SAVANT
Tecnologia

Serviço de Diretórios com OpenLDAP

Marcos Sungaila

marcos@savant.com.br

- Por que LDAP
- Conceitos básicos
- Instalando e Configurando o OpenLDAP
- Criando a estrutura do Diretório
- Trabalhando com senhas de usuários
- Consultando os dados
- Alterando e removendo entradas
- Performance tunning
- Controle de acesso
- Criptografia
- Ferramentas de gerenciamento

Por que LDAP?

SAVANT Tecnologia

- Complexidade em gerenciar ambientes com vários mecanismos de login, por exemplo: estações Windows, internet via proxy, …
- Complexidade em manter informações sincronizadas
- Evitar a redundância de informações
  - Cadastrar o usuário em vários serviços e servidores
- Compartilhamento de informações de forma eficiente

Conceitos básicos

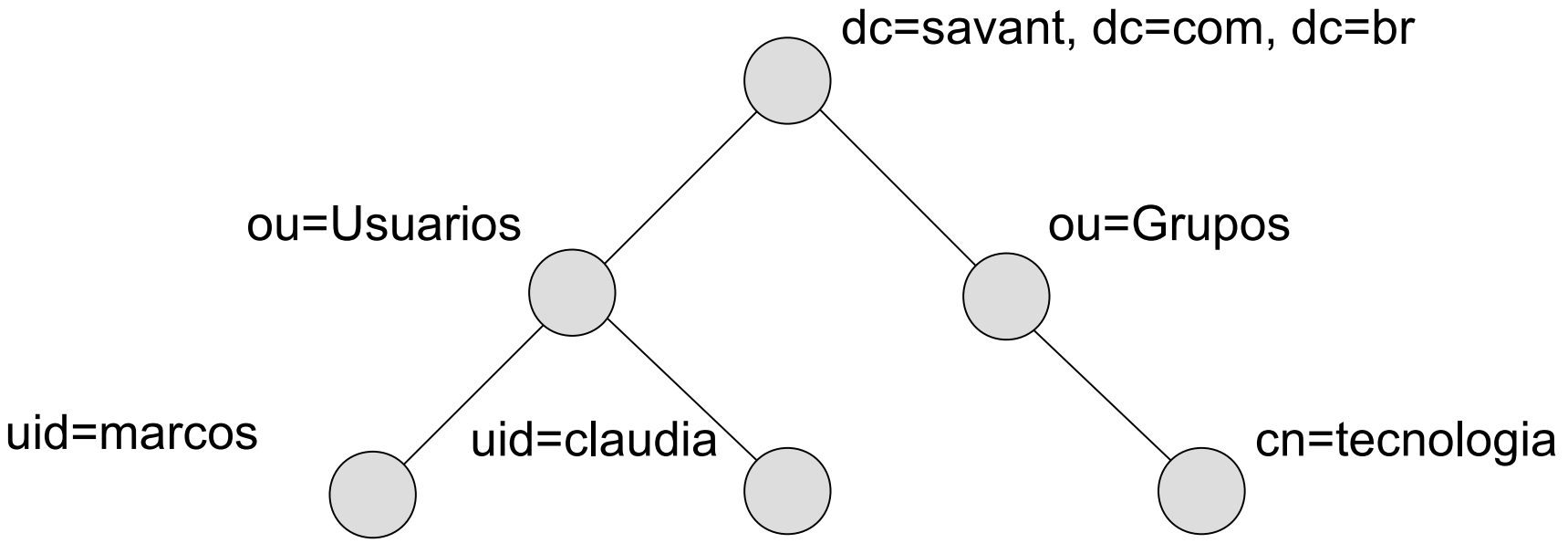
SAVANT Tecnologia

- LDAP (Lightweight Directory Access Protocol)
- Protocolo para acesso a informações via rede
- Baseado no padrão X.500
- Padrão definido nas RFC's 1777 e 2251
- Armazena informações baseadas em atributos
- Implementa modelo de objetos hierárquico e extensível
- Pode utilizar diferentes backends para armazenamento dos dados
- Desenhado para alta performance em consultas
- Baixa performance em operações de escrita

