Segurança de dados

Aula 10 – Alta disponibilidade - parte 1

Gustavo Bianchi Maia

gustavo.maia@faculdadeimpacta.com.br

Sumário

- Revisão - Termos da Segurança da Informação
- Introdução à Alta Disponibilidade
  - Problemas
  - Estratégias
  - Aferição
- Técnica Log Shipping
- AC3

Segurança da Informação

O que é informação ? (DICS)

Dado contexto/significado Informação

Informação usada / aplicada Conhecimento

Conhecimento uso coerente / experiência Sabedoria

Ciclo de vida da informação *Cada etapa requer controles específicos sobre a informação

Criada Armazenada Processada Transmitida Usada ...

... Descartada / Perdida / Destruida

Arquitetura é armazenamento estruturado (classificado e segregado) e intuitivo (uso fácil e rápido) para garantir que a informação seja levada até o usuário.

Análise e gerenciamento da informação é uma sequência de ‘fluxos’ dentro de uma organização para: planejar, coletar, organizar, usar e divulgar suas informações

Confiabilidade da informação

A garantia da confiabilidade é feita por três requisitos básicos:

Confidencialidade – garantia de acesso restrito à informação
- Exclusividade – apenas usuários ou grupos autorizados
- Privacidade – garantia / proteção sobre o acesso exclusivo.

Integridade – garantia de preservação de estado.
- Autenticidade – garantia de propriedade da informação original
- Não-repúdio – impossibilidade de negar responsabilidade sobre uma ação
- Auditabilidade – devida checagem da origem e consistência da informação

Disponibilidade – garantia de uso contínuo da informação
- Pontualidade – informação disponível quando necessária
- Continuidade – garantia do uso mesmo em caso de desastre
- Robustez – garantia de capacidade operacional suficiente

Definições de segurança

Vulnerabilidade – fraqueza ou grau em que algo pode ser explorado

Internas – causada por ações, processos ou algo sob o controle da companhia. Podem ser eliminadas ou reduzidas.

Externas – causada por ações externas fora do controle. Normalmente não podem ser eliminadas e nem sempre reduzidas o suficiente, ex: terremotos, greves, queda da bolsa de valores.

Ameaça – causa potencial capaz de explorar uma vulnerabilidade

Humanas – Hackers (black / grey / white Hat), Funcionários, Engenharia Social

Não Humanas – Infraestrutura, eventos naturais (terremotos).

Risco – probabilidade que uma ameaça explore uma vulnerabilidade

Incidente – Evento ou ocorrência da ameaça

Dano – Consequência do incidente. Prejuízo aos ativos.

Diretos – Causam prejuízo direto ao negócio em decorrência direta do incidente.

Indiretos – Dano posterior ou consequência. Ex: incapacidade de cumprir um contrato

Recuperação – uso de medidas ou ações sobre o dano.

Gerenciamento de riscos

É um processo contínuo que se utiliza de medidas de segurança para identificar, examinar e reduzir à um nível aceitável os riscos ao negócio.
Trata das ameaças ao negócio e não necessariamente as vulnerabilidades.

Análise de riscos é o processo em que se visa:

- Identificação dos ativos e seu valor (o que proteger)
- Determinar as vulnerabilidades e suas possíveis ameaças.
- Determinar os riscos (probabilidades)
- Determinar o equilíbrio entre viabilidade de custos e implantação das medidas de segurança

A **análise dos riscos** pode ser feita das seguintes formas:

- **Quantitativa**: determina as probabilidades numericamente, o grau provável de perda (nível do prejuízo) por evento. *Difícil de ser realizada, muitos bens não tem valor estimável (Ex: monalisa , reputação).
- **Qualitativa**: determina as ameaças e a extensão da exploração das vulnerabilidades, assim como contra-medidas em caso de incidentes. *Baseada em processos de estimativa (brainstorming), classificações de gravidade.

Estratégias de risco significa que todo risco deve ser:

- **Evitado** – risco zero, prevenção total, imunização
- **Neutralizado** – risco reduzido, dano mínimo, há garantias.
- **Aceito** – não compensa atuar.

Gestão de continuidade de negócio (GCN)

O objetivo é evitar a interrupção dos processos, atividades e tecnologias essenciais ao negócio, proteger seus ativos e ajudar na sobrevivência frente à situações de crise ou desastre.

Segundo a ISO 22.301 um plano de continuidade de negócio (PCN) requer:

- Amplo conhecimento do negócio
- Estratégias de continuidade para: pessoas, processos e tecnologias
- Plano de respostas associadas ao plano de GCN
- Auditorias para manter e exercitar o plano (testes / simulados)
- Criação de uma cultura organizacional sobre o plano GCN

Um PCN é um conjunto de planos ações e estratégias e é composto por:

- **PGC**: Plano de gestão de crises
  Foco em cenários de crises, com destruição total ou sem recuperação em tempo hábil.
- **PCO**: Plano de continuidade operacional / Plano de contingência
  Foco em processos críticos e essenciais ao negócio – determinados pela BIA / AIN
- **PRD**: Plano de recuperação de desastres
  Foco em tecnologias críticas que suportam o negócio. Ex: email, internet, ERPs, etc.

Por que Alta Disponibilidade?

O PCN precisa que o termo Disponibilidade seja levado ao “extremo” [possível], pois:

- Vulnerabilidades sempre vão existir.
- Maior parte das ameaças não são eliminadas e novas ameaças são ‘criadas’ [ou descobertas] o tempo todo.
- Grande parte dos riscos não é identificado ou quando é apenas são assumidos.
- Maior parte dos ‘problemas’ são de causas internas (hardware, energia, mal uso)
- Cada dado perdido é informação ou conhecimento desperdiçado.
- Cada segundo fora do ar resulta em prejuízos financeiros e de reputação que podem ser irrecuperáveis.

Só um PRD não é suficiente, pois, quando elas são acionadas, significa que já houve prejuízo ou perda.

