Segurança de dados

Aula 12 – Alta disponibilidade - parte 3

Gustavo Bianchi Maia

gustavo.maia@faculdadeimpacta.com.br

Sumário

- Revisão
  - Log Shipping
  - Replicação
- Novas técnicas
  - Espelhamento / Mirroring
  - Always on Failover Cluster
  - Always on Availability Groups
- Prévia AC5

Mecanismos de Alta disponibilidade

Na disciplina de Segurança de Dados, as técnicas para gerenciamento de contingência (ou redundância) associadas à alta disponibilidade, ou HA do termo em inglês High Availability serão:

- **[LS]** - Log Shipping - Técnica de envio de logs transacionais via BACKUP/RESTORE entre servidores.
- **[Rep]** - Replicação (Transactional Replication without updatable subscribers) - Técnica de envio de informações (artigos) para outros servidores (assinantes) coordenados por uma central de distribuição
- **[PtP]** - Replicação (Peer-to-peer) - Técnica de compartilhamento de informações entre múltiplos servidores, cada um tendo o papel de publicador, distribuidor e assinante dos dados do conjunto.
- **[Mirroring]** - Espelhamento - Técnica de sincronização entre bancos de dados.
- **[Cluster]** - Clustering - Técnica de utilização de múltiplos nós (instâncias) utilizando [preferencialmente] um Shared Disk Array
- **[AG]** - AllWaysOn - Técnica de sincronização entre bancos pela formação de grupos de disponibilidade (AG = Availability Groups)

Por quê Backup / Restore NÃO é considerada uma técnica de alta disponibilidade ?

Mecanismos de Alta disponibilidade

Lista de siglas ou termos que serão utilizadas em nossas aulas, segue uma revisão / apresentação:

DR = Recuperação de desastres, reversão de danos ou prevenção de perda de dados

HA *= High Availability (Alta disponibilidade), redução ou eliminação do tempo de DownTime.*

MTTR *= Tempo de reparo médio, ou o tempo de se colocar em prática uma solução de DR.*

WSFC *= Windows Server Failover Cluster (cluster à nível sistema operacional)*

FCI *= Failover Cluster Instance (cluster das instâncias do MSSQL)*

SDA *= Shared Disk Array (Conjunto de Discos Compartilhados)*

Backup INIT *= Rotina de Inicialização, BACKUP do principal seguido de RESTORE nas réplicas*

DNS *= Registro de aliases na rede –Uso do DNS ao invés de IPs ou Nomes físicos para localização de servidores*

FIREWALL *= Configurações ou necessidade de manutenção de portas de acesso na rede*

RAID *= Solução a nível dos discos, normalmente utilizados para garantir segurança e/ou velocidade.*

Failover *= técnica de promoção um servidor secundário (ou réplica) à primário.*

Principal = Servidor principal utilizado pelas aplicações da empresa (nó ativo, status = RECOVERY)

Réplica = Nome dado os múltiplos servidores secundários que não são o principal, capazes [ou não] de failover.

Mecanismos de Alta disponibilidade

Após a apresentação de todas as técnicas, você deverá apresentar a seguinte tabela preenchida conforme orientações:

Técnica	Principal Finalidade	Janela de perda	Tipo de Failover	Qtde Réplicas	Reversibilidade	Status Réplica	Nível Sincronização	Setup / Recomendações (Liste os números)	Edição mínima	Versão mínima	Disp. Azure
LS											
Rep											
PtP											
Mirror											
WSFC											
AG											

Mecanismos de Alta disponibilidade

Onde:

- **Principal Finalidade.**
  - Propósito ou 'ponto forte' da técnica, para DR ou HA (mesmo atendendo às duas, uma ainda é a principal)
  - **Opções: DR** (evitar perda de dados, pouca perda), **HA** (downtime zero, aplicação não 'sentir' a queda)
- **Janela de perda / tempo de cópia / tipo de sincronização.**
  - Tempo em que as informações do principal levam para serem transferidas para o secundário. Durante esta janela, tais informações estão vulneráveis, ou seja, numa eventual crise, elas podem ser perdidas.
  - **Opções: Min**utos**, Seg**undos**, Zero** (sem perda, ou sem necessidade de cópia de dados)
- **Tipo de Failover** (recomendação)
  - Capacidade de promoção do servidor secundário à primário. Assume-se que, se há risco de perda de dados, é necessário a intervenção humana para realizar ou autorizar um failover (ou seja, se há perda de dados, não é recomendado deixar o sistema decidir pelo failover, devido aos falsos positivos como: erro de rede, latência)
  - **Opções: Manual** (pois há riscos de perdas de dados)**, Auto**mático (não há riscos de perda de dados)
- **Quantidade de réplicas / servidores secundários.**
  - Número de réplicas que posso configurar para que, em caso de falha, um deles possa assumir o papel de primário em caso de failover. Ou se possível, utilizar para me conectar no SGBD.
  - **Opções: Um** (um principal, limite de uma única réplica)**, N** (um principal, possibilidade de múltiplas réplicas)
- **Reversibilidade**
  - Promoção do secundário à primário (failover) e depois de volta à secundário (outro failover) sem necessidade de re-configuração (Backup INIT) ou risco de existirem dois servidores que se acham principais.
  - **Opções: Total** (Ida e volta, à vontade)**,** Só **Ida** (feito o failover não há ou não é recomendado o retorno)

