



5 - Configuração de Conexões Seguras e Protocolos de Banco no OGG

Oracle GoldenGate — Segurança, Credenciais e Protocolos de Rede para Ambientes de Replicação

Objetivos da Aula

Ao final desta aula, você será capaz de dominar os seguintes tópicos essenciais do Oracle GoldenGate:

1

Credential Store

Eliminar senhas em texto puro utilizando o repositório de segurança do OGG.

2

USERIDALIAS

Configurar e gerenciar o parâmetro USERIDALIAS nos processos de Extract e Replicat.

3

Protocolos de Rede

Compreender a diferença prática e de performance entre TCP, Bequeath (BEQ) e IPC para o GoldenGate.

4

tnsnames.ora Multitenant

Customizar o arquivo tnsnames.ora focado no ecossistema Multitenant do OGG.



Segurança em Primeiro Lugar: O Credential Store e o USERIDALIAS

❌ O Passado: Senha em Texto Puro

No passado do GoldenGate, era comum abrir o arquivo de parâmetros de um Extract e encontrar a linha de conexão escrita assim:

```
USERID ggadmin, PASSWORD minha_senha_secreta
```

Isso é uma **falha de segurança gravíssima** — um prato cheio para auditorias reprovarem o ambiente inteiro.

✅ O Presente: Credential Store

Na arquitetura moderna, o padrão obrigatório é o uso do **Credential Store** (Repositório de Credenciais). Os dados de login — Usuário, Senha e Connection String — são mascarados dentro de um **cofre criptografado** do GoldenGate sob um codinome chamado **Alias**.

Nos arquivos de parametrização .prm, passamos apenas a instrução:

```
USERIDALIAS <nome_do_alias>
```

- ✅ O Credential Store é o padrão obrigatório em ambientes corporativos modernos com Oracle GoldenGate. Nunca exponha senhas em arquivos de parâmetros.



Prática: Consultando o Cofre de Credenciais

Para validar quais aliases estão criados e para quais bancos e portas eles apontam no ecossistema do OGG, utilizamos o comando `INFO CREDENTIALSTORE` informando o domínio de segurança — geralmente `OracleGoldenGate` por padrão.

Comando no Admin Client ou GGSCI

```
INFO CREDENTIALSTORE DOMAIN OracleGoldenGate
```

Exemplo de Saída Esperada

Domain: `OracleGoldenGate`

Alias: `ggeast`

Userid: `ggadmin@dc1.example.com`

`:1521/DBEAST.example.com`

O que este resultado nos diz?

Alias: `ggeast`

O codinome utilizado nos arquivos `.prm` dos processos Extract e Replicat.

Userid: `ggadmin@dc1.example.com`

O usuário real do banco de dados, encapsulado de forma segura no cofre.

Porta e Host: `:1521/DBEAST.example.com`

O banco de dados real, a porta e o host ficam encapsulados no alias de forma limpa e segura.

