# Criação e Gerenciamento de buckets

## Introdução ao Azure Management Services (Azure MSM)

Azure Management Services (MSM) é uma coleção de serviços e ferramentas que ajudam a gerenciar, monitorar, e operar recursos no Microsoft Azure. Ele oferece uma interface centralizada para a administração de todos os recursos e serviços implantados na nuvem Azure, permitindo automação, monitoramento, gerenciamento de políticas, e governança.

- **Serviços Chave do Azure MSM:**
  - Azure Portal: Interface web para gerenciar e monitorar recursos.
  - Azure Resource Manager (ARM): Framework para gerenciar a infraestrutura através de templates declarativos.
  - Azure Monitor: Ferramenta de monitoramento e telemetria para rastrear desempenho e saúde dos recursos.
  - Azure Policy: Serviço para criar e aplicar políticas de governança que garantem a conformidade com padrões e regulamentos.

Uma grande empresa que opera em várias regiões pode usar o Azure MSM para garantir que todos os recursos de TI estejam em conformidade com as políticas corporativas e que os custos sejam monitorados em tempo real.

### Grupos de Recursos no Azure

Grupos de Recursos são um componente essencial da arquitetura do Azure, que serve como contêiner lógico para organizar e gerenciar recursos relacionados.

- **Função dos Grupos de Recursos:**
  - Organização: Permitem agrupar recursos relacionados (como VMs, redes, bancos de dados) em uma única unidade lógica.
  - Gerenciamento Centralizado: Facilitam o gerenciamento, monitoramento, e aplicação de políticas a todos os recursos de um grupo específico.
  - Ciclo de Vida: Todos os recursos em um grupo de recursos compartilham o mesmo ciclo de vida, facilitando a implantação, atualização, e exclusão conjunta.
- **Práticas Recomendadas:**
  - Agrupamento por Projeto ou Aplicação: Organize os recursos por projeto, ambiente (desenvolvimento, teste, produção), ou aplicação.
  - Aplicação de Políticas: Use o Azure Policy para aplicar políticas de conformidade ao nível do grupo de recursos.

Uma equipe de desenvolvimento trabalhando em uma aplicação web pode criar um grupo de recursos que contém as VMs, banco de dados, e serviços de rede necessários, facilitando a gestão como um todo.

### Contas de Armazenamento no Azure

Contas de Armazenamento no Azure são o ponto central para armazenar todos os dados do Azure, desde blobs até tabelas, filas, e discos.

- **Tipos de Armazenamento:**

- Blob Storage: Usado para armazenar grandes quantidades de dados não estruturados, como imagens, vídeos, backups, e arquivos de log.

- File Storage: Armazenamento de arquivos baseado em SMB, ideal para migrações lift-and-shift de servidores de arquivos.

- Queue Storage: Armazenamento de mensagens para comunicação entre componentes distribuídos.

- Table Storage: Armazenamento NoSQL para grandes volumes de dados estruturados.

- **Gerenciamento:**
  - Escalabilidade: As contas de armazenamento são altamente escaláveis, suportando petabytes de dados.

  - Segurança: Permite criptografia em repouso, chaves gerenciadas, e controle de acesso granular.

Um sistema de backup de arquivos pode usar uma conta de armazenamento no Azure para armazenar cópias diárias de todos os documentos críticos, garantindo que estejam seguros e acessíveis em caso de falhas.

**Diferença Entre Blob Storage, Data Lake, e Lakehouse**

**1. Blob Storage:**

- **Definição**: Blob Storage é o serviço de armazenamento de objetos do Azure, ideal para armazenar grandes volumes de dados não estruturados, como arquivos de mídia, logs, e backups.

- **Casos de Uso**: Arquivamento de dados, armazenamento de dados não estruturados, distribuição de conteúdo.

### 2. Azure Data Lake Storage (ADLS):

- **Definição**: Azure Data Lake Storage é uma solução de armazenamento otimizada para análises de big data, oferecendo armazenamento em escala de petabytes com segurança e desempenho integrados.

- **Características:**
  - Hierarquia de Diretórios: Suporta uma estrutura de diretórios, facilitando a organização dos dados.

