Acesso condicionado

É uma camada extra de segurança antes de permitir que usuários autenticados acessem dados ou outros ativos, usuários pertencentes a um determinado grupo é obrigatória o fornecimento da autenticação multifator para se conectar a um aplicativo.

Política de acesso condicionado consiste em atribuição e controles de acesso

Security.microsoft.com

- Atribuições – controla quem oque e quando e em que ponto, todas são avaliadas com AND lógicos (ao ter mais de uma atribuição configurada todas as atribuições devem ser atendidas para disparar uma política
    a) Usuários e grupos: quem a politica incluirá ou excluirá podendo se incluir grupos específicos de usuários, funções de diretório ou usuários convidados externos (também podendo incluir entidades de serviço como aplicativos que estejam registrados no seu locatório)
    b) Aplicativos de nuvem ou ações: podem incluir ou excluir os aplicativos de nuvem, ações de usuários ou contextos de autenticação sujeitos a política (integração do Microsoft defender para nuvem condicionado habilita a visibilidade e o controle em tempo real sobre o acesso e as atividades executadas no seu ambiente nuvem)
    c) Condições: define o ponto em que a política será aplicada podendo ter várias condições que podem ser combinadas para criar políticas de acesso condicional específicas e refinadas
        I. Entrada suspeita e usuário suspeito: miscrosoft id protection permite que as políticas de acesso condicional identificar ações suspeitas relacionadas a contas de usuários no diretório e disparem uma política. entrada suspeita é a probabilidade de que uma determinada entrada, ou solicitação de autenticação não seja autorizada pelo proprietário de identidade. Usuário suspeito é a probabilidade de uma determinada identidade ou conta seja comprometida
        II. Plataforma de dispositivos: caracterizado pelo sistema operacional executado em um dispositivo podendo ser utilizado na imposição da política de acesso condicional
        III. Informação de localização do IP: pode definir intervalos de endereço de ip confiáveis na tomada de decisão da política podendo optar por bloquear ou permitir tráfego do intervalo de IP de um país/região inteira
        IV. Aplicativos clientes: software que está empregando para acessar o aplicativo de nuvem (navegadores, aplicativos móveis e clientes de desktop) também pode ser utilizado na decisão da política de acesso
        V. Filtros para dispositivos: organizações podendo impor políticas com base na propriedades do dispositivo, filtrar dispositivos
- Controles de acesso – política sendo acionada é tomada uma decisão sobre bloquear o acesso, conceder, conceder com verificação extra ou aplicar um controle de sessão (experiência limitada)
        a) Bloquear acesso

b) Permitir acesso: podendo conceder com nenhum controle adicional ou optar por impor um ou mais controles ao conceder acesso, exemplo desses controles – a exigência que usuários façam a autenticação multifatorial; métodos de autenticação especifico para acessar um recurso; exigência de dispositivos atender a requisitos específicos da política de conformidade; exigência de alteração de senha
c) Sessão: administrador pode habilitar uma experiencia limitada em aplicativos nuvem específicos. Exemplo – controle de aplicativos de acesso condicional usa sinais de aplicativos do Microsoft Defender para nuvem bloquear as funcionalidades de baixar , recortar, copiar e imprimir documentos confidenciais ou para exigir a rotulagem de arquivos confidenciais ; podendo também ter frequência de entrada e restrições aplicadas no aplicativo

Microsoft Entra funções e controle de acesso baseado em função (RBAC)

Funções do Microsoft entra controlam as permissões para gerenciar recursos do Microsoft Entra. O Microsoft Entra ID dá suporte a funções internas e personalizadas.

RBAC faz as funções internas e personalizadas do Microsoft Entra

- Funções internas: conjunto fixo de permissões
  a) Administrador global: tem acesso a todos os recursos administrativos no Microsoft entra sendo a pessoa que se inscreve no locatório do Microsoft entra
  b) Administrador do usuário: podem criar e gerenciar todos os aspectos de usuários e grupos e pode gerenciar tíquetes de suporte e monitorar a integridade do serviço
  c) Administrador de cobrança: podem fazer compras, gerenciar assinaturas e tíquetes de suporte e monitorar a integridade do serviço
- Funções personalizadas: podendo oferecer uma flexibilidade ao conceder acesso. É uma lista predefinida de permissões que podem ser escolhidas essas permissões sendo as mesmas usada pelas funções internas tendo a diferença de poder escolher quais deseja incluir em uma função personalizada
    a) 1 etapa é a criação de uma definição de função personalizada (coleção de permissões que podem ser escolhidas de uma lista predefinida) --- 2 etapa é atribuir essa função a um usuário ou grupo criando uma atribuição de função
    b) Atribuição de função: usuário recebe permissão em uma definição de função em um escopo especificado (escopo sendo o conjunto de recursos do Microsoft Entra ao qual o membro da função tem acesso) podendo então ser atribuída o escopo de toda a organização (tem permissão de todos os recursos) ou sendo atribuída a um escopo de objeto com permissão a apenas um único aplicativo
    c) Funções personalizadas exigem uma licença P1 ou P2 do Microsoft entra Id
- Conceder acesso apenas para os usuários que precisam: concedendo apenas a função de administrador de usuários e não a de administrador global tendo privilégios mínimos limitando os danos que podem ocorrer com uma conta comprometida
- Categorias das funções do Microsoft Entra: muitos outros serviços utilizam as funções do Microsoft Entra ID para acessos administrativos então foram feitas funções internas especificas aos serviços