Escolha do Protocolo de Rede: A Armadilha do IPC e o Ganho de Performance

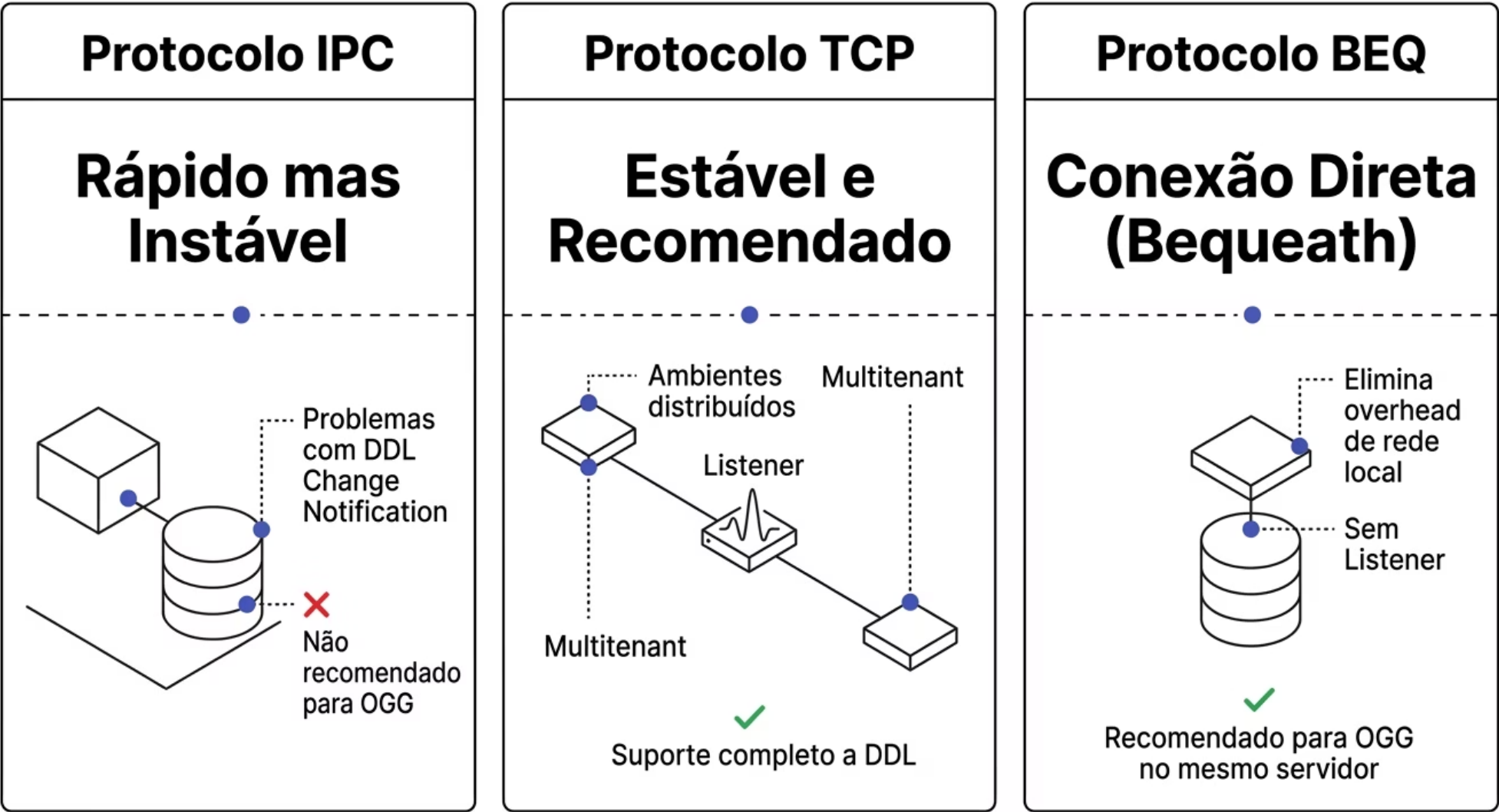
⚠ **Aviso Crítico de Produção (Padrão Sênior):** Evite o protocolo IPC com o Oracle GoldenGate! O uso do IPC apresenta problemas intermitentes graves relacionados à notificação de alterações de DDL do dicionário de dados (DDL Change Notification). Se você utilizar IPC, o seu Extract integrado pode falhar ou ignorar comandos estruturais aleatoriamente.

A Tentação do IPC

Quando o Oracle GoldenGate está instalado no mesmo servidor físico ou VM onde reside o banco de dados Oracle, muitos DBAs caem na tentação de utilizar o protocolo **IPC (Inter-Process Communication)** na string de conexão, acreditando que ele será mais rápido por mapear diretamente a memória local.

A Recomendação Oracle

Para garantir estabilidade máxima e o funcionamento correto das notificações de DDL, a própria Oracle recomenda enfaticamente o uso exclusivo dos protocolos **TCP** ou **Bequeath (BEQ)**. Estes protocolos garantem que o Extract integrado receba corretamente todos os eventos estruturais do banco de dados.



Protocolo Bequeath (BEQ): Conexão Direta Sem Listener

Conceito Essencial

O protocolo **Bequeath (BEQ)** é uma joia oculta do Oracle SQL*Net. Ele permite que uma aplicação local — no nosso caso, o Extract ou Replicat — se conecte diretamente a uma instância de banco de dados **sem passar pelo Listener da rede**.