Mecanismos de Alta disponibilidade

Onde:

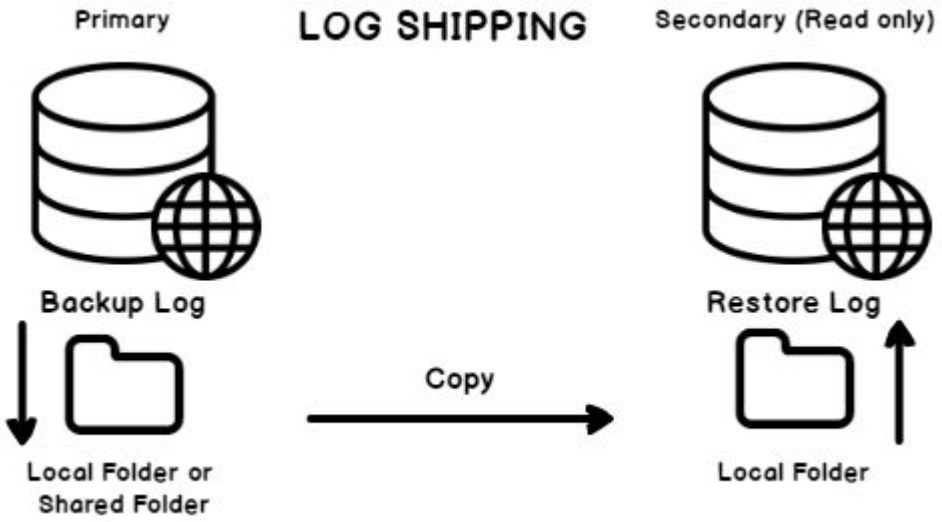
- **Status da réplica / Usos extras para o servidor Secundário**
  - Capacidade de uso das réplicas para algo mais além da função de alta disponibilidade, afetado diretamente pelo tipo de recuperação (ou status) das réplicas.
  - **Opções: Não** (NORECOVERY)**, RO** - Read Only (STANDBY)**, RW** - Read Write (RECOVERY)
- **Nível de sincronização:**
  - Nível em que a técnica é aplicada, limita a quantidade de informações que pode ser sincronizada.
  - **Opções: Inst**ância (Tudo o que está na instalação)**, D**ata**B**ase (Banco de dados)**, Obj**etos (tabelas, visões)
- **SETUP / Dificuldade de implementação / pré-requisitos / Recursos extras.**
  - Configurações, etapas necessárias ou altamente recomendadas para a implantação desta técnica.
  - **Opções múltiplas**(anote os números/ordem, ex:1,3,5): **WSFC**[1], **FCI**[2], **SDA**[3], **Backup INIT**[4], **DNS**[5], **RAID**[6], **Firewall**[7]
- **Edições / Licenciamento mínimo necessário.**
  - Capacidade de execução em uma determinada Edição do SQL Server
  - **Opções: Express, Compact, Web, Standard, Enterprise**
- **Versões / Disponibilidade mínima nas versões:**
  - Versões inicial em que esta técnica se tornou disponível.
  - **Opções: 2000, 2005, 2008, 2008R2, 2012, 2014, 2016, 2017, 2019**
- **Disponibilidade no Azure:**
  - Possibilidade de utilizar esta técnica em um banco de dados localizado no Azure (Azure Cloud Databases).
  - **Opções: Não** (Não disponível)**, Parcial** (uso limitado, ex:só importação)**, Sim** (uso normal, como uma instância local)

Log Shipping - Revisão

Esta é a técnica de realizar backups em um servidor e automaticamente restaurá-los em outro(s) servidor(es) em uma janela muito pequena (minutos), criando assim um servidor “morno”.

São necessários bancos diferentes para a realização de log shipping, mas por segurança é recomendado que o restore seja realizado em um servidor físico, geograficamente isolado do principal.

Atua a nível de banco de dados, que devem estar em modo de recuperação FULL.
O(s) servidor(es) secundário(s) pode estar em modo somente leitura.
Posso ter um servidor com o papel de monitoria, porém, ainda se recomenda failover manuais.



