Bootcamp: Profissional Azure Cloud Computing

Desafio Prático

Módulo 4: Soluções de Segurança, Governança, Compliance e Migração no Azure

Objetivos de Ensino

Exercitar os seguintes conceitos trabalhados no Módulo:

1. Criação de Usuários no Entra ID
2. Criação de Grupos no Entra ID
4. Criar e configurar de forma básica o Sentinel
5. Entender melhor e ver na prática o Azure Monitor

Enunciado

Com o objetivo de avaliar os conhecimentos obtidos, você deverá criar um ambiente com as seguintes premissas:

Atividades

Os alunos deverão desempenhar as seguintes atividades:

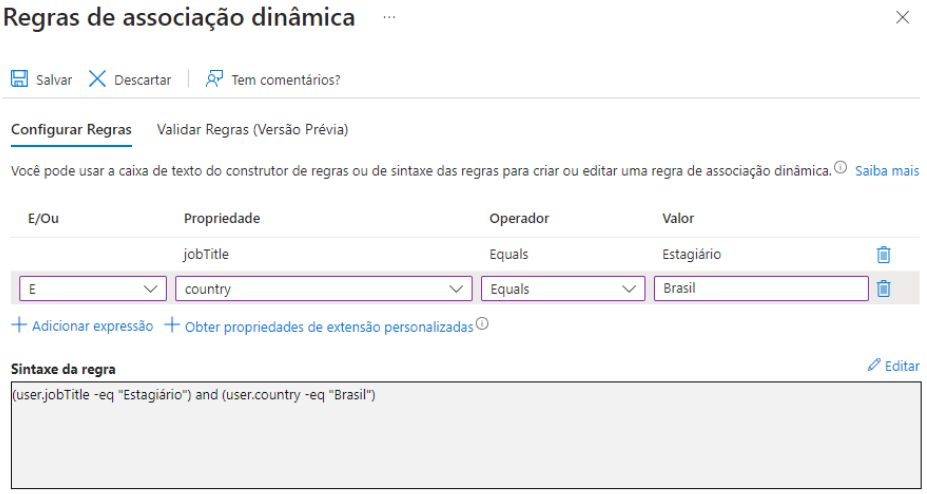
1. Criar 5 usuários no Entra ID com base na tabela abaixo:

Nome	Cargo	País ou Região
User1	Gerente de TI	Brasil
User2	Administrador de Rede	Brasil
User3	Diretor de TI	Estados Unidos
User4	Secretario	Estados Unidos
User5	Estagiário	Brasil

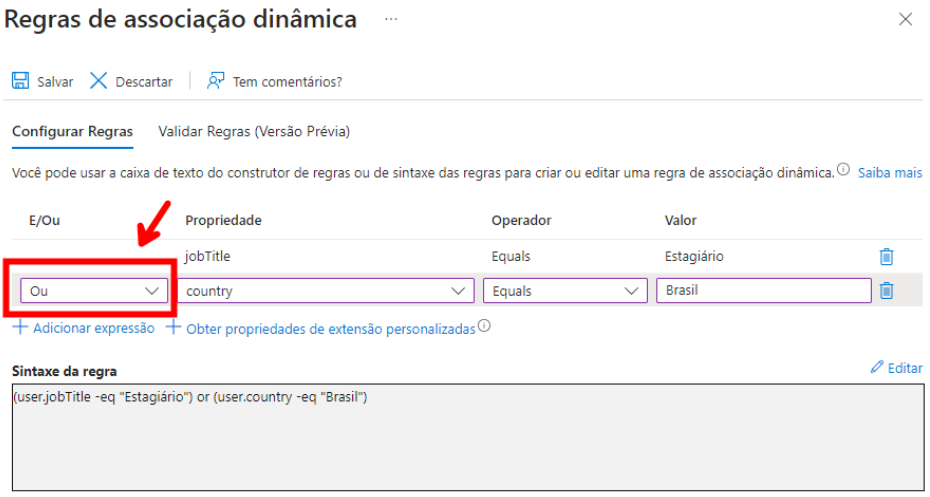
2. Dar permissão no Entra ID para que os Usuários Administradores (User1 e User3) tenham permissões de Global Administrator.

Atividades

3. Crie um Grupo de Segurança com o Nome “Estagiários” e, no tipo de associação, configure como “Usuário Dinâmico”, clique em “Adicionar consulta dinâmica” e deixe da forma abaixo:



4. Observe e anote, após 10 minutos quais usuários foram incluídos no grupo.
5. Acesse novamente o Grupo “estagiários”.
6. Acesse novamente o grupo e altere o as regras de associação dinâmica de “e” para “ou”:



7. Observe, após 10 minutos, os usuários que estão dentro do grupo e anote quais são.

Atividades

8. Dentro do portal do Azure, crie um recurso “Azure Sentinel” (será solicitado para criar um workspace, crie um com o nome XP-MODULO04 na região East-US)

13. Acesse a guia conectores de dados e localize “Azure Active Directory Identity Protection”, selecione ele, role a barra da blade da direita até o máximo e clique em “Abrir a página do conector”.

14. Na página aberta, em Configuração clique em Conectar.

15. Volte para o Azure Sentinel e clique em “Pastas de Trabalho” (Workbooks) e localize “Logs de Entrada do Azure AD” e, após selecionar ele, clique no botão (do lado direito) em Salvar e OK.

16. Volte ao Azure Sentinel e vá novamente para a guia “Pastas de Trabalho”, selecione “Minhas pastas de trabalho”, Logs de Entrada do Azure AD e clique em “Ver pasta de trabalho salva”.

17. Verifique os Resultados, caso ainda não tenha nada, aguarde mais um tempo e verifique novamente (como acabamos de criar o log analytics workspace pode levar um tempo até aparecer os primeiros dados, que leva de 1 a 12 horas, após estar tudo ok os resultados são bem rápidos de aparecer).

18. Crie um alerta com as seguintes premissas:

Escopo: Sua Assinatura

Condição: Create Resource Group

Ação: Enviar um SMS para o seu número de celular

Nome: New RG

19. Aguarde alguns minutos e, em seguida, crie um grupo de recursos chamado “alerttest”.

20. Apague a Regra de Alerta após receber um alerta via SMS.

21. Exclua o Grupo “Estagiários” e observe atentamente a mensagem que ele