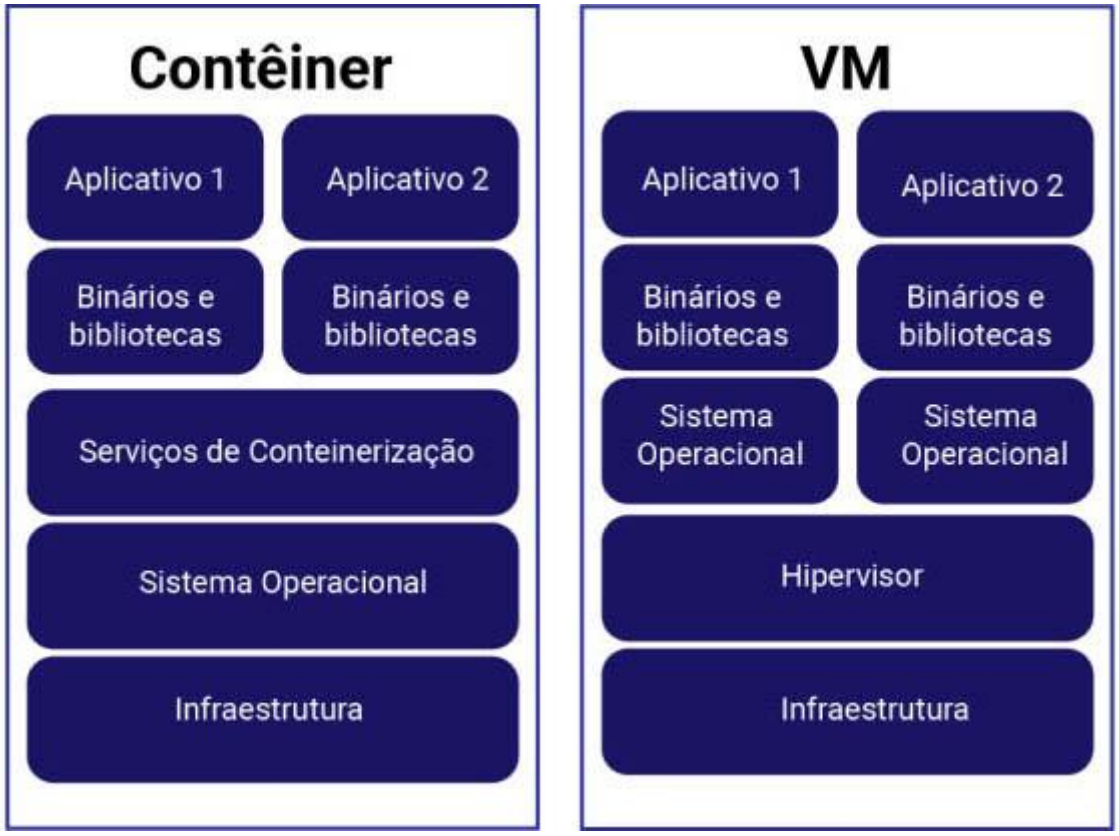
Espaço reduzido

Apenas as bibliotecas e os binários necessários são armazenados dentro de um contêiner.

Velocidade

As implementações e atualizações são mais rápidas se comparadas com as VMs.

A imagem a seguir apresenta as diferenças de arquitetura entre contêineres e VMs.



Comparação entre contêiner e máquina virtual.

Ainda na fase de desenvolvimento, é possível instalar um serviço de contêiner em uma máquina caseira, criar um novo contêiner (ou baixar um existente) e concluir todo o desenvolvimento localmente. Passando para a produção, com um orquestrador (serviço de conteinerização) é possível executar centenas de instâncias do contêiner. O serviço é autogerenciado para implantação, monitoramento e verificação de integridade, reciclagem de contêineres e muito mais. Veja a seguir as características do Docker e do Kubernetes.