Fonte: SQL Server Transaction Log and High Availability Solutions (sqlshack.com)

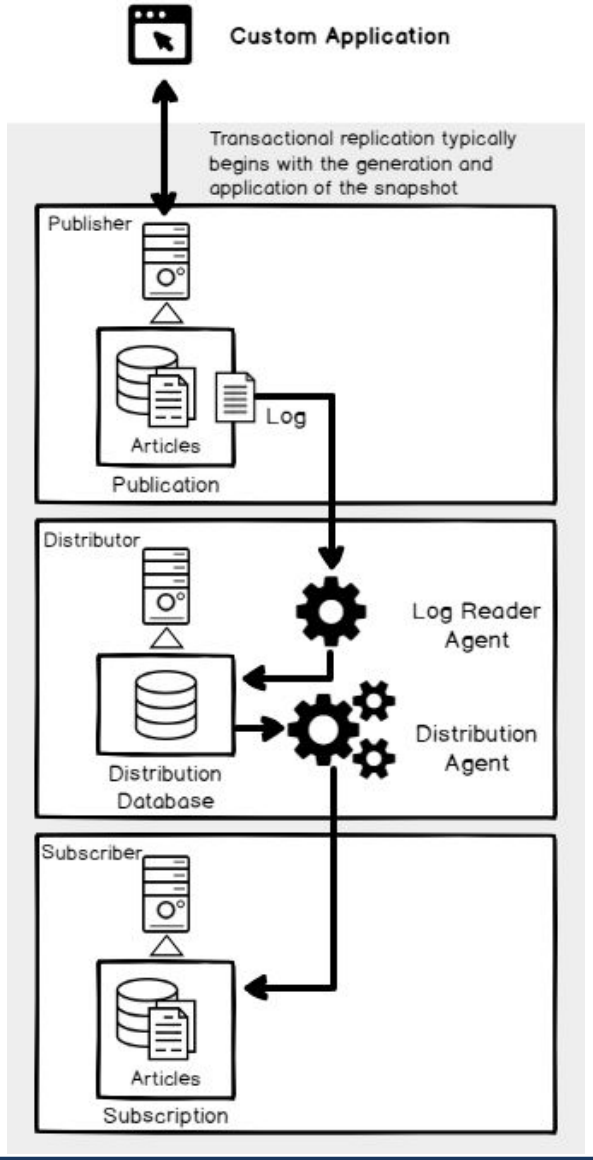
Replicação

A Replicação é uma técnica que pode ser comparada à uma editora.

Suponha que existam milhares de escritores enviando artigos para serem publicados para uma revista, e que dentre todos, o editor deve selecionar quais ele deseja publicar na edição deste mês, fechando então o que chamamos de ‘publicação’.

O conteúdo é então encaminhado à distribuidora, que é responsável por gerenciar transporte da informação até seu ponto final.

Do outro lado temos os assinantes, pessoas que desejam receber tal conteúdo através dos diversos meios de distribuição.



Fonte: SQL Server Transaction Log and High Availability Solutions (sqlshack.com)

Replicação - Tipos de Replicação

Snapshot replication

Esta técnica tira uma 'foto' dos artigos (tabelas/bancos/etc) e os envia aos assinantes, uma vez que o conteúdo foi consumido, a 'foto' original é descartada, por não se tratar do dado real.

É muito recomendada para cenários que não precisam de atualização contínua, ou que contenha dados estáticos.

Transactional replication

Esta técnica não aborda os dados, mas sim as transações (transactional log) sobre os artigos (tabelas), enviando-os em tempo real para os assinantes tentando mantê-los atualizados o mais rápido possível.

Um primeiro snapshot é realizado para a sincronização inicial, depois disso, todo e qualquer comando que gera log será enviado aos assinantes para manter a sincronia da base.

A sincronização rápida é justamente a grande vantagem desta técnica.

Replicação - Tipos de Replicação

Merge replication

Esta técnica é comumente utilizada quando não há comunicação constante entre assinante e distribuidor, permitindo trabalho independente até que os dados sejam sincronizados.

Ela também precisa de um snapshot inicial para configuração, a partir dai, as mudanças são rastreadas com a utilização de triggers.

Peer-to-peer replication

É um subtipo da replicação transacional, onde todos os 'nós' são editores e assinantes ao mesmo tempo, a informação nem precisa estar toda completa em cada uma das bases pois todas elas 'conversam' entre si para sincronizar e distribuir a informação.

Espelhamento - Mirroring

Espelhamento, ou mirroring, é uma técnica implementada no servidor no nível de banco de dados, ou seja, não há como espelhar apenas parte do banco, ou uma tabela em específica.