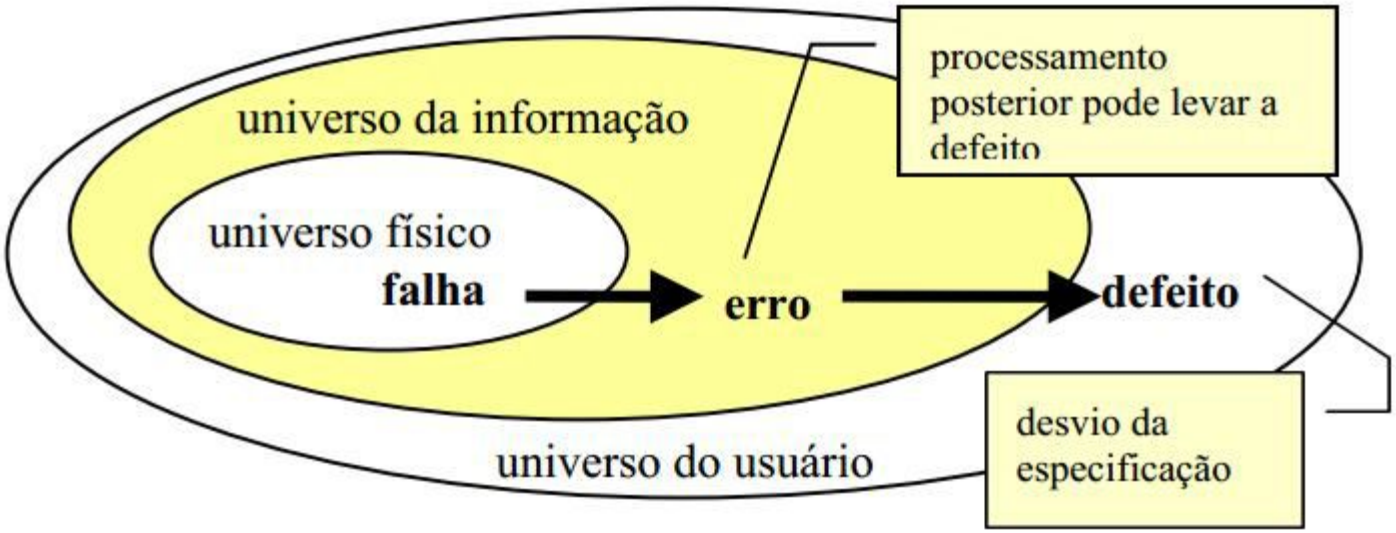
As medidas de Alta Disponibilidade fazem parte do PCO.

Classificação dos problemas.

Um **defeito** (failure) é definido como um desvio da especificação, estão mais próximos do usuário e portanto, podem ser corrigidos por treinamento, revisões de código ou especificações, exceto quando eles foram causados por erros ou falhas.

Erros (errors) são situações em que um processamento ou estado errôneo quando ocorrido, pode levar ao defeito. Podem ser corrigidas por revisão de código ou especificações, exceto quando eles foram causados por falhas.

Falhas são definidas como a causa física ou algorítmica do erro, de sistemas dedicados ou servidores.



Fonte: http://www.inf.ufrgs.br/~taisy/disciplinas/textos/ConceitosDependabilidade.PDF

Sistemas tolerantes à falhas.

Como falhas são críticas, porém são também inevitáveis, um dos objetivos da alta disponibilidade é tornar os sistemas tolerantes à falhas, evitando que falhas de hardware ou de software em servidores.

As principais causas de falhas são problemas de especificação, problemas de implementação, componentes defeituosos, imperfeições de manufatura, fadiga dos componentes físicos além de distúrbios externos como radiação, interferência eletromagnética, variações ambientais (temperatura, pressão, umidade) e também problemas de operação.

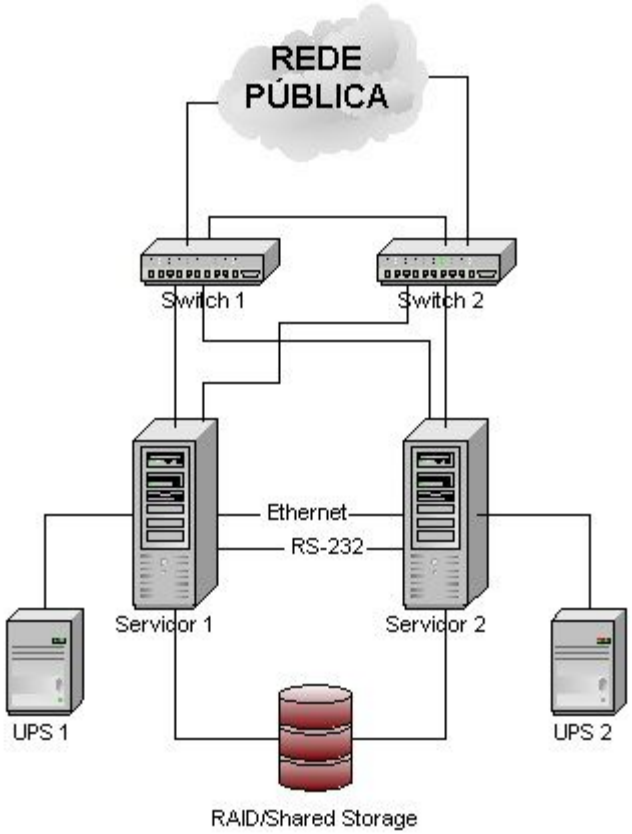
Sistemas tradicionais			
Não tolerante a falhas		**Tolerante a falhas**	
Mean time to failure: 6 a 12 semanas Indisponibilidade após defeito: 1 a 4 h		Mean time to failure: 21 anos (Tandem)	
Defeitos:		**Defeitos:**	
hardware	50%	software	65%
software	25%	operações	10%
comunicações / ambiente	15%	hardware	8%
operações	10%	ambiente	7%

Fonte: http://www.inf.ufrgs.br/~taisy/disciplinas/textos/ConceitosDependabilidade.PDF

Estratégias

A principal estratégia é através da eliminação dos chamados pontos únicos de falha, ou **SPOF** da sigla em inglês para **single-point-of-failure**, pela criação ou implantação de sistemas de contingência, também chamados de sistemas redundantes, para cada ponto crítico do conjunto de servidores.

Quanto mais **redundância** existir, menores serão os **SPOF** (Single Point Of Failure), e menor será a probabilidade de interrupções no serviço