Modelos de Diretórios

SAVANT Tecnologia

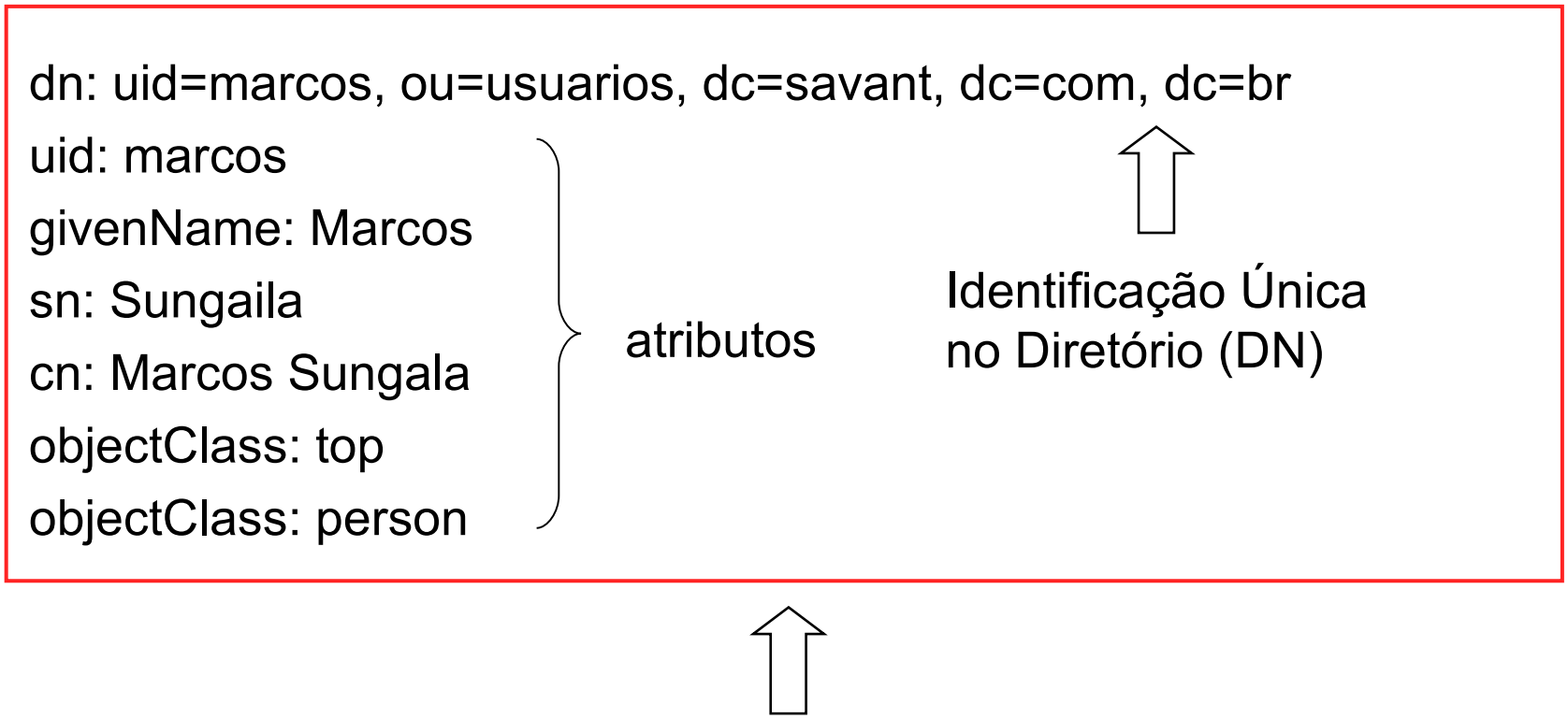
- Estrutura simples do tipo domínio Internet (domainComponent):