Docker

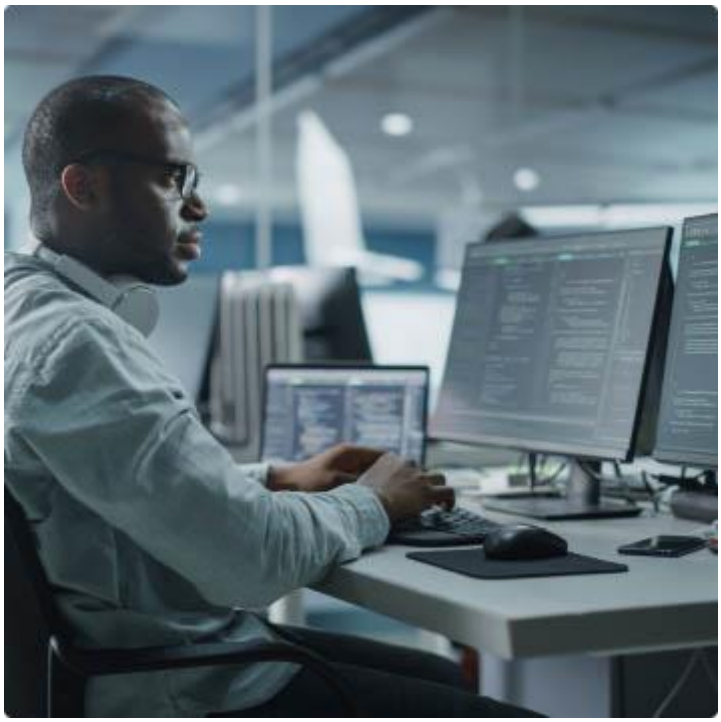
Foi adotado pela indústria como um padrão, de fato, para encapsular contêineres e, nos últimos anos, mais e mais fornecedores de nuvem começaram a oferecer suporte a uma nova iniciativa para encapsular contêineres, chamada Open Container Initiative (OCI).

Kubernetes

É um projeto de código aberto (desenvolvido originalmente pela Google) e agora está se popularizando no setor de computação em nuvem para orquestrar, implantar, dimensionar e gerenciar contêineres.

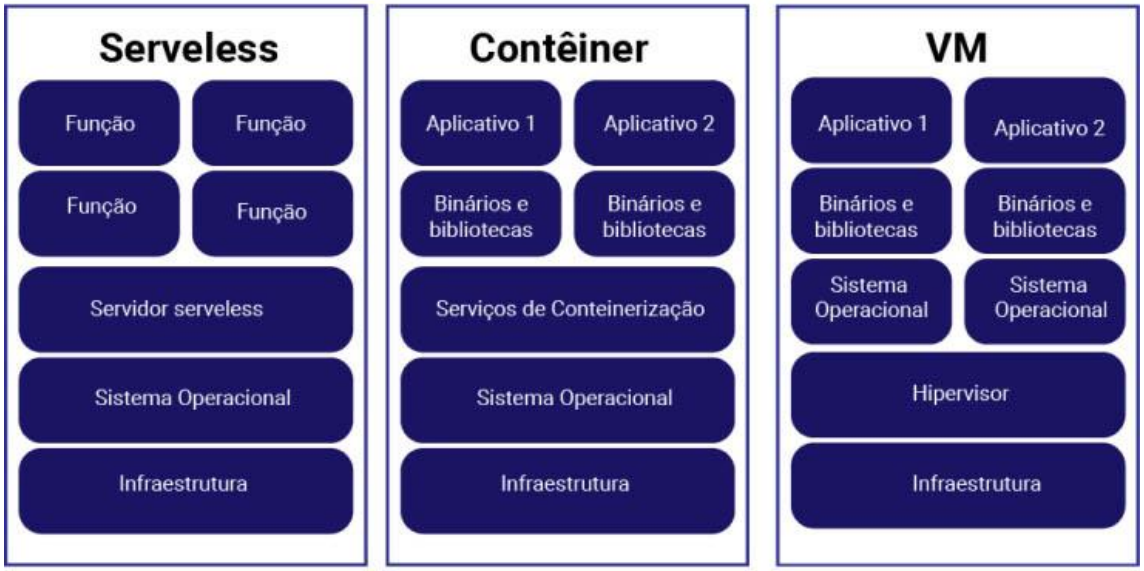
Funções como Serviço (abordagem serverless)

Embora o nome dê a entender que não há servidores, o termo serverless ou "função como serviço" significa que o cliente do serviço de nuvem não é responsável pela infraestrutura de computação subjacente, isto é, manutenção do sistema operacional, escala, gerenciamento de tempo de execução, e assim por diante.