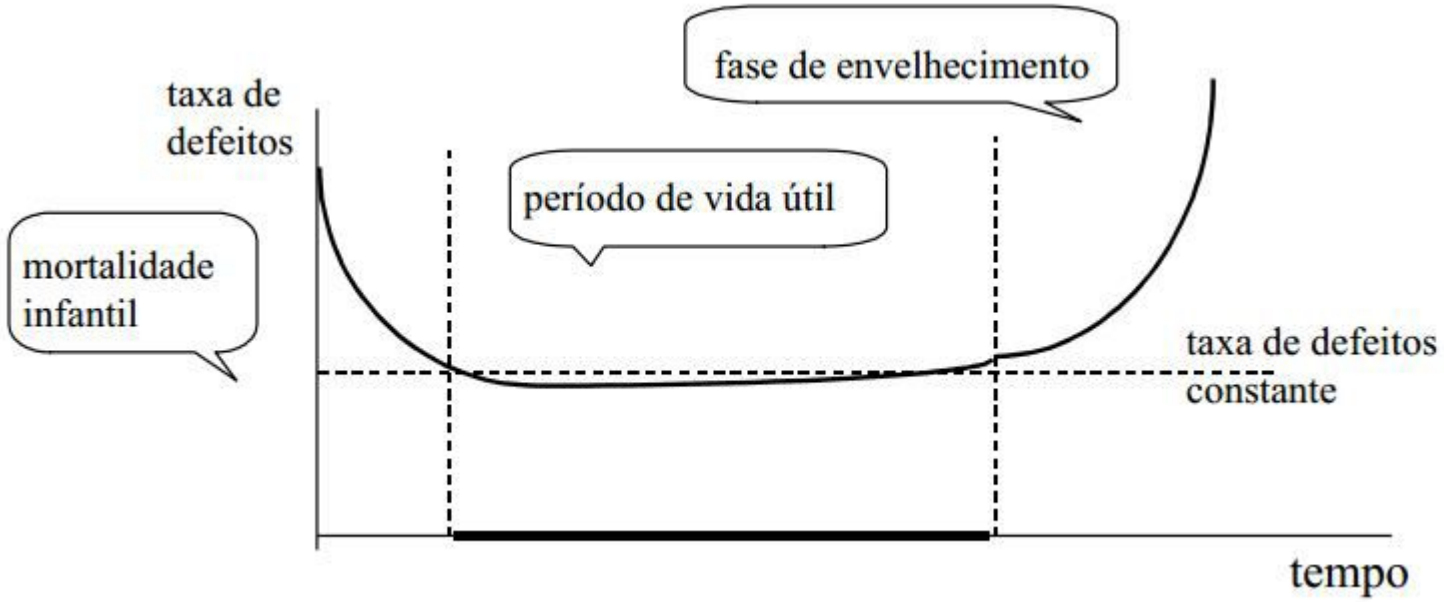


Fonte: [Sistema de alta disponibilidade – Wikipédia, a enciclopédia livre (wikipedia.org)]

Ciclos de vida

A taxa de defeitos de um componente é dada por falhas por unidade de tempo e varia com o tempo de vida do componente. Uma representação usual para a taxa de defeitos de componentes de hardware é dada pela curva da banheira, nela são identificadas as seguintes fases:

- mortalidade infantil: componentes fracos e mal fabricados
- vida útil: taxa de falhas (defeitos) constante
- envelhecimento: taxa de falhas crescente



Fonte: http://www.inf.ufrgs.br/~taisy/disciplinas/textos/ConceitosDependabilidade.PDF

Como medir Alta Disponibilidade ?

Uptime: tempo que o sistema está ativo / operando

Downtime: tempo que o sistema está inativo / inoperante

SLA - Service Level Agreement - Acordo com previsão de multa, de garantia de tempo de UPTIME em percentual.

SLO - Service Level Objective - Objetivo, sem previsão de multa, de meta de tempo de UPTIME em percentual.

Disponibilidade (%)	Downtime/ano	Downtime/mês
95%	18 dias 6:00:00	1 dias 12:00:00
99%	3 dias 15:36:00	0 dias 7:12:00
99,9%	0 dias 8:45:35.99	0 dias 0:43:11.99
99,99%	0 dias 0:52:33.60	0 dias 0:04:19.20
99,999%	0 dias 0:05:15.36	0 dias 0:00:25.92

High availability - Wikipedia

Como medir Alta Disponibilidade ?

A tolerância a falhas consiste, basicamente, em ter hardware/software redundante que entra em funcionamento automaticamente após a detecção de falha do hardware/software principal.

Independentemente da solução adoptada, existem parâmetros que possibilitam mensurar o grau de tolerância a falhas.

Taxa de defeitos - failure rate, hazard function, hazard rate	número esperado de defeitos em um dado período de tempo, assumido um valor constante durante o tempo de vida útil do componente.
MTTF - mean time to failure	tempo esperado até a primeira ocorrência de defeito
MTTR - mean time to repair	tempo médio para reparo do sistema
MTBF - mean time between failure	tempo médio entre as falhas do sistema

Simulação

Você foi contratado como gerente de uma garagem e tem a missão de NUNCA deixar o presidente da companhia sem um carro.

Foi-lhe dado uma verba de $$$$$$ (6 x $) e você tem que escolher entre a solução do fornecedor importado ou do fornecedor nacional.

(*) os valores e dados utilizados nesta simulação são hipotéticos

Você tem que fazer um planejamento para 5 anos e após reuniões com os representantes você chegou à seguinte planilha com valores de MTTF, MTTR e MTBF.

	Custo	Qtde	MTTF	MTTR	MTBF
Carro Importado	$$$	2	3 anos	30 dias	1 ano
Carro Nacional	$$	3	1 ano	7 dias	6 meses

Qual opção é a menos arriscada ?

(ou seja, que lhe garantiria maior disponibilidade)

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

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

Em uma estratégia de alta disponibilidade esta estratégia contem as piores taxas de MTTR (mean time to repair), em vista que os backups demoram para serem restaurados, além de normalmente ocasionarem perdas de dados.

Para reduzir as perdas e tornar esta técnica o mais viável possível, é muito comum realizar backups o mais próximo possível, num plano ainda mais restrito como o visto na última aula.

Para que esta estratégia tenha um MTTR relativamente baixo, é recomendado também armazenar permissões, jobs, outros bancos não essenciais etc. (lembre-se, nem sempre só um banco é comprometido).

***Nota: Pela microsoft toda técnica que não garante zero downtime ou zero perda de dados durante uma operação de failover é considerada DR e não HA, isso excluiria Log Shipping e Replicação (transacional) como técnicas de alta disponibilidade, mas como veremos, elas diferem em MUITO de um simples BACKUP / RESTORE por isso ainda são classificadas como HA/DR.**

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:

