

# Administrador de Banco de Dados (extra Abril) - Turma 2024A

## 5.17 Soluções de alta disponibilidade e recuperação de desastres

Soluções de alta disponibilidade e recuperação de desastres são essenciais em bancos de dados para garantir que os dados estejam sempre disponíveis e que a recuperação seja possível em caso de falhas no sistema. A alta disponibilidade refere-se à capacidade do sistema de continuar operando mesmo em caso de falha em um dos componentes do sistema. A recuperação de desastres é a capacidade de restaurar os dados após uma falha ou desastre, como um incêndio, terremoto ou ataque cibernético.

Algumas das soluções de alta disponibilidade e recuperação de desastres em bancos de dados incluem:

- Replicação de dados: Como mencionado anteriormente, a replicação de dados envolve a criação de cópias dos dados em diferentes servidores. Se um servidor falhar, os dados ainda estarão disponíveis nos servidores secundários.
- Cluster de failover: O cluster de failover envolve a configuração de vários servidores em um cluster, com um servidor primário e vários servidores secundários. Se o servidor primário falhar, um dos servidores secundários assume automaticamente as operações para garantir a continuidade do serviço.
- Backup e recuperação: O backup e recuperação envolve a criação regular de cópias dos dados do banco de dados e a recuperação desses dados em caso de falha. Essas cópias de backup são armazenadas em um local seguro para facilitar a recuperação de desastres.
- Monitoramento e diagnóstico: O monitoramento e diagnóstico envolve a implementação de práticas regulares de monitoramento do sistema para identificar possíveis problemas antes que eles se tornem críticos. Isso pode incluir o monitoramento do desempenho do sistema, a verificação da integridade dos dados e a identificação de possíveis ameaças à segurança.
- Tolerância a falhas: A tolerância a falhas envolve a capacidade do sistema de continuar operando mesmo em caso de falhas em um ou mais componentes do sistema.

A implementação de soluções de alta disponibilidade e recuperação de desastres em um banco de dados pode trazer várias vantagens, como a redução do tempo de inatividade do sistema, a garantia da disponibilidade contínua dos dados e a proteção contra a perda de dados em caso de falhas no sistema. É importante implementar essas soluções de forma adequada e testá-las regularmente para garantir a disponibilidade e

segurança dos dados em um banco de dados.

Imagine que uma empresa financeira mantém seus dados em um banco de dados e ocorre um desastre natural, como uma inundação que destrói o centro de dados da empresa. Os servidores e os backups são todos perdidos, e a empresa precisa recuperar seus dados para garantir a continuidade do negócio.

Nessa situação, a empresa precisa implementar um plano de recuperação de desastres para recuperar os dados do banco de dados. O plano de recuperação de desastres pode incluir as seguintes etapas:

1. Avaliação da situação: A empresa deve avaliar a extensão dos danos e identificar o que foi perdido. Isso pode incluir a perda de backups, servidores, discos rígidos e outros componentes do sistema.
2. Criação de um plano de recuperação: Com base na avaliação da situação, a empresa deve criar um plano de recuperação que identifica as etapas necessárias para recuperar os dados do banco de dados. Isso pode incluir a aquisição de novos servidores, a instalação do banco de dados e a recuperação dos dados a partir de fontes alternativas, como backups em nuvem ou registros em papel.
3. Recuperação do banco de dados: Com base no plano de recuperação, a empresa deve implementar as etapas necessárias para recuperar o banco de dados. Isso pode incluir a reinstalação do banco de dados em um novo servidor, a recuperação dos dados de backups em nuvem ou a recuperação de dados a partir de registros em papel.
4. Verificação da integridade dos dados: Após a recuperação dos dados, é importante verificar a integridade dos dados para garantir que não haja corrupção ou perda de dados durante o processo de recuperação.
5. Testes de continuidade do negócio: Após a recuperação do banco de dados, a empresa deve testar a continuidade do negócio para garantir que todas as operações estejam funcionando corretamente.

A recuperação de desastres pode ser um processo longo e complicado, mas é essencial para garantir a continuidade do negócio após um desastre natural ou outro evento que possa causar a perda de dados críticos. Ao implementar um plano de recuperação de desastres, as empresas podem garantir que seus dados estejam disponíveis e protegidos contra a perda em caso de falhas do sistema.

Última atualização: terça, 21 mar 2023, 13:37

## ◀ 5.16 Configuração e gerenciamento de replicação

Seguir para...

[5.18 Princípios de segurança de banco de dados ►](#)