



AZURE -AZ900 (M4)

Serviços de Segurança.

▼ Defense in depth

tambem conhecida como defesa em camadas, segue uma filosofia de uma defesa militar , seu objetivo é proteger a informação, prevenindo que seja acessado por de forma não autorizada, uma estrategia, é colocar varios mecanismos que retardam o avanço indevido.

▼ Security azure firewall

Similar ao firewall de rede que usaria no data-center, utiliza ele como serviço, ai inves de comprar e colocar no on premise coisas como cisco, nokia, voce vai utilizar eles na azure, e ela tomara conta, também ajuda a segregar o trafego o ambiente externo, on premises e ambiente das vms

▼ Network Security groups

Entendivel como um firewall interno, está vinculado com o recurso, , complementa o firewall, trabalhando em formato de camadas, servindo como filtro na camada de rede ainda interno do firewall, por padrão todo tráfego originado na própria Vnet é permitido. Ou seja, as máquinas podem se comunicar entre si.

▼ Azure DDoS protection

Serviço para mitigar ataques DDoS, o plano basic, já utiliza a estrutura da azure para evitar acessos indevidos, sem custo, no plano pago, tem uma amplitude maior de serviço, envolvendo relatórios e outras verificações

▼ Azure Security Center

Faz acompanhamentos, gera relatórios, faz acompanhamentos dos níveis de segurança, podendo trabalhar da forma híbrida

▼ Azure Defender

Cofre para armazenar, chaves como ssh, certificados, feito para armazenar informações sensíveis com segurança, onde sua aplicação pode acessar essas chaves no vault para fazer validações, serviço standard, que é digital via software, e o premium trabalha com módulo físico para proteger sua informação.

▼ Azure Information protection

Serviço para classificar informação, classifica, emails documentos, para atender normas, marcando com labels, documentos sensíveis ou não, públicos ou não, pode ser integrado com o microsoft 365.

Serviços de Identidade e Compliance

▼ Azure Active Directory (AAD)

O Azure Active Directory é a próxima evolução da identidade e Soluções de gerenciamento de acesso para a nuvem. Microsoft. Introduziu serviços de domínio do Active Directory no Windows 2000 para dar organizações a capacidade de gerenciar múltiplos Componentes e sistemas de infraestrutura no local usando uma identidade única por usuário.

▼ Single Sign-On

Com login único, os usuários assinam uma vez com uma conta para Acessar dispositivos unidos ao domínio. recursos da empresa. Software AS. Aplicativos de serviço (SaaS) e aplicativos da Web.

O usuário pode iniciar aplicativos do Office 365







▼ Multi-Factor Authentication

A autenticação multi-fator é um processo em que um usuário é solicitado durante o processo de login por uma forma adicional de identificação, como para inserir um código em seu celular ou para fornecer uma digitalização digital.

▼ Azure Policy

A política do Azure ajuda a aplicar os padrões organizacionais e conformidade em escala. Através de seu conformidade avaliar painel, fornece uma vista agregada para avaliar o estado geral do ambiente, com a capacidade de detalhar para a granularidade por recurso, por política.

Casos de uso comum para a política do Azure incluem a implementação governança para a comissão de recursos, conformidade regulamentar, segurança, custo e gerenciamento.

 Sustain secure configurations for compute resources	 Non-compliant	Posture and Vulnerability Mana...	1
 Use Endpoint Detection and Response (EDR)	 Non-compliant	Endpoint Security	1
 Ensure regular automated backups	 Non-compliant	Backup and Recovery	1
 Encrypt backup data	 Non-compliant	Backup and Recovery	1
 Deploy intrusion detection/intrusion prevention systems (IDS/I--	 Compliant	Network Security	0
 Simplify network security rules	 Compliant	Network Security	0
 Secure Domain Name Service (DNS)	 Compliant	Network Security	0

▼ Azure RBAC

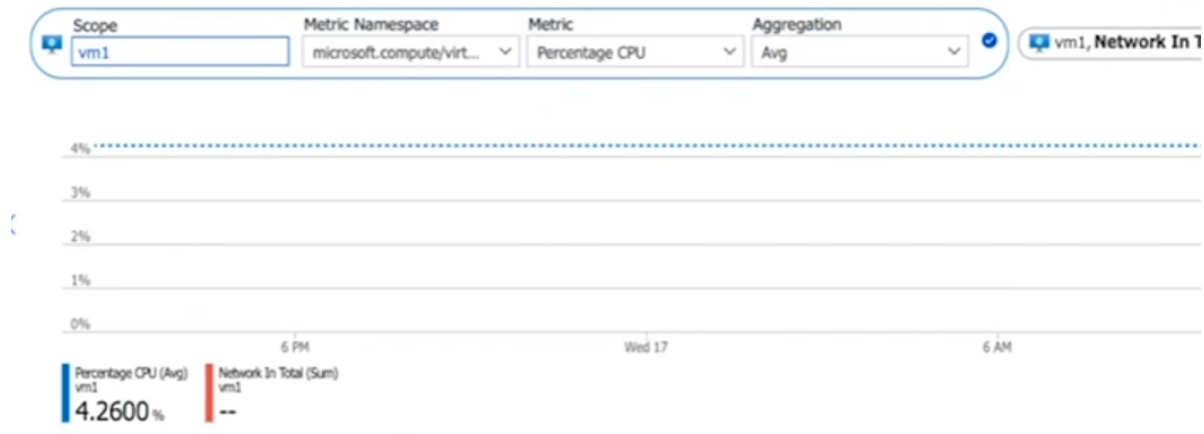
O controle de acesso baseado em função do Azure (Azure RBAC) ajuda você a gerenciar quem tem acesso a recursos azure, o que eles podem fazer com esses recursos e quais áreas eles têm acesso.

Azure RBAC é um sistema de autorização construído em recursos do Azure Manager

▼ Azure Monitor

É baseado em uma plataforma de dados de monitoramento comum que inclui Logs e Métricas. Quando coletados nessa plataforma, os dados de diversos recursos são analisados juntos usando um conjunto comum de ferramentas no Azure Monitor. Os dados de monitoramento também podem ser enviados para

outros locais para dar suporte a determinados cenários, e alguns recursos podem ser gravados em outros locais antes de serem coletados em Logs ou Métricas.



▼ Azure Health

Azure oferece uma suíte de experiências para mantê-lo informado sobre a saúde dos seus recursos em nuvem. Essa informação inclui questões atuais e futuras, como o serviço impactando eventos, manutenção planejada e outras mudanças que pode afetar sua disponibilidade.