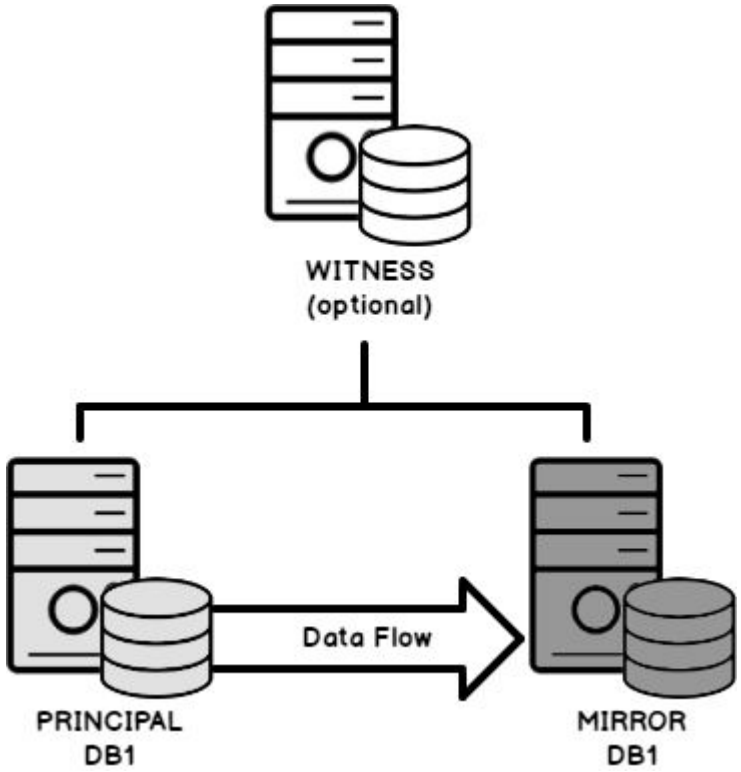
Sua implementação envolve duas cópias distintas do mesmo banco, uma delas ativa de cada vez. Preferencialmente as cópias devem ficar em servidores distintos.

Papéis:

Principal: é o servidor principal, ativo (ou quente), utilizado em produção

Mirror: é o servidor secundário, inativo (ou morno), que recebe todas as transações do servidor principal, portanto a qualquer momento pode assumir o papel de principal

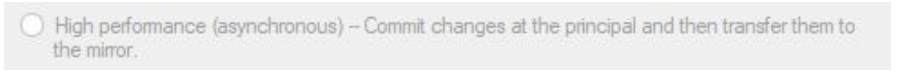
Witness: é o agente controlador, é um servidor opcional, sua função é controlar as filas de envio e recebimento dos servidores e atuar quando um deles para de responder, promovendo o mirror a principal, por exemplo.



Fonte: SQL Server Transaction Log and High Availability Solutions (sqlshack.com)

Espelhamento - Modos

Alta performance:



– As transações são executadas independentemente nos servidores principal e espelho, ou seja, o principal não espera a confirmação de execução para dar continuidade aos processos. Desta forma o servidor principal praticamente nem 'percebe' a presença do servidor espelho.

– Não é garantias de que os dois servidores estão sempre sincronizados, pois o servidor espelho dependerá da velocidade de consumo das transações recebidas do principal.

– Não permite a utilização de um witness server, ou seja, todo "failover" é realizado manualmente.

– Só está disponível nas edições Enterprise e superiores.

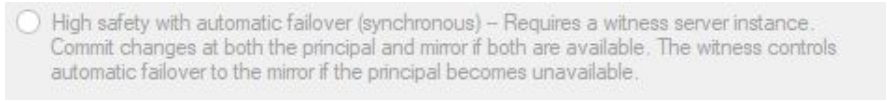
Alta segurança sem Servidor Testemunha:

– As transações apesar de serem executadas independentemente em ambos os servidores, apenas são dadas como concluídas após ambos confirmarem sua execução. Desta forma o servidor principal pode sofrer da latência que a informação leva para ir ao servidor espelho e a chegada da confirmação de execução.

– Há garantia de que os servidores estão sempre sincronizados.