Como funciona o BEQ?

1

Spawn Direto pelo SO

O processo OGG cria um processo sombra (*spawn*) do Oracle diretamente pelo binário do sistema operacional.

2

Elimina Overhead de Rede

Por não passar pelo Listener, elimina completamente o overhead de rede local entre o OGG e o banco de dados.

3

Resiliência ao Listener

Contorna quedas acidentais do Listener, garantindo que o Extract continue operando mesmo em falhas de rede.

Lab Prático: Configurando o Bequeath no tnsnames.ora

Para que o OGG use o Bequeath, precisamos criar um descritor de conexão específico no arquivo `tnsnames.ora` localizado no diretório apontado pela variável `$TNS_ADMIN`. Abra o `tnsnames.ora` e adicione a entrada local:

```
dbbeq =
(DESCRIPTION=
  (ADDRESS=
    (PROTOCOL=beq)
    (ENVS='ORACLE_SID=sales,ORACLE_HOME=/app/db_home/oracle,LD_LIBRARY_PATH=/app/db_home/oracle/lib')
    (PROGRAM=/app/db_home/oracle/bin/oracle)
    (ARGV0=oraclesales)
    (ARGS='(DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq))))')
  (CONNECT_DATA=
    (SID=sales)))
```

  **Atenção milimétrica:** Não pode haver nenhum espaço em branco (*white space*) entre as definições de variáveis dentro das aspas do parâmetro `ENVS`. Caso contrário, a conexão falhará com erro de sintaxe do SQL*Net.



Análise do Script pelo Instrutor

Vamos dissecar cada componente crítico da entrada BEQ no `tnsnames.ora` para garantir o entendimento completo:

`/app/db_home/oracle`

Representa o diretório home real do banco de dados de destino/origem (`$ORACLE_HOME`). Este caminho deve apontar exatamente para onde o Oracle Database está instalado no servidor.

`sales` — O SID da Instância

É o `ORACLE_SID` da instância local. Tanto o parâmetro `ARGV0=oraclesales` quanto o `ORACLE_SID=sales` dentro do `ENVS` devem referenciar o mesmo SID.

Parâmetro `ENVS`

Passa as variáveis de ambiente necessárias para o binário do banco rodar em background: `ORACLE_SID`, `ORACLE_HOME` e `LD_LIBRARY_PATH`. Estas variáveis são essenciais para que o processo sombra seja inicializado corretamente.

⚠ Regra do Sem Espaços no `ENVS`

Não pode haver nenhum espaço em branco entre as definições de variáveis dentro das aspas do parâmetro `ENVS` (`ORACLE_SID=sales,ORACLE_HOME=...`). Qualquer espaço causará falha de sintaxe do SQL*Net e a conexão não será estabelecida.

Protocolo TCP: O Padrão para Ambientes Híbridos e Multitenant

Quando o seu ambiente OGG está consolidado em um servidor centralizado apartado — ou os bancos de dados estão distribuídos — o protocolo **TCP** associado ao Listener tradicional é a escolha definitiva.

Ambientes Distribuídos

Ideal quando o servidor OGG está separado fisicamente dos bancos de dados de origem e destino, comunicando-se via rede TCP/IP padrão.

Arquitetura Multitenant

Em cenários modernos de bancos Multitenant, precisamos mapear de forma organizada as conexões para o **CDB\$ROOT** e para cada **PDB** de negócio.

Níveis de Conexão OGG

O Extract e o Replicat logarão em **níveis diferentes** da arquitetura Multitenant — o Extract a nível de PDB e o monitoramento global a nível de CDB.