Por intermédio dessa abordagem, basta importar um código com sintaxe de acordo com o provedor do serviço de nuvem, selecionar o interpretador, selecionar a quantidade de CPU e memória necessárias para rodar a função e definir o gatilho para invocar a função. Podemos dizer que o serverless é orientado a eventos, permitindo que os desenvolvedores criem, executem e gerenciem pacotes de aplicações como se fosse funções.

A imagem a seguir apresenta um diagrama esquemático que mostra as similaridades e diferenças da abordagem serverless para os já mencionados esquemas de implementação por contêiner e máquina virtual.



Comparação entre serverless, contêiner e máquina virtual.

Alguns provedores classificam essa abordagem como um novo tipo de serviço, diferente da categorização estabelecida pelo NIST. Nesse caso, além dos tipos IaaS, PaaS e SaaS, haveria o FaaS, isto é, função como serviço.

Serviço de Base de Dados Gerenciadas

Mais uma vez, para sermos precisos, é preciso esclarecer que cada provedor tem sua própria forma de implementação de bases de dados gerenciadas.

De forma geral, quando o cliente tem a necessidade de implantar uma compilação específica de um banco de dados, isso pode ser feito dentro de uma VM. Porém, de acordo com o modelo de responsabilidade compartilhada, se o cliente partiu para uma abordagem usando base de dados gerenciada, significa que o cliente “fugiu” do modelo IaaS. Nesse caso, o provedor do serviço de nuvem supervisiona a segurança de todo o sistema operacional e do banco de dados (incluindo hardening, backup, gerenciamento de patches, monitoramento e auditoria).

Então, uma solução gerenciada para executar um banco de dados – seja ele do tipo mais comum, como MySQL, PostgreSQL, Microsoft SQL Server, um servidor de banco de dados Oracle ou bancos de dados proprietários, como Amazon DynamoDB, Azure Cosmos DB ou Google Cloud Spanner – emprega basicamente o mesmo conjunto geral de passos a serem realizados pelo cliente.

- Selecionar o tipo de banco de dados de acordo com sua finalidade ou caso de uso (banco de dados relacional, banco de dados NoSQL, banco de dados gráfico, banco de dados em memória, dentre outros).
- Selecionar o banco de dados (por exemplo, MySQL, PostgreSQL, Microsoft SQL Server ou servidor de banco de dados Oracle).
- No caso de bancos de dados relacionais, selecionar um tipo de máquina (ou tamanho) e uma proporção entre a quantidade de vCPU e memória, de acordo com seus requisitos (uso geral, otimização de memória e assim por diante).
- Decidir, de acordo com suas necessidades, se há exigência de alta disponibilidade.
- Implementar uma instância do banco de dados gerenciada (ou cluster).
- Configurar o controle de acesso à rede do seu ambiente de nuvem para seu banco de dados gerenciado.
- Ativar o registro (em logs) para qualquer tentativa de acesso ou alterações de configuração em seu banco de dados gerenciado.
- Configurar backups em seu banco de dados gerenciado para fins de recuperação.
- Conectar seu aplicativo ao banco de dados gerenciado e começar a usar o serviço.

Vários podem ser os motivos para se optar pelo uso de um serviço de banco de dados gerenciado em detrimento de simplesmente provisionar uma VM e instalar tudo lá dentro. Dentre essas vantagens, podemos destacar:

- A manutenção do banco de dados é de responsabilidade do provedor de nuvem.
- A atualização de patches de segurança é de responsabilidade do provedor de nuvem.
- A disponibilidade do banco de dados é de responsabilidade do provedor de nuvem.
- Os backups estão incluídos como parte do serviço (até certa quantidade de armazenamento e de histórico de backup) de acordo com planos oferecidos.
- A criptografia do tráfego e dos dados armazenados são incorporadas como parte da solução gerenciada.

- A auditoria também é incorporada como parte de uma solução gerenciada, como registro de logs e monitoramento oferecido pelo provedor.

Serviço de Armazenamento

Outro serviço comumente oferecido nos serviços em nuvem é o **armazenamento (storage)**. Os serviços apresentados até então neste conteúdo guardam relação com recursos de computação. Storage diz respeito a um recurso de armazenamento e, normalmente, se divide em três categorias: file storage, object storage e block storage (que vamos traduzir aqui respectivamente como armazenamento de arquivo, armazenamento de objeto e armazenamento de bloco).