  - Integração com Hadoop: Ideal para cenários de análise de dados com Apache Hadoop e Spark.

- **Casos de Uso**: Processamento de big data, armazenamento de grandes volumes de dados brutos para análise.

### 3. Lakehouse:

- **Definição**: Um conceito mais recente, o Lakehouse combina os benefícios dos data lakes e data warehouses. Ele suporta tanto dados estruturados quanto não estruturados e permite análises avançadas com baixa latência.

- **Características:**
  - Camada de Armazenamento Unificada: Armazena todos os tipos de dados em um único local.

  - Suporte a Transações: Como os data warehouses, suporta operações ACID, garantindo integridade dos dados.

- **Casos de Uso**: Análises avançadas em tempo real, machine learning, relatórios empresariais integrados.

**Comparação:**

- Blob Storage é ideal para armazenamento simples de objetos.
- Data Lake Storage é otimizado para big data e análises em larga escala.
- Lakehouse oferece uma solução híbrida, combinando o melhor dos dois mundos para análises avançadas e gestão de dados em grande escala.

Uma empresa que precisa armazenar grandes volumes de dados brutos para análises pode usar o Azure Data Lake Storage, enquanto uma equipe de ciência de dados pode preferir a flexibilidade e capacidade analítica de um Lakehouse para executar modelos de machine learning e gerar insights.

**Criar e Usar Buckets no Azure**

No Azure, o conceito de "buckets" se refere ao Armazenamento de Blobs (Blob Storage), onde blobs (objetos de dados) são organizados em contêineres, que funcionam de maneira similar aos buckets em outras plataformas de nuvem, como o Amazon S3.

**1. Criação de um Bucket e Tornando-o Público**

**Criação de um Bucket (Contêiner) no Azure Blob Storage:**

- **Passos para Criar um Contêiner:**
  - No Azure Portal, acesse sua Conta de Armazenamento.
  - No painel da conta de armazenamento, selecione "Contêineres" em "Serviços de Dados".

- Clique em “Adicionar Contêiner”.

- Dê um nome ao contêiner e escolha o nível de acesso público:
  - Privado (sem acesso anônimo): Apenas os usuários autenticados têm acesso.

  - Blobs (acesso público anônimo aos blobs): Blobs dentro do contêiner podem ser acessados anonimamente, mas não o contêiner em si.

  - Contêiner (acesso público anônimo a todo o conteúdo): Tanto o contêiner quanto os blobs podem ser acessados anonimamente.

- **Tornando o Contêiner Público**:
  - Escolha a opção de acesso público desejada ao criar o contêiner ou edite as configurações de acesso posteriormente para torná-lo público.

Se você precisa armazenar e compartilhar imagens publicamente na web, criar um contêiner com acesso público facilita o compartilhamento direto dos URLs das imagens.

### 2. Configuração de Chaves de Criptografia

A criptografia é uma prática essencial para proteger dados sensíveis armazenados em contêineres.

#### Configurando Chaves de Criptografia:

- **Criptografia por Padrão:**

- O Azure Blob Storage criptografa todos os dados automaticamente com chaves gerenciadas pela Microsoft.

- **Usando Chaves Gerenciadas pelo Cliente (CMK):**

- Crie ou use uma chave existente no Azure Key Vault.

- No Azure Portal, vá para sua conta de armazenamento.

- Selecione “Configurações” e, em seguida, “Criptografia”.

- Escolha “Usar chaves gerenciadas pelo cliente” e selecione sua chave do Key Vault.

Empresas que precisam de controle total sobre a segurança de seus dados podem optar por gerenciar suas próprias chaves de criptografia, garantindo conformidade com políticas internas e regulatórias.

### 3. Habilitação do Gerenciamento do Ciclo de Vida

O gerenciamento do ciclo de vida permite automatizar a transição dos dados entre diferentes camadas de armazenamento com base em políticas de tempo.

**Configurando o Gerenciamento do Ciclo de Vida:**

- **Passos para Habilitar:**
  - Na conta de armazenamento, vá para “Gerenciamento do Ciclo de Vida” nas configurações.

  - Crie uma nova política de ciclo de vida.