Lab Prático: Mapeamento de TNS Multitenant para o OGG

Abaixo está o modelo ideal de um arquivo `tnsnames.ora` configurado no host de origem **DBEAST**, preparado para atender os processos do GoldenGate com Extract a nível de PDB e replicação paralela:

```
#####
## Amostra de tnsnames.ora para o Host: DBEAST
#####

# Conexão com o Container Raiz
# (Utilizado para monitoramento global ou Extracts Root-Level)
cdb23_root =
  (DESCRIPTION=
    (ADDRESS=(PROTOCOL=TCP)(HOST=DBEAST)(PORT=1521))
    (CONNECT_DATA=(SERVICE_NAME=rdbms.oracle.com)))

# Conexão com o PDB Padrão 0 (Root Template)
cdb23_pdb0 =
  (DESCRIPTION=
    (ADDRESS=(PROTOCOL=TCP)(HOST=DBEAST)(PORT=1521))
    (CONNECT_DATA=(SERVICE_NAME=cdb1_pdb0.rdbms.oracle.com)))

# Conexão com o PDB de Origem "East"
# (Onde o nosso per-PDB Extract se conectará)
cdb23_pdbeast =
  (DESCRIPTION=
    (ADDRESS=(PROTOCOL=TCP)(HOST=DBEAST)(PORT=1521))
    (CONNECT_DATA=(SERVICE_NAME=cdb1_pdbeast.rdbms.oracle.com)))

# Conexão com o PDB de Destino "West"
# (Onde o Replicat aplicará as transações)
cdb23_pdbwest =
  (DESCRIPTION=
    (ADDRESS=(PROTOCOL=TCP)(HOST=DBEAST)(PORT=1521))
    (CONNECT_DATA=(SERVICE_NAME=cdb1_pdbwest.rdbms.oracle.com)))
```



cdb23_root

Conexão com o **CDB\$ROOT** — usado para monitoramento global ou Extracts em nível de container raiz.



cdb23_pdbeast

PDB de **origem** — onde o processo Extract per-PDB se conectará para capturar as transações.



cdb23_pdb0

Conexão com o **PDB\$SEED** ou PDB padrão 0 — template raiz da arquitetura Multitenant.



cdb23_pdbwest

PDB de **destino** — onde o processo Replicat aplicará as transações replicadas.

Console Web: Passo a Passo do Cadastro de Credenciais

Mão na Massa — O fluxo padrão de mercado para cadastrar uma nova conexão de banco de dados:

01

Acesse a Console Web

Abra o Administration Service e faça login com o usuário administrador do deployment.

02

Navegue até DB Connections

No menu de navegação do lado esquerdo, clique na opção **DB Connections**.

03

Adicione Nova Conexão

No painel central, clique no botão de adição **(+)** ao lado do título DB Connections.

04

Preencha as Credenciais

A caixa de diálogo **Credentials** será exibida com todos os campos de configuração.

Campos de Configuração e Jargões Técnicos

Campo	Descrição	Exemplo / Observação
Credential Domain	Agrupamento lógico do cofre de credenciais. Padrão: OracleGoldenGate	PROD_DOMAIN, TEST_DOMAIN
Credential Alias	Codiname amigável usado nos arquivos de parâmetros .prm	ggeast, ggwest
Connection Type	DSN (alias do tnsnames.ora / ODBC) ou Database Server and Port (Hostname/IP + Porta)	DSN para Oracle; Server+Port para heterogêneos
User ID	Schema administrador criado nas aulas anteriores	ggadmin ou c##ggadmin
Password	Senha real do usuário — criptografada e guardada no wallet	Confirmada no campo Verify Password

⊗ **⚠ Alerta de Produção — A Pegadinha do Traço/Hífen:** O nome do usuário do banco de dados **nunca deve conter um hífen ou traço** (Ex: OGG-ADMIN). Se o time de segurança criar o usuário com esse caractere, o processo Extract falhará categoricamente na inicialização ou no registro, gerando o erro:

ERROR OGG-08221 Cannot register or unregister EXTRACT extract_name because of the following SQL error: OCI Error ORA (status = 44004-ORA-44004: invalid qualified SQL name).

Correção: O nome deve conter apenas letras, números ou underscore. Ex: ogg_admin

Ações Administrativas Pós-Conexão

O Ciclo de Vida da Conexão

Uma vez preenchidos os dados e clicado em **Submit**, o alias aparecerá na listagem. Clique no ícone de **Connect database** (formato de tomada) para validar. Se as credenciais, portas e privilégios estiverem 100% corretos, o ícone cinza ficará **azul instantaneamente**.