Todos se prestam a armazenar os dados do cliente em diferentes formatos e estão sujeitos, de maneira geral, às seguintes ameaças de segurança:

- Acesso não autorizado;
- Vazamento de dados;
- Exfiltração de dados;
- Perda de dados.

Existe outra categoria mais moderna de serviço de armazenamento, chamada de **Container Storage Interface**, conhecida pela sigla CSI.Para todos os serviços de armazenamento, considerando as principais ameaças apresentadas, existem contramedidas a serem empregadas, como veremos a seguir.

Lista de controle de acesso

Conhecidas nos provedores pela sigla ACL.

Gerenciamento de acesso e identidade

Conhecida em alguns provedores como IAM, sigla sugestiva que passa a ideia de identidade. Assim como a ACL, busca restringir o acesso ao serviço de armazenamento no ambiente da nuvem.

Criptografia

Conhecida tanto nos dados em trânsito como nos dados armazenados, busca assegurar confidencialidade.

Auditoria

Feita a partir de registro de logs de acesso sobre quem, quando e que ações foram executadas sobre os dados armazenados (por exemplo, uploads, downloads, modificações, apagamentos etc.).

Backups

Conhecidos por permitirem resgate de dados apagados, alterados ou, ao menos, retorno para uma versão anterior do dado.

Os armazenadores de objeto são um tipo especial de armazenamento destinado a armazenar dados. Os objetos (ou arquivos) são armazenados em buckets, que podem ser compreendidos como um conceito lógico similar ao conceito de algo de conhecimento mais amplo, diretórios. O acesso a arquivos nos armazenadores de objeto é feito por meio de Application Programming Interface (API) no protocolo HTTPS, com linha de comando ou interface específica, dependendo do provedor. Esses armazenadores não se destinam a armazenar sistemas operacionais ou bancos de dados.

Comentário

O armazenamento em bloco é um esquema de armazenamento como Storage Area Network (SAN) local. Oferece ao cliente funcionalidade para que ele monte um volume (disco), formate-o em um sistema de arquivos comum (como NTFS para Windows ou Ext4 para Linux, por exemplo) e armazene vários arquivos, bancos de dados ou sistemas operacionais inteiros.

O armazenamento de arquivos é um tipo de armazenamento similar ao **Network-attached Storage** (NAS) local. Oferece suporte para protocolos comuns de compartilhamento de arquivos (como NFS e SMB/CIFS). Tem a capacidade de montar um volume de um serviço de arquivo gerenciado em um sistema operacional para armazenar e recuperar arquivos paralelamente para várias VMs e de controlar as permissões de acesso ao sistema de arquivos remoto. Além disso, permite o crescimento automático do sistema de arquivos de forma transparente para o usuário.

Finalizando sobre o serviço de armazenamento, descrevemos o tipo CSI. De forma simples, podemos dizer que um CSI é um driver padrão para conectar sistemas de orquestração de contêineres, como Kubernetes, a fim de bloquear e armazenar arquivos de vários provedores de nuvem.Os provedores de serviço de nuvem mais citados, AWS, Azure e GCP, possuem serviços de armazenamento de arquivos, objetos, blocos e contêineres.

Serviço de Rede

Outra classe de serviços em nuvem são os associados ao recurso rede, tais como:

- Domain Name System (DNS);
- Content Delivery Network (CDN);
- Virtual Private Network (VPN);
- Web Application Firewall (WAF);
- Proteção Distributed Denial of Service (DDoS protection).

Dentro de uma infraestrutura de nuvem, as redes são configuradas virtualmente, o que é conhecido como virtual networking. As redes virtuais dão poder para o cliente realizar configurações específicas. Porém, com essa abordagem, criam um desvio no modelo comum de responsabilidade compartilhada, uma vez que tornam a responsabilidade pela segurança da rede algo dividido entre cliente e provedor.

A camada física da rede permanece sob encargo do provedor, mas a camada que possibilita o acesso entre servidores virtuais, serviços de armazenamento e bancos de dados gerenciados fica a cargo do cliente.

Os serviços gerenciados de DNS incluem funcionalidade para traduzir nomes de host para endereços IP, diferentes tipos de serviços de registros DNS (como Alias, CNAME etc.), balanceamento de carga, e outros.