    a) Função específica do Microsoft Entra: oferece permissão para gerenciar recursos somente no Microsoft Entra (administrador de usuário de aplicativos e de grupos concedem permissão para gerenciamento dos recursos que estão no Microsoft entra ID)
    b) Função específica do serviço: para principais serviços do Microsoft 365 oferece permissões para gerenciar recursos dentro do serviço (Microsoft entra ID inclui funções internas para funções de Administrador do Exchange, administrador do Intune, administrador do Sharepoint e administrador do Teams podendo gerar recursos em seus respectivos serviços
    c) Funções entre serviços: possui alguns que abrangem serviços como o Microsoft entra ID ter funções relacionados á segurança, como o administrador de segurança concedendo acesso a vários serviços de segurança no Microsoft 365
- Diferença entre o RBAC do Microsoft Entra e o RBC do Azure: assim como as funções do Microsoft Entra podem controlar o acesso aos recursos dele próprio o Azure também pode controlar o acesso aos recursos do Azure mas possuindo diferenças
    a) RBAC do Microsoft Entra: controlam o acesso a recursos do Microsoft Entra, como usuários, grupos e aplicativos
    b) RBAC do Azure: as funções do Azure controlam o acesso a recursos do Azure como maquina virtuais ou armazenamento usando o Gerenciamento de recursos do Azure

Portal de conformidade e Compliance Manager

Utilizando Microsoft Purview reúne todas as ferramentas e os dados necessários para ajudar a entender e gerenciar as necessidade de conformidade de uma organização e simplifica essa conformidade e reduz os riscos

Como entender a pontuação de conformidade – é calculada usando pontuações que são atribuídas a ações

a) Suas ações aprimoradas: ações que a organização deve gerenciar
b) Ações da Microsoft: ações que a Microsoft gerencia para a organização

As ações são classificadas como obrigatórias, condicionais, preventivas de detecção ou corretivas

a) Obrigatório – essas ações não devem ser ignoradas (criação de uma política para definir os requisitos de duração ou expiração da senha)
b) Discricionária – essas ações precisam que os usuários compreendam e adiram a uma política (uma política em que os usuários são obrigados a garantir que seus dispositivos sejam bloqueados antes de deixá-los)

Subcategorias das classificações

a) Ações preventivas – projetadas a lidar com riscos específicos, como usar a criptografia para proteger os dados inativos se houver violação ou ataques
b) Ações de detecção – monitoram ativamente os sistemas para identificar irregularidades que podem representar riscos ou que podem ser usadas para detectar violações ou invasões (exemplo desses tipos de ações são auditoriais de acesso do sistema ou auditorias de conformidade regulatória)

c) Ações corretivas ajudam os administradores a minimizar os efeitos adversos dos incidentes de segurança, executando medidas corretivas para reduzir seu efeito imediato ou possivelmente até mesmo danos inversos

Diferença entre o Compliance Manager e a pontuação de conformidade

a) Gerenciamento de conformidade: uma solução de ponta a ponta no portal de conformidade do Microsoft Purview permitindo o gerenciamento dos administradores e o acompanhamento das atividades de conformidade
b) Pontuação de conformidade é um cálculo da postura de conformidade geral em toda a organização (está disponível por meio do Compliance Manager)
c) O Compliance manager oferece aos administradores os recursos para entender e aumentar sua pontuação de conformidade, de forma que possam, por fim, melhorar a postura de conformidade da organização e ajuda-la a se manter em conformidade com os requisitos de compatibilidade

Modelos de preços para serviços em nuvem do Microsoft

- Clound Solution Provider (CSP) é um parceiro do Microsoft que proporciona a experiencia e serviços cuidando da sua inscrição no Microsoft 365 também podendo ser adicionados outros produtos baseados em nuvem no contrato como Microsoft Entra e Dynamic 365 com *pagamento enquanto usa* mensal
- Enterprise Agreement é uma empresa que quer licenciar softwares e serviços nuvem por um período mínimo de 3 anos por período. Oferecendo os melhores preços podendo ser mudado dando flexibilidade para comprar esses serviços em um único contrato sob uma grande organização
- Direct Billing é o pagamento direto por cartão de crédito ou debito
- Trial uma inscrição grátis por 30 dias no Microsoft 365 Business Standard, Microsoft Business Premium ou Microsoft 365 Apps