– Está disponível nas edições Standard e superiores

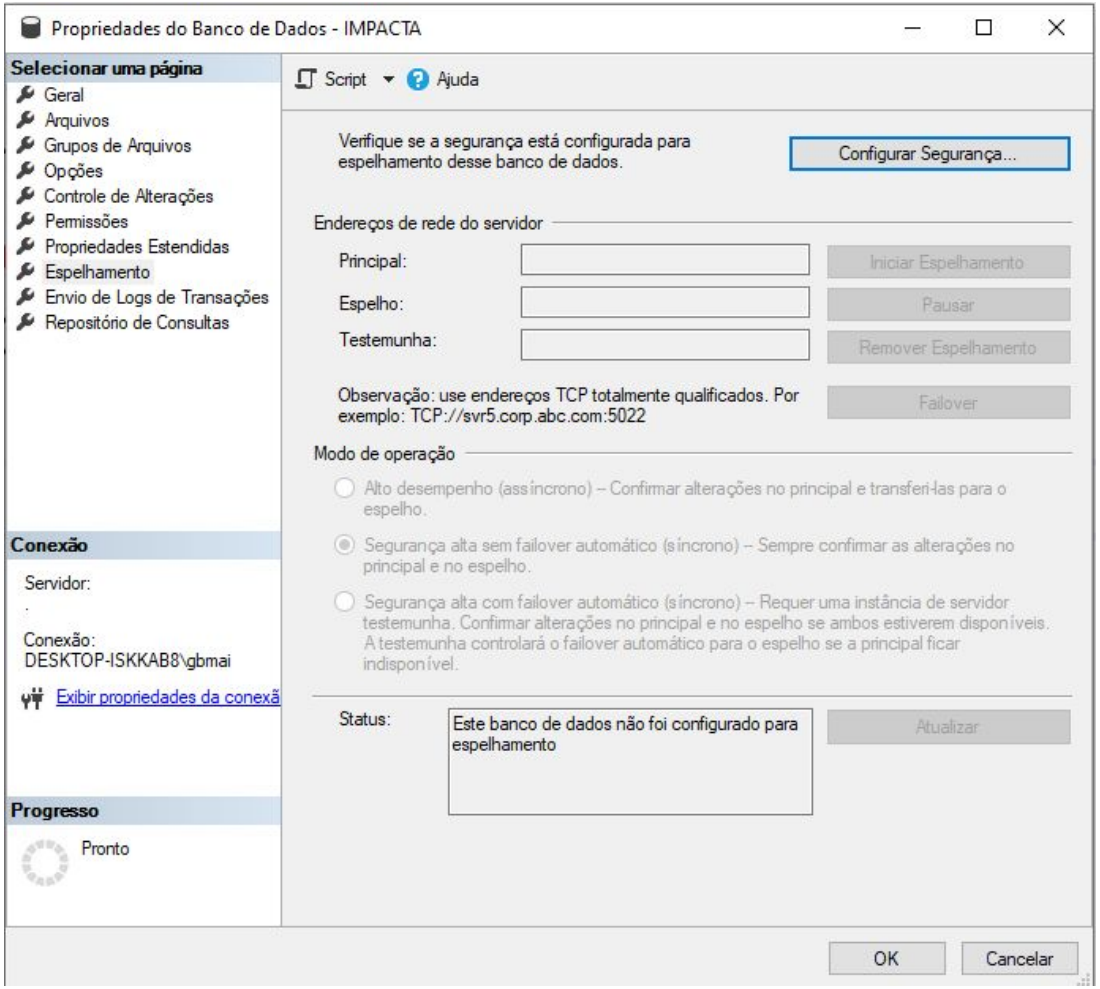
Alta segurança com Servidor Testemunha:



– Faz a utilização de um witness server, ou seja, quando presente os servidores pode realizar o que denominados "failover" automaticamente.

Espelhamento - Mirroring

Demonstração:



Mais detalhes: [How to configure SQL Server mirroring on a TDE encrypted database (sqlshack.com)]

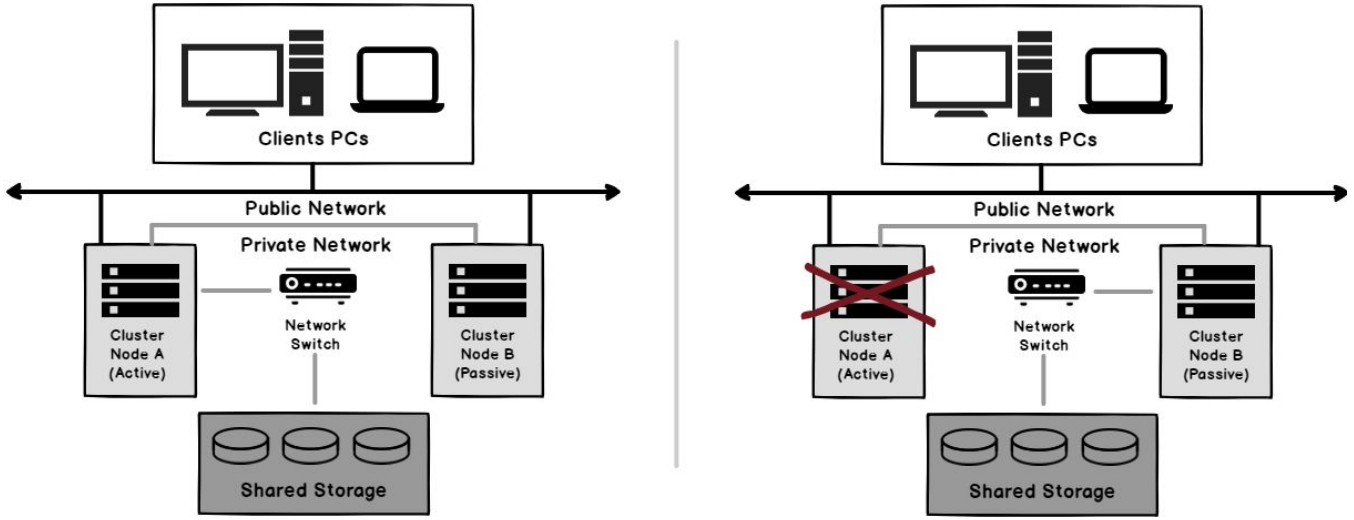
Always on Failover Cluster

Implementada a nível de Sistema operação com o nome WSFC ou Windows Server Failover Cluster.