Modelos de Diretórios

SAVANT Tecnologia

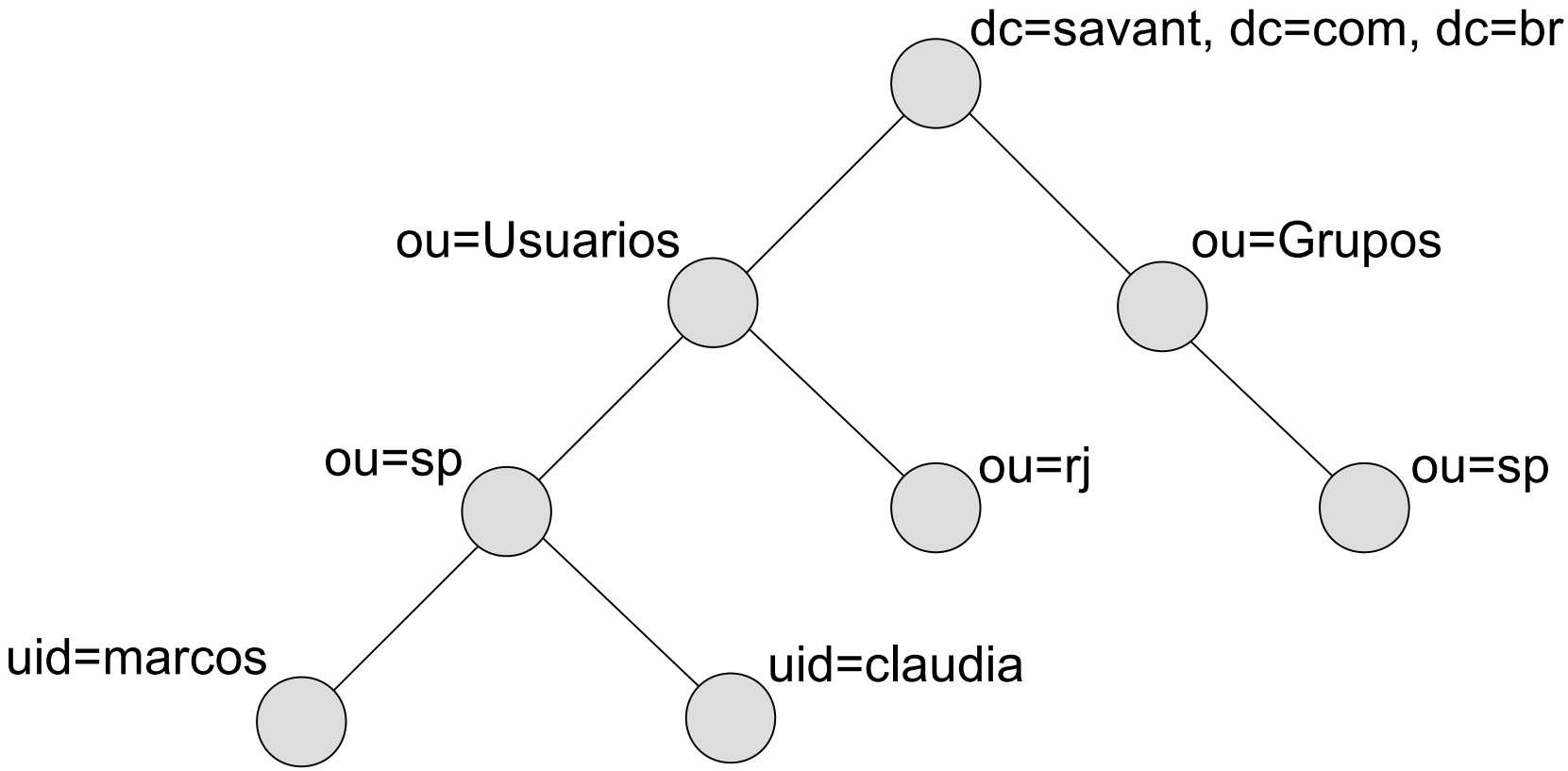
- Dados de um usuário:



Modelos de Diretórios

SAVANT Tecnologia

- Uma variação do modelo elaborado com domainComponent:



Modelos de Diretórios

SAVANT Tecnologia

- distinguishedName (identificação única):

```
uid=marcos,ou=usuarios,dc=savant,dc=com,dc=br

uid=marcos,ou=sp,ou=usuarios,dc=savant,dc=com,dc=br
```

- Facilita a identificação do usuário e sua localização geográfica na empresa – é um modelo lógico que pode facilitar a administração

Principais Componentes

SAVANT Tecnologia

- Antes de cadastrar dados em um serviço de Diretórios é necessário identificar para que estes dados serão utilizados.
- De acordo com o uso escolhemos quais objectClasses devem ser atribuídas à entrada
- objectClasses mais comuns e seus usos:
  - person: identificação de pessoas com dados básicos como nome, telefone, descrição e senha
  - organizationalPerson: acrescenta novos dados como endereço, cep, caixa postal, unidade, cidade, estado e outros
  - inetOrgPerson: endereço pessoal, mail, celular, foto, certificados digitais, idioma
  - posixAccount: conta de usuário linux
  - sambaSamAccount: conta de usuário samba