Connect / Disconnect

Ativar ou desativar a sessão de banco de dados diretamente pela interface, sem linha de comando.



Copy DB Connection

Clonar os dados de conexão para criar um alias semelhante — útil para conexões em PDBs irmãos.



Alter / Delete

Modificar senhas expiradas ou remover conexões antigas sem intervenção manual no sistema.

Habilitação de Infraestrutura Automática

Com a tomada azul, a interface abre seções dedicadas na parte inferior da página. Com apenas um clique, o DBA pode criar e injetar no banco:



Tabelas de Checkpoint

Cruciais para o Replicat marcar a última transação aplicada com precisão.



Tabelas de Heartbeat

Mecanismo automático que calcula a latência fim-a-fim da replicação minuto a minuto.



TRANDATA / SCHEMATRANDATA

Ative o Supplemental Logging do schema de negócio diretamente por botões nesta tela — sem GGSCI!



✓ Resumo do Ciclo Completo: Cadastrar credenciais → Validar conexão (tomada azul) → Habilitar Checkpoint, Heartbeat e TRANDATA — tudo pela interface web do Administration Service, sem digitar uma única linha de código.

Inserindo o Alias no Processo (.PRM)

Uma vez mapeado o TNS e registrado o alias no Credential Store do OGG, a chamada dentro do arquivo do processo fica extremamente resumida e segura. Todo o mapeamento de rede e credenciais fica encapsulado no cofre.

Arquivo EX_HR.prm (Extract)

```
EXTRACT EX_HR  
USERIDALIAS ggeast
```

```
-- O OGG usará a credencial do cofre  
-- que aponta para o alias de rede  
-- cdb23_pdbeast
```

 O parâmetro `USERIDALIAS ggeast` instrui o OGG a buscar no Credential Store o alias `ggeast`, que internamente aponta para o usuário, senha e connection string do PDB de origem.

Fluxo Completo de Segurança

01

tnsnames.ora

Define o alias de rede `cdb23_pdbeast` apontando para o PDB correto via TCP.

02

Credential Store

Armazena usuário, senha e connection string sob o codinome `ggeast`.

03

Arquivo .PRM

Referencia apenas `USERIDALIAS ggeast` — sem nenhuma senha exposta.

04

Conexão Segura

O OGG resolve o alias, busca as credenciais no cofre e estabelece a conexão de forma transparente.

Conexões Heterogêneas e Protocolos de Segurança

O Oracle GoldenGate 23ai/26ai é uma ferramenta fantástica para cenários híbridos (Multi-Cloud e bancos heterogêneos como **SQL Server, MySQL e PostgreSQL**). A segurança da informação exige protocolos de criptografia configurados no campo **Security Protocol**:

1	 Plaintext (Texto Puro) Padrão ao conectar via Database Server and Port. Dados trafegam sem criptografia TLS adicional. Usado apenas em redes locais ou ambientes isolados de laboratório.
2	 TLS (Transport Layer Security) Criptografa o canal de comunicação. No SQL Server, a opção Trust Server Certificate é marcada por padrão. Se desmarcada, o DBA deve apontar os caminhos físicos do certificado (SSL Path e SSL Certificate).
3	 mTLS (Mutual TLS — Zero Trust) Nível máximo de segurança em redes corporativas. Tanto o servidor de banco quanto o cliente (OGG) validam seus certificados digitais mutuamente. Comum para MySQL e PostgreSQL.

Modos de Validação mTLS

PREFERRED / REQUIRE Exige criptografia, mas pode tolerar algumas validações. Permite atributos adicionais na caixa Additional Attributes .	VERIFY_CA / VERIFY_IDENTITY Modos estritos. Exigem preenchimento obrigatório dos caminhos de certificados no servidor Linux.	 Campos Obrigatórios no mTLS Estrito • SSL Path: Diretório com certificados das CAs confiáveis • SSL CA: Arquivo do certificado da CA em formato <code>.pem</code> • SSL Certificate: Certificado de chave pública do cliente OGG • SSL Key: Chave privada <code>.key</code> para validação de identidade • SSL CRL: Lista de revogação de certificados banidos
---	--	--