Esta técnica consiste da utilização de computadores idênticos (ou muito similares), denominados nós (nodes) que vão formar um grupo (ou cluster) de forma que, a cada momento, apenas um dos nós responderá como 'ativo'.

Toda a informação é armazenada em compartimentos compartilhados (Shared Storage ou Shared Disk Array - fazendo referência à técnica de RAID), ou seja, quando um nó for desligado, qualquer outro pode assumir o 'mesmo' dado.

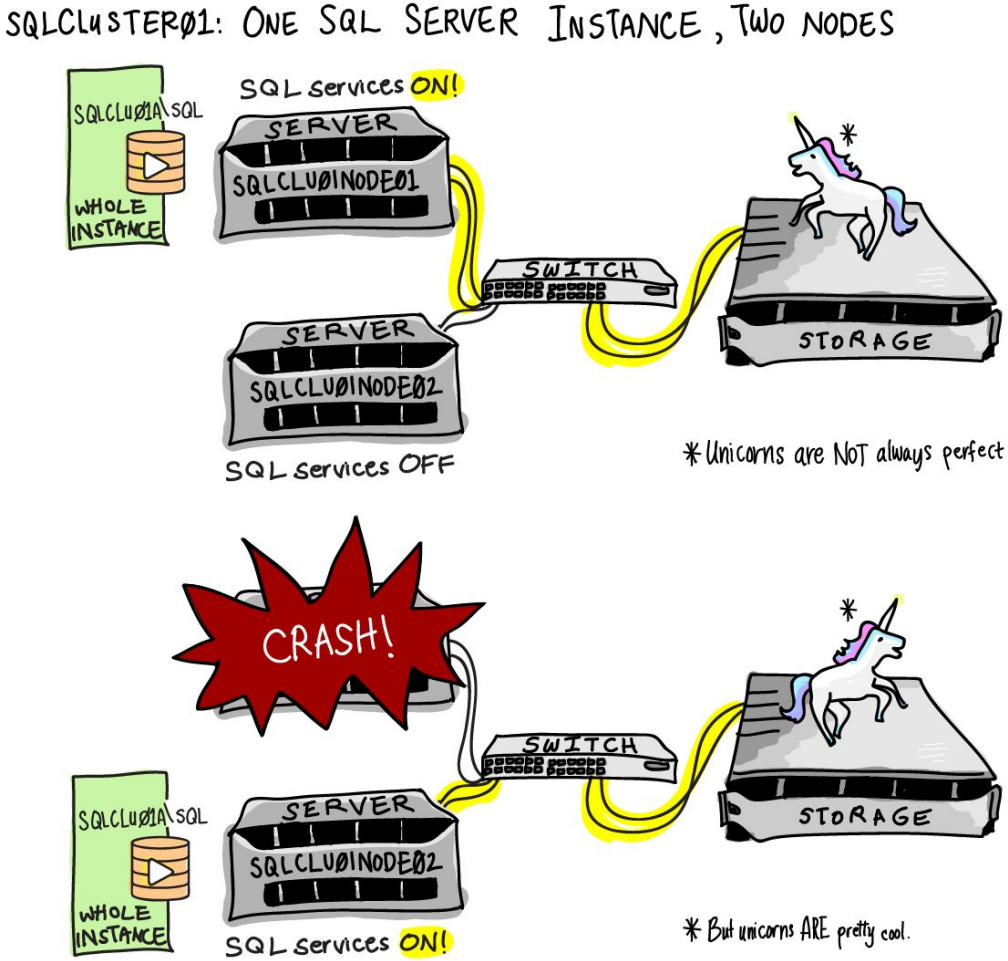
Note que esta técnica é feita a nível da instância, não do banco, ou seja, ela não utiliza o log transacional. Outro detalhe é que não há um processo específico para cópia dos dados.



Fonte: SQL Server Transaction Log and High Availability Solutions (sqlshack.com)

Always on Failover Cluster

Failover é uma operação de troca de servidores que usam o mesmo storage, nada mais.



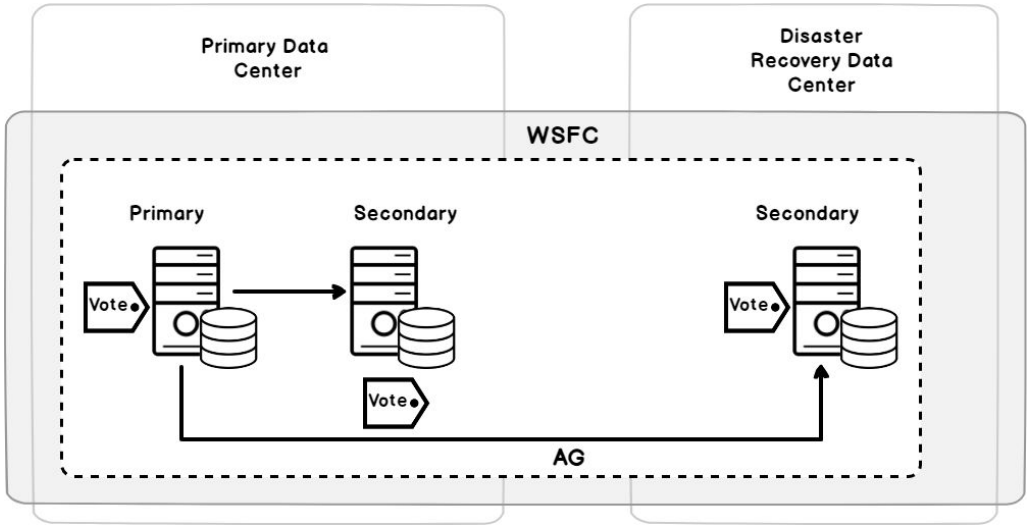
Fonte: [An Introduction to SQL Server Clusters with Diagrams (brentozar.com)]