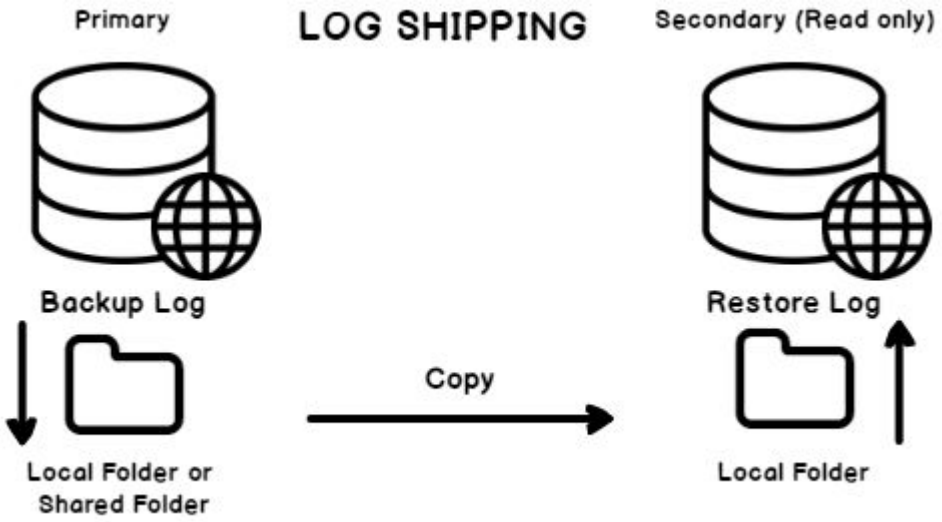
- **Status da réplica / Usos extras para o servidor Secundário**
  - Capacidade de uso das réplicas para algo mais além da função de alta disponibilidade, afetado diretamente pelo tipo de recuperação (ou status) das réplicas.
  - **Opções: Não** (NORECOVERY)**, RO** - Read Only (STANDBY)**, RW** - Read 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

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”.

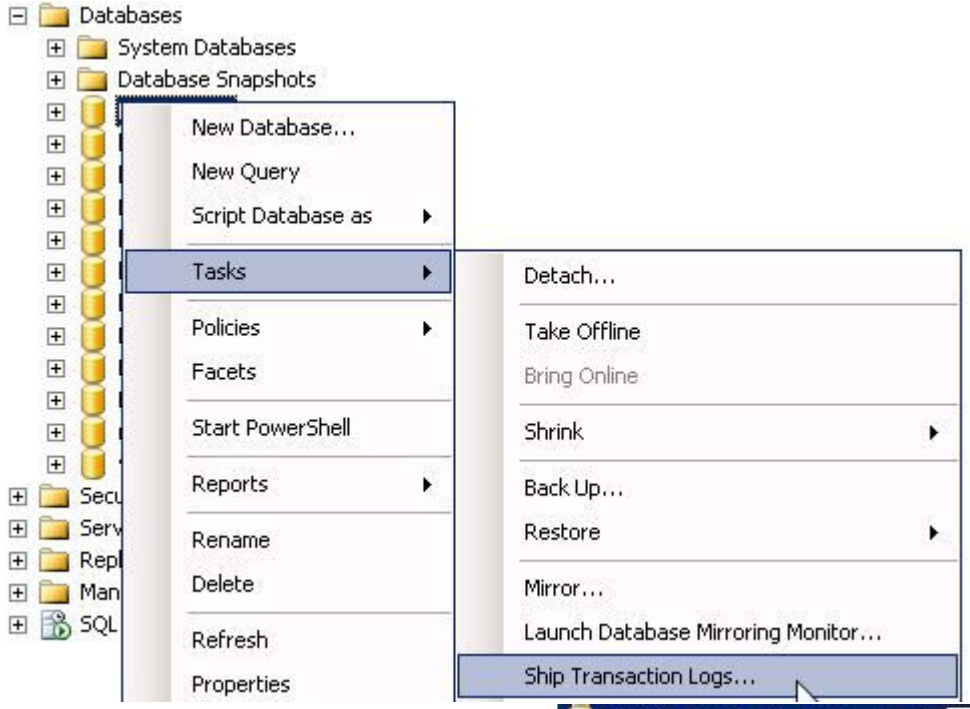
São necessários bancos diferentes para a realização de log shipping, mas por segurança é recomendado que o restore seja realizado em um servidor físico, geograficamente isolado do principal.

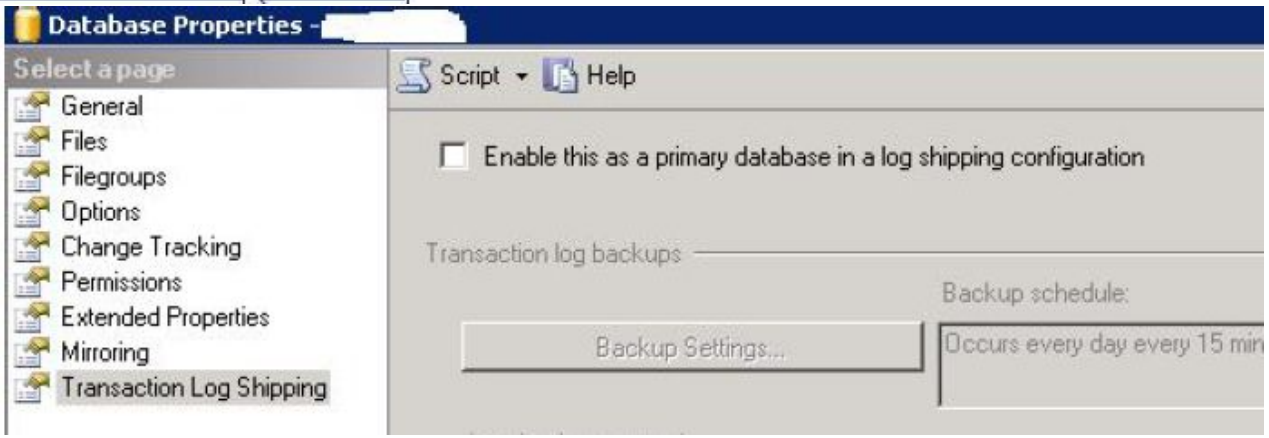
Atua a nível de banco de dados, que devem estar em modo de recuperação FULL.
O(s) servidor(es) secundário(s) pode estar em modo somente leitura.
Posso ter um servidor com o papel de monitoria, porém, ainda se recomenda failover manuais.