Principais Componentes

SAVANT Tecnologia

- Uma entrada (o cadastro de um usuário por exemplo) pode ter vários atributos do tipo objectClass.

dn: uid=marcos, ou=usuarios, dc=savant, dc=com, dc=br
uid: marcos
givenName: Marcos
sn: Sungaila
cn: Marcos Sungala
objectClass: top
objectClass: person

Instalação

SAVANT Tecnologia

- Instalando os pré-requisitos (pág 5)
  - OpenSSL: biblioteca básica de suporte a criptografia

    ```
    apt-get install openssl
    ```

  - Berkeley DB: backend para armazenamento dos dados

    ```
    apt-get install db4.2-util
    ```

  - Cyrus-SASL: suporte a autenticação e comunicação criptografada

    ```
    apt-get install sasl2-bin libsasl2 \
    libsasl2-modules libsasl2-modules-ldap
    ```

Instalação

- Instalando **OpenLDAP** (pág 5)
  - Servidor e ferramentas de gerenciamento

```
apt-get install slapd ldap-utils
```

- No Debian o instalador irá perguntar a senha de administração do LDAP. Responda com:

  tux

Configuração

SAVANT Tecnologia

- Toda a configuração do servidor **OpenLDAP** é realizada no arquivo `/etc/ldap/slapd.conf`.
  - Vamos começar uma configuração a partir do zero para entender todo o funcionamento do servidor.
  - Renomeando o arquivo original:

```
cd /etc/ldap
mv slapd.conf slapd.conf.old
```

  - Iniciando uma nova configuração (vi ou mcedit):

```
vi slapd.conf

ou

mcedit slapd.conf
```

Configuração

SAVANT Tecnologia

- Diretivas do arquivo `slapd.conf (pág 6)`:

```
# Versão de protocolo para consultas LDAP
allow bind_v2

# Schemas – dados suportados pelo servidor
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
```

Configuração

SAVANT Tecnologia

- Diretivas do arquivo `slapd.conf` (cont):

```
# Controle de processos e argumentos
pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd/slapd.args

# Módulos – localização e ativação
modulepath      /usr/lib/ldap
moduleload      back_hdb

# Nível de log padrão
loglevel        stas
```

Configuração

SAVANT Tecnologia

- Diretivas do arquivo `slapd.conf` (cont):

```
# Base de dados
database hdb

# Estrutura do diretório e administrador
suffix   “dc=empresa,dc=com,dc=br”
rootdn   “cn=Manager,dc=empresa,dc=com,dc=br”
rootpw   tux
```

Configuração

SAVANT Tecnologia

- Diretivas do arquivo `slapd.conf` (cont):

```
# Local de armazenamento dos dados
directory /var/lib/ldap

# Índices de pesquisa
index objectClass eq
```

Configuração

SAVANT Tecnologia

- Definindo a senha do usuário root:
  - Armazenada na configuração do servidor ou na base LDAP
  - Texto puro ou Criptografada com comando `slappasswd`:

```
slappasswd
New password: tux
Re-enter new password: tux
{SSHA}hLLfSLt73/YwNYEJU/T7PAcLd0AOBOje
```

  - Copie a senha com o mouse e cole no arquivo de configuração `slapd.conf`.

Iniciando o LDAP

SAVANT Tecnologia

- Para ter certeza que seu arquivo slapd.conf está correto, faça o seguinte teste:

```
slaptest
```

- Antes de iniciar o serviço LDAP com nossas novas configurações devemos parar o servidor slapd e remover os dados antigos gerados automaticamente pela instalação do pacote slapd:

```
/etc/init.d/slapd stop
cd /var/lib/ldap
rm *
/etc/init.d/slapd start
```

Verificando as conexões

SAVANT Tecnologia

- Você pode verificar se a porta tcp/389 foi habilitada:

```
netstat -lntp | grep 389
```

- Você também pode verificar se o servidor slapd está em execução

```
ps ax | grep slapd
```

Cadastrando dados

SAVANT Tecnologia

- Não há um browser de dados para ver as informações do Diretório.
- Cadastramento em modo batch.
  - Criamos um arquivo com os dados a serem importados no Diretório
  - Inserimos as informações no Diretório de uma única vez com o comando ldapadd
- Definindo a estrutura inicial do Diretório:

```
dn: dc=empresa,dc=com