Always on Availability Groups

Tecnologia criada utilizando-se como base o WSFC ou Windows Server Failover Cluster par a criação de um grupo de disponibilidade e opcionalmente um **listener** para 'responder' em nome do grupo.

Consiste da inclusão de réplicas em um grupo de disponibilidade, cada réplica recebe os dados, sincronizados pelo log transacional (da mesma forma que o espelhamento), porém, no AG as réplicas podem assumir o papel de somente leitura.

Permite também a realização de técnicas de balanceamento de carga de forma que a principal receba requisições de alteração (INSERT, DELETE, UPDATE, CREATE, ALTER, etc) mas todas as réplicas possam receber requisições de SELECT.



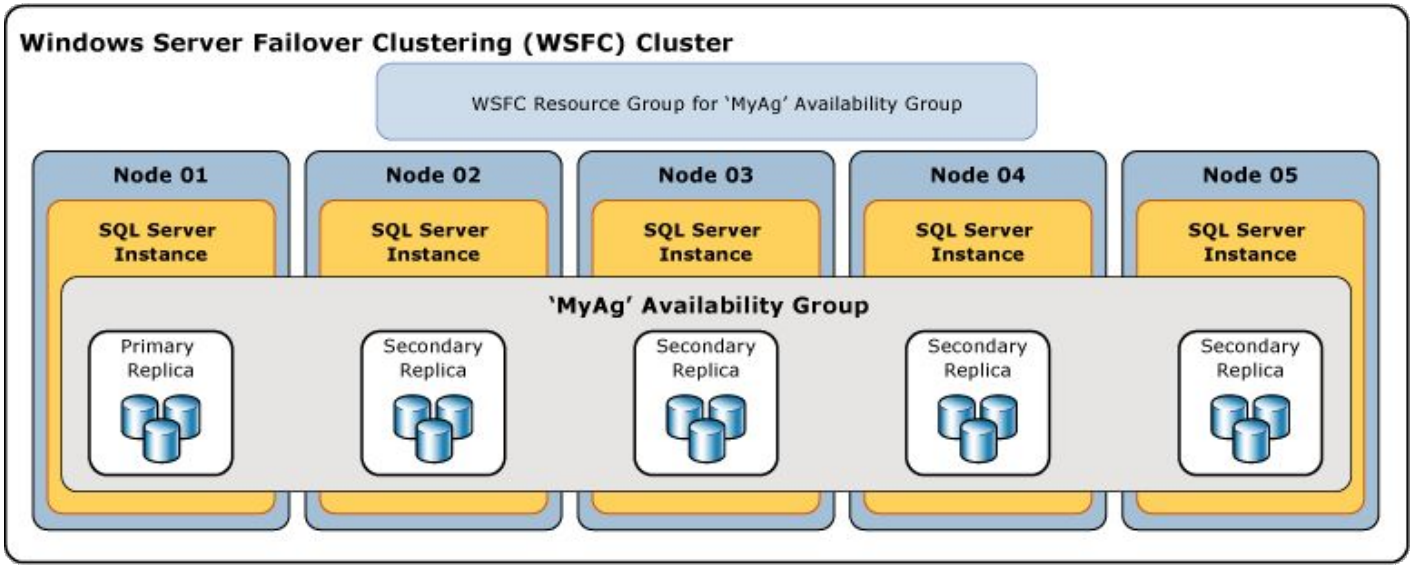
Fonte: SQL Server Transaction Log and High Availability Solutions (sqlshack.com)

Always on Availability Groups

Permite a sincronização nos modos de Asynchronous-commit mode (equivalente à opção Alta Performance da técnica de espelhamento) e Synchronous-commit mode (equivalente à opção Alta Segurança da técnica de espelhamento).

Não precisa (mas pode) compartilhar discos entre as máquinas (ver Shared Disk Array).