Um serviço CDN é um serviço de entrega de conteúdo com base na abordagem de que quanto mais próximo do cliente estiver o conteúdo, mais eficiente o serviço será. Então, uma CDN armazena conteúdo em cache (como imagens, vídeos ou páginas da web estáticas) em vários locais ao redor do mundo, permitindo que os clientes recebam o conteúdo rapidamente de um desses locais mais próximos. CDNs também servem como um mecanismo extra de defesa contra os ataques DDoS por servirem de camada prévia de resposta a requisições, ou seja, um dos primeiros serviços que atendem a solicitação de um cliente, antes mesmo que a solicitação chegue aos servidores ou aplicativos.

As VPNs oferecem acesso mais seguro a recursos privados em redes não confiáveis. Combinadas com um firewall, uma VPN permite que as organizações acessem e gerenciem seus recursos internos (por meio do que é conhecido como **túnel** VPN) de maneira segura. Uma VPN permite que usuários corporativos se conectem ao ambiente de nuvem de sua organização a partir da rede corporativa ou de casa por uma conexão criptografada. A conexão com o ambiente de nuvem é transparente para o cliente, isto é, tem a mesma aparência que trabalhar localmente de dentro da rede corporativa. É bastante comum nos principais provedores que a VPN imponha o uso de **autenticação multifator** (MFA) para usuários finais que se conectam ao ambiente.

Um serviço WAF é um firewall de camada de aplicação com capacidade de detectar e mitigar ataques comuns ao protocolo HTTP/HTTPS. Suas regras tomam por base a defesa aos ataques expostos publicamente sobre aplicações web.

Como têm largura de banda muito grande, os provedores de nuvem podem oferecer, adicionalmente, mecanismos para proteger os ambientes dos clientes contra os ataques DDoS, usualmente utilizando grupos de recurso autoescaláveis combinados com serviços de balanceamento de carga.

Amazon

Possui um serviço específico para esse fim, chamado AWS Shield, que no modo avançado opera conjuntamente com Route53 (DNS), CloudFront (CDN) e Elastic Load Balancing (ELB).

Microsoft

Oferece o Azure DDoS Protection, também com um modo de operação avançada que se combina com outras ferramentas como gateway e WAF.

Google

Emprega a mesma abordagem com o Google Cloud Armor Standard para configurações mais básicas e o Managed Protection Plus integrado a outros serviços.

Serviço de Monitoramento e Auditoria

O monitoramento é uma parte crucial da segurança na nuvem. O monitoramento refere-se às atividades de registro feitas nos serviços do ambiente de nuvem. Eventos de login do usuário (sucesso e falha) e ações tomadas (quem fez o quê e quando, e qual foi o resultado final com sucesso ou falha) são os exemplos principais.

O registro documentado de todas as ações realizadas é conhecido como trilha de auditoria. É importante que esse registro de eventos seja armazenado em um repositório central de logs com acesso limitado, cumprindo o conceito da necessidade de conhecimento.

O sistema de geração de alertas de acordo com regras pré-configuradas, como só alertar quando a conta root ou o administrador conseguir fazer login com sucesso no console de gerenciamento, também faz parte do serviço de monitoramento e auditoria.

Atenção!

Ao falarmos sobre monitoramento e auditoria, todos os serviços da nuvem vistos neste conteúdo podem e devem enviar seus logs para um serviço central que os organize e os mantenha em formato compatível para análise posterior. Recomenda-se realizar uma análise de risco nos respectivos serviços para habilitar o registro de eventos de dados de acordo com os objetivos de segurança estipulados porque o custo do armazenamento de eventos versus o valor pode não ser compensador, uma vez que o armazenamento de logs pode ser explosivo em termos de consumo de recursos.

Existe uma classe de produto conhecida como **Security Information and Event Management (SIEM)**, muito empregada atualmente em soluções complexas de monitoramento e auditoria que se responsabiliza por alertar condições associadas de logs em mais de um serviço conjuntamente.

Isto é, se um evento ocorre no serviço A e outro no serviço B, a correlação entre essa conjunção de fatores pode representar uma assinatura de risco muito mais alta do que cada um dos eventos separadamente. Apenas nessa

condição específica seria disparado o alerta, economizando recursos para análise de um problema ou resultando numa ação inadequada de proteção devido a um falso positivo de ataque ao ambiente de nuvem.