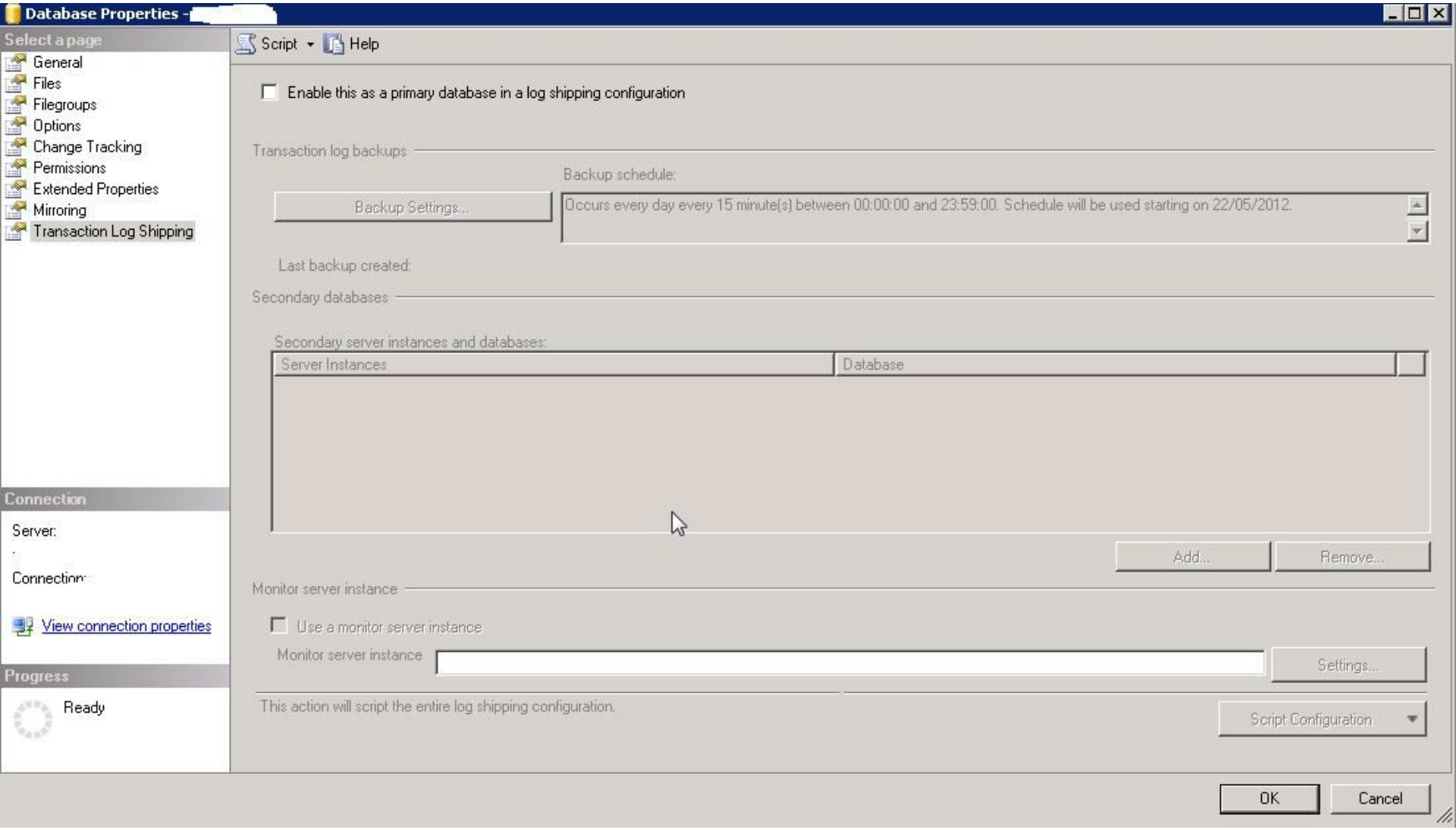
Fonte: SQL Server Transaction Log and High Availability Solutions (sqlshack.com)