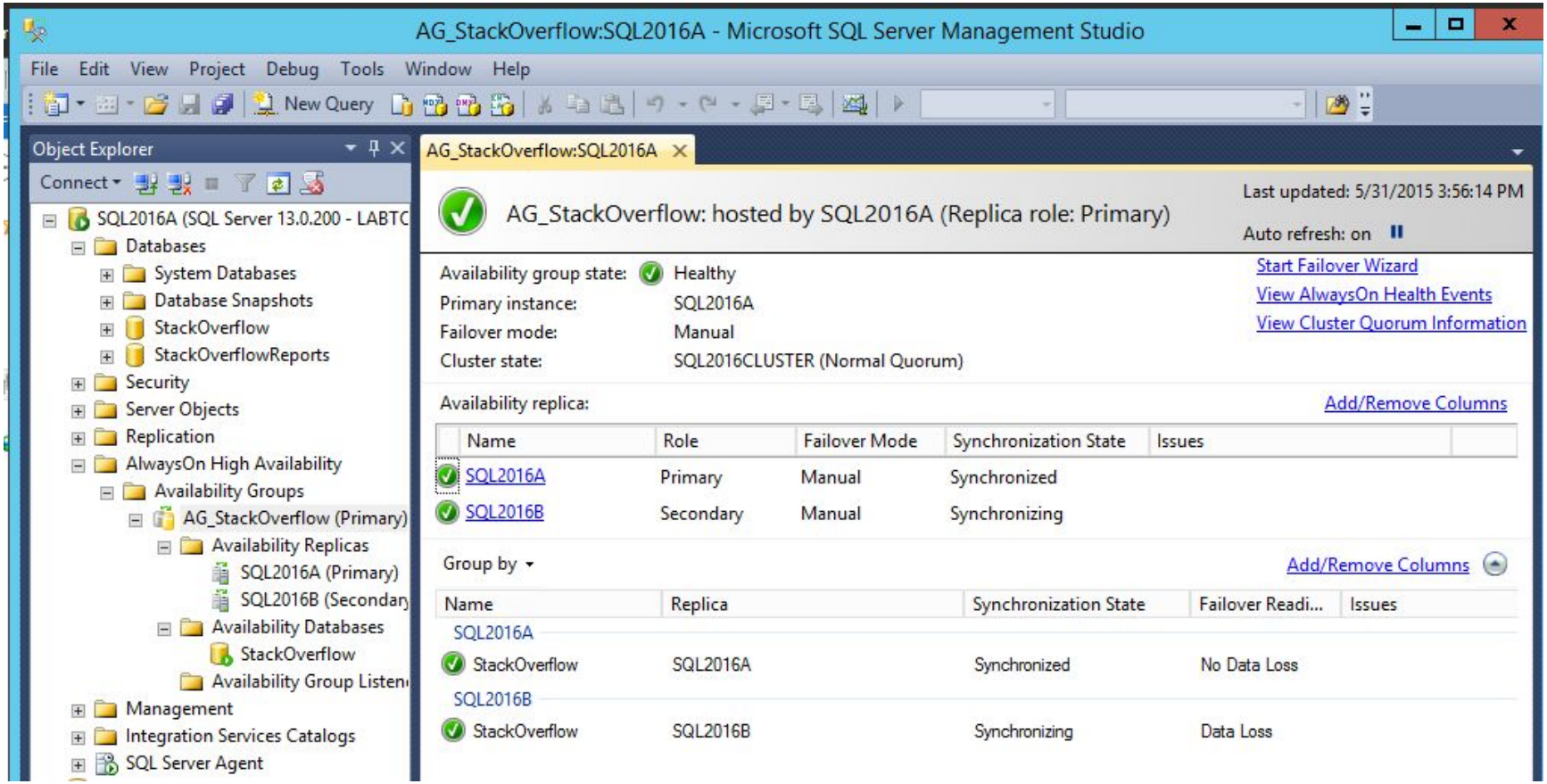
Permite o failover automático e transparente para qualquer máquina do grupo, porém o Failover [automático] não é causado por problemas no banco de dados, mas sim da instância (assim como na solução de Clustering).



Fonte: [O que é um grupo de disponibilidade Always On? - SQL Server Always On | Microsoft Docs]

Always on Availability Groups

Ambiente de acompanhamento e auditoria da saúde do grupo



Fonte: [How to Set Up Standard Edition Always On Availability Groups in SQL Server 2016 - Brent Ozar Unlimited®]

Prévia AC5

Ficha de comparação sobre Alta disponibilidade

Como prévia da AC5, preencha a ficha de comparação conforme instrução já passada em sala.

Técnica	Principal Finalidade	Janela de perda	Tipo de Failover	Qtde Réplicas	Reversibilidade	Status Réplica	Nível Sincronização	Setup / Recomendações (Liste os números)	Edição mínima	Versão mínima	Disp. Azure
LS											
Rep											
PtP											
Mirror											
WSFC											
AG											

Dúvidas ?

- Fale com o professor
- Sigam as referências previamente incluídas nos slides.
- Usem a internet para pesquisa de conteúdo

Obrigado

Segurança de dados

Aula 12 – Alta Disponibilidade - parte 3

Gustavo Bianchi Maia
gustavo.maia@faculdadeimpacta.com.br