  - Defina regras para mover blobs entre camadas de armazenamento (hot, cool, archive) ou excluir blobs após um certo período.

- **Políticas Comuns:**

- Mover blobs não acessados por 30 dias para a camada cool (menos frequente).
- Arquivar blobs não acessados por 180 dias.
- Excluir blobs após 365 dias.

Um sistema de backup que armazena grandes volumes de dados pode usar o gerenciamento do ciclo de vida para mover automaticamente backups antigos para a camada de arquivo, economizando custos.

### 4. Ativação do Controle de Versão

O controle de versão permite que você mantenha várias versões de um blob, recuperando versões anteriores em caso de exclusão ou modificação indesejada.

**Ativando o Controle de Versão:**

- **Passos para Ativar:**
  - Na conta de armazenamento, acesse “Configurações” > “Controle de Versão de Dados”.
  - Ative a opção de controle de versão para que o sistema comece a manter versões antigas dos blobs.
- **Usando o Controle de Versão:**
  - Cada vez que um blob é modificado ou excluído, uma nova versão é criada automaticamente. Você pode restaurar versões anteriores conforme necessário.

Em um ambiente de desenvolvimento colaborativo, onde múltiplos usuários estão modificando arquivos de configuração, o controle de versão assegura

que qualquer alteração indesejada possa ser revertida facilmente.

### 5. Criação de Recursos no Segundo Projeto

Em cenários onde você precisa replicar ou compartilhar recursos entre diferentes projetos ou contas de armazenamento, é essencial saber como criar e configurar adequadamente esses recursos.

**Passos para Criar Recursos:**

- **Criação de Contêineres:**
  - Siga o mesmo processo usado anteriormente para criar contêineres no novo projeto ou conta de armazenamento.

- **Compartilhamento entre Projetos:**
  - Utilize o Azure Shared Access Signatures (SAS) para permitir acesso seguro e temporário a contêineres ou blobs específicos entre projetos.

Se você está trabalhando em um projeto de análise de dados em conjunto com outra equipe, você pode criar um contêiner no segundo projeto e fornecer acesso seguro a essa equipe através de SAS.

### 6. Criação e Verificação de Recursos no Primeiro Projeto

Depois de configurar recursos no segundo projeto, é importante garantir que os recursos do primeiro projeto estejam adequadamente integrados ou interligados.

**Passos para Verificação:**

- **Verificação de Integração:**
  - Certifique-se de que os contêineres ou blobs criados no segundo projeto estão acessíveis a partir do primeiro projeto.

- Teste o acesso e a integridade dos dados transferidos ou replicados entre projetos.

- **Monitoramento e Auditoria:**
  - Use o Azure Monitor para rastrear o uso, acessos, e quaisquer anomalias nos recursos compartilhados entre os projetos.

Em um cenário onde dados coletados por diferentes equipes precisam ser centralizados para análise, garantir a integração e a acessibilidade entre os recursos do primeiro e segundo projetos é crucial para a continuidade e sucesso das operações.

## Conteúdo Bônus

Guia passo a passo para a criação e administração de buckets utilizando o Google Cloud Storage:
**Título:** Criar buckets
**Plataforma:** Cloud.Google

## Referências Bibliográficas

BASSO, D. E. **Administração de Redes de Computadores**. Contentus, 2020.
KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 8. ed. Pearson, 2021.
MARINHO, A. L.; CRUZ, J. L. da. (Orgs.). **Desenvolvimento de Aplicações para Internet**. 2. ed. Pearson, 2020.
PUGA, S.; RISSETTI, G. **Lógica de Programação e Estruturas de Dados, com Aplicações em Java**. 3. ed. Pearson, 2016.
ROHLING, L. J. **Segurança de Redes de Computadores**. Contentus, 2020.
SILVA, C. F. da. **Projeto Estruturado e Gerência de Redes**. Contentus, 2020.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. J. **Redes de Computadores**. 6. ed. Pearson, 2021.

TOCCI, R. J.; WIDMER, N. S.; MOSS, G. L. **Sistemas Digitais: Princípios e Aplicações**. 12. ed. Pearson, 2018.

## Ir para exercício