Log Shipping - Automático

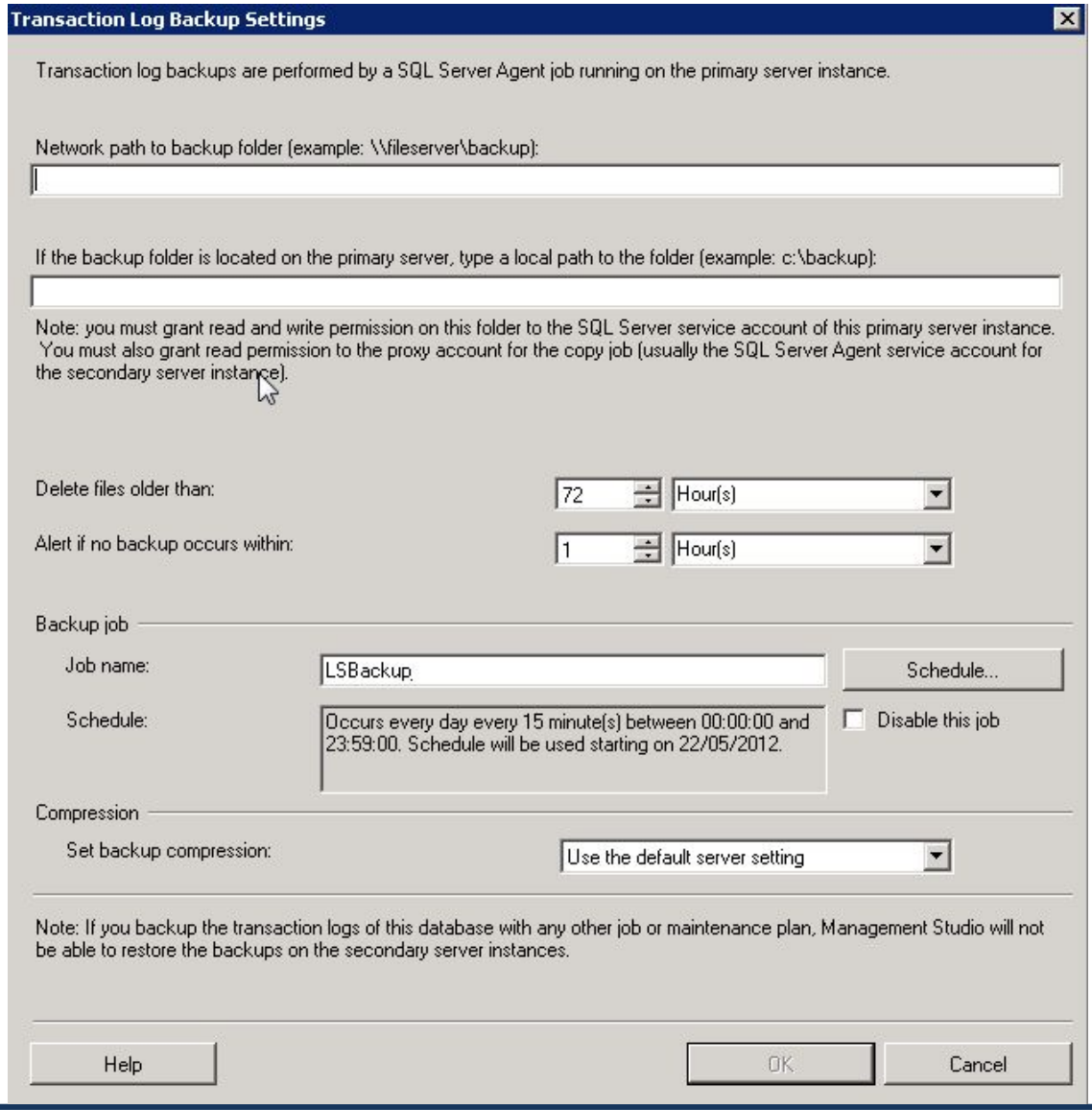




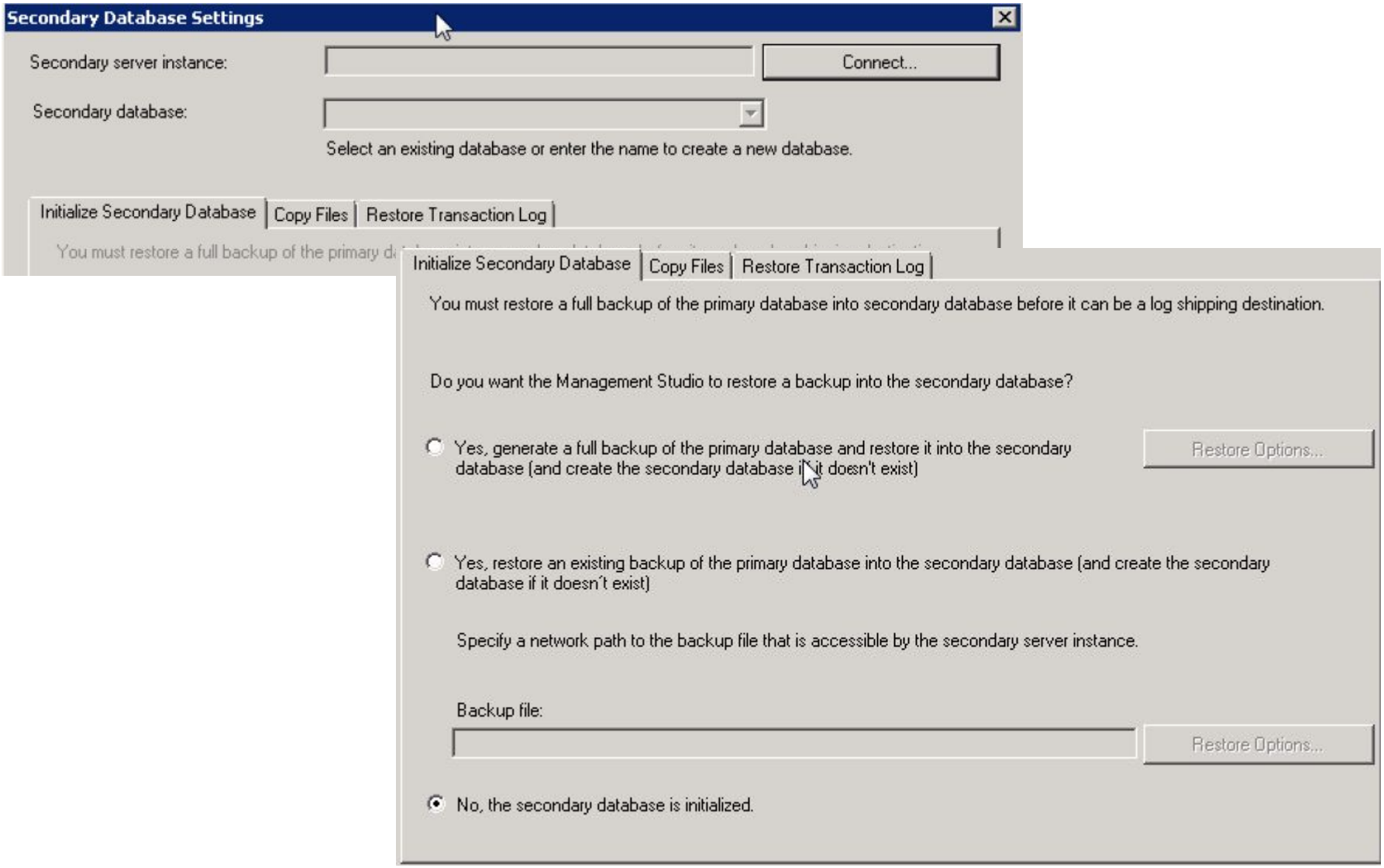
Log Shipping - Automático



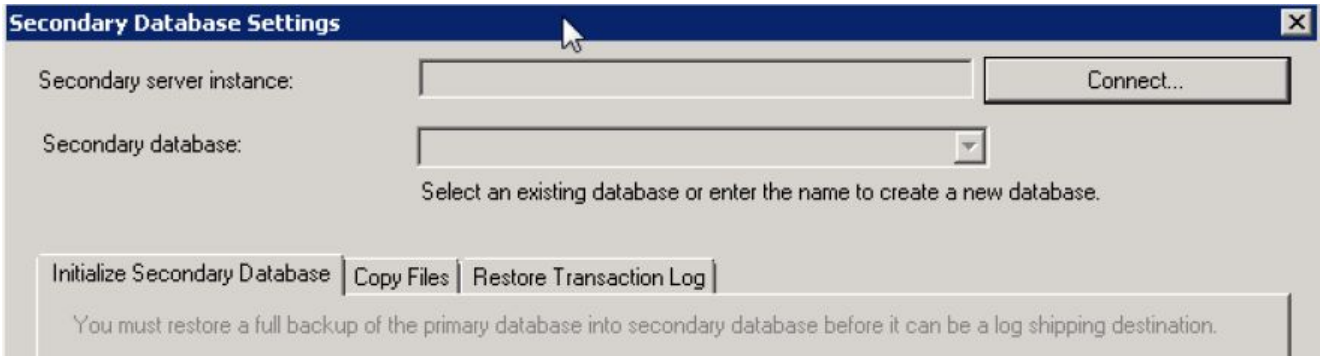
Log Shipping - Automático

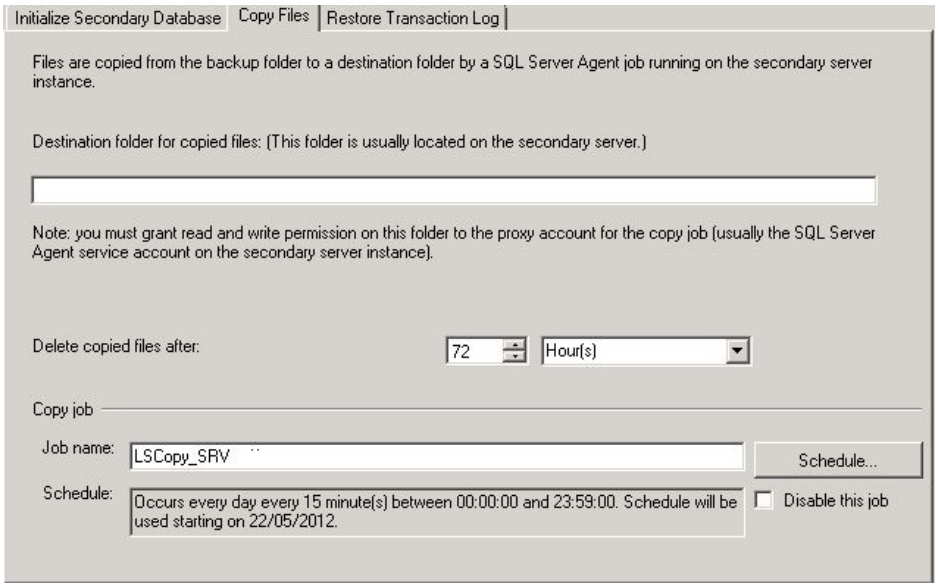


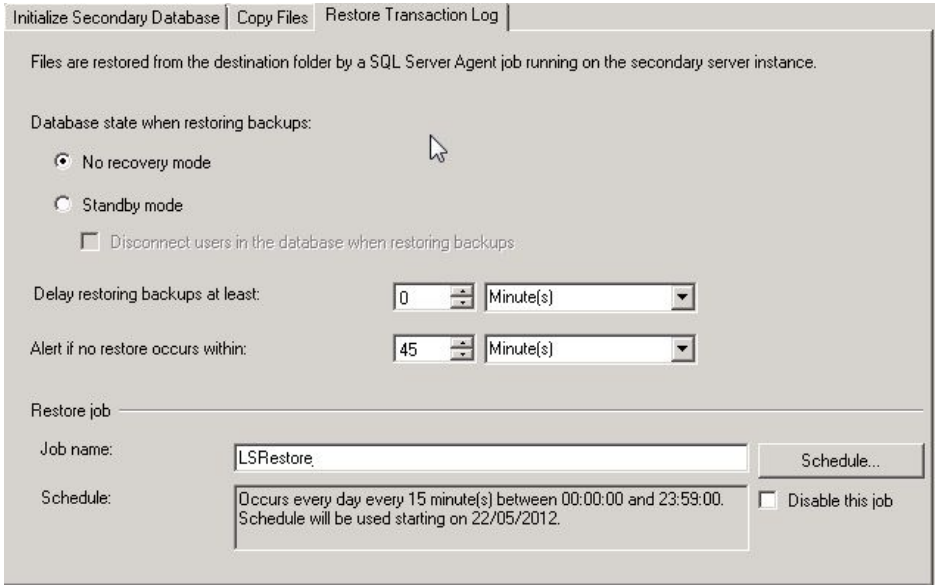
Log Shipping - Automático



Log Shipping - Automático





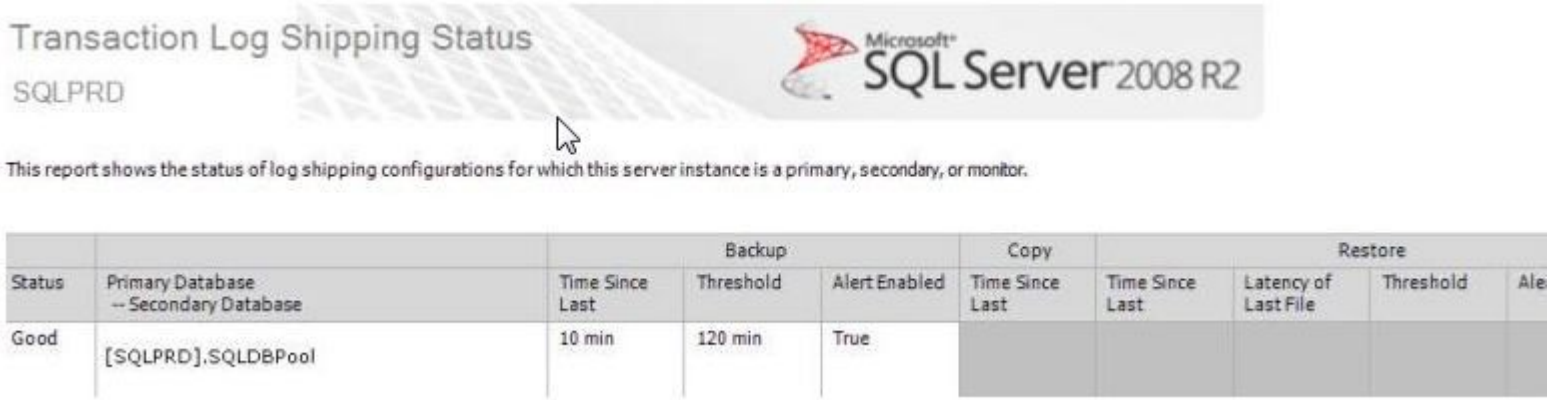


Log Shipping - Automático

Monitorando

Master.dbo.sp_help_log_shipping_monitor

Standard Server Report Transaction Log Shipping Status



Transaction Log Shipping Status

SQLPRD

Microsoft SQL Server 2008 R2

This report shows the status of log shipping configurations for which this server instance is a primary, secondary, or monitor.

		Backup			Copy	Restore			
Status	Primary Database -- Secondary Database	Time Since Last	Threshold	Alert Enabled	Time Since Last	Time Since Last	Latency of Last File	Threshold	Ale
Good	[SQLPRD].SQLDBPool	10 min	120 min	True					

Log Shipping - Implementação Manual

Principal	Principal	Secundario	Secundario
Inicialização			
BACKUP FULL do banco PRINCIPAL			
Cópia para repositório no SECUNDARIO			
		RESTORE em modo NORECOVERY	
Repetição			
BACKUP de LOG do banco PRINCIPAL			
Registro do Backup em tabela de controle (Linked server com SECUNDARIO)		Recebe dados na tabela de controle	
Cópia para repositório no SECUNDARIO			
		Ler tabela de controle, para cada pendência RESTORE do LOG em modo STANDBY Registra Restore e retira pendência.	
Failover			
Banco Offline OU RESTORE em modo NORECOVERY		RESTORE em modo RECOVERY	

AC3 - Completa

AC3 - Implementação de LOG Shipping Manual

Critérios de sucesso / Pontuação:
4 pts – Ambiente configurado (Máquinas virtuais, portas, SQL com linked servers)
+2pts – Você implementou os 2 primeiros Jobs de Setup (1,2), sem agendamento.
+2pts – Você implementou os 2 jobs de Trabalho (3,4) em jobs com execução automática.
+2pts – Você implementou o último Job (5) que automaticamente promove o servidor secundário em primário no caso de falha (status = offline) do primário (FAILOVER).

Tarefa: Crie 5 JOBS (Tarefas agendadas), distribuídos da seguinte forma:

Tarefas (Jobs) de SETUP (sem agendamento, utilizados para o SETUP ou o RESET do ambiente)
No servidor Principal:

- #1 - Job de Backup Database
  - Passo #1 - Realizar o backup do banco de dados principal em um disco local.
  - Passo #2 - Reset da tabela de controle (Truncate ou SET do bit restaurado para 1)
  - Passo #3 - Realizar a cópia do arquivo de backup local para o secundário.

  Não criar agendamento, será utilizado apenas para 'resetar' o ambiente

No servidor Secundário:

#2 - Job de Restore Database
- Passo #1 - Realizar o restore do banco de dados sobre o banco secundário.

Não criar agendamento, será utilizado apenas para 'resetar' o ambiente

AC3 - Implementação de LOG Shipping Manual

Tarefas (Jobs) de Trabalho (com agendamento, atenção com o offset do restore)
No servidor Principal:

- #3 - Job de Backup Log
  - Passo #1 - Realizar o backup do log banco de dados principal em um disco local.
    (Atualizar tabela de controle no servidor secundário, registrando o backup)
  - Passo #2 - Realizar a cópia do arquivo de backup local para o secundário.

  Criar agendamento para execuções de 5 em 5 mins (sem offset - 00:00, 00:05, 00:10 ...)

No servidor Secundário:

#4 - Job de Restore Log

- Passo #1 - Realizar o restore do log banco de dados sobre o banco secundário.
  (Ler o que deve ser restaurado da tabela de controle a marcá-los como 'restaurado')

Criar agendamento para execuções de 5 em 5 mins (offset+1 - 00:01, 00:06, 00:11 ...)

Tarefas (Jobs) de Failover
No servidor secundário:

#5 - JOB de "Failover"

- Passo #1 - Verificar o status do servidor principal e, caso este não esteja 'online' promova o servidor secundário a primário, ou seja, altere o status do banco de standby para recovery.

Criar agendamento para execuções de 1 em 1 min
(opcionalmente: desligue os jobs de Trabalho para que eles não sejam mais executados)

Demonstre a implementação para o professor.
Esta entrega não pode ser feita por email, ou seja, é uma apresentação presencial.
Se prepare para responder à 1 ou 2 questões (chamada oral) sobre seu processo.

AC3 - Dicas

```
--Seja uma tabela de controle criada no servidor SECUNDARIO
-- porém em outro banco de dados que não o SECUNDARIO
CREATE TABLE ctrl_backups
  (
     id         INT NOT NULL IDENTITY(1, 1),
     arquivo    VARCHAR(255) NOT NULL,
     restaurado BIT NOT NULL DEFAULT(0),
     data       DATETIME NOT NULL DEFAULT (Getdate()),
     CONSTRAINT pk_ctrl_backups PRIMARY KEY (id)
  )

go
```

AC3 - Dicas

```
--NO JOB DE BACKUP...
DECLARE @NOME_BACKUP VARCHAR(255)

SELECT @NOME_BACKUP = 'C:\BD\BACKUPS\impacta_'
                    + CONVERT(VARCHAR(max), Getdate(), 112)
                    + LEFT(Replace(Replace(CONVERT(VARCHAR(max), CONVERT(TIME,
                          Getdate())), ':', ''), '.', ''), 6)
                    + '.BAK'

--SELECT @NOME_BACKUP -- C:\BD\BACKUPS\impacta_20200923203508.BAK
BACKUP log [impacta] TO DISK = @NOME_BACKUP WITH init

INSERT INTO ctrl_backups (arquivo)
VALUES     ( @NOME_BACKUP )
```

AC3 - Dicas

```
--restore sem cursor
DECLARE @ARQUIVO VARCHAR(50)
WHILE EXISTS (SELECT TOP 1 arquivo
              FROM   ctrl_backups
              WHERE  restaurado = 0
              ORDER  BY data)
  BEGIN
      --peque o primeiro arquivo
      SELECT TOP 1 @ARQUIVO = arquivo
      FROM   ctrl_backups
      WHERE  restaurado = 0
      ORDER  BY data

      RESTORE log [impacta_ha]
          FROM DISK = @ARQUIVO
          WITH standby = 'C:\BD\TRN\standby.trn'

      UPDATE ctrl_backups SET    restaurado = 1
      WHERE  arquivo = @ARQUIVO
  END
```

AC3 - Dicas

```
-- exemplo de restore com cursor
DECLARE @ARQUIVO VARCHAR(50)
DECLARE arquivos CURSOR local FOR  (
     SELECT arquivo FROM   ctrl_backups WHERE  restaurado = 0)
OPEN arquivos
FETCH next FROM arquivos INTO @ARQUIVO
WHILE ( @@FETCH_STATUS = 0 )
  BEGIN

      RESTORE log secundario FROM DISK = @ARQUIVO WITH standby =
      'C:\BD\TRN\standby.trn'

      UPDATE ctrl_backups
      SET    restaurado = 1
      WHERE  arquivo = @ARQUIVO
      FETCH next FROM arquivos INTO @ARQUIVO
  END
CLOSE arquivos
DEALLOCATE arquivos
go
```

AC3 - Preparação para apresentação

```
--cenário inicial: devem estar iguais
SELECT * FROM   [principal].[principal].dbo.teste
SELECT * FROM   [secundario].[secundario].dbo.teste

--mude algo no banco principal...
INSERT INTO [principal].[principal].dbo.teste VALUES(...)

--neste momento, as tabelas estarão diferentes...
SELECT * FROM   [principal].[principal].dbo.teste --contém 1 linha extra
SELECT * FROM   [secundario].[secundario].dbo.teste

--rodar os jobs #3 e #4 e/ou aguardar execução automática dos jobs
WAITFOR delay '00:01:00' --aguardar 1 min

--neste momento, as tabelas voltaram a ficar iguais
-- pois os jobs #3 e #4 fizeram a atualização
SELECT * FROM   [principal].[principal].dbo.teste
SELECT * FROM   [secundario].[secundario].dbo.teste --recebeu a 1 linha extra
```

Obrigado

Segurança de dados

Aula 10 – Alta Disponibilidade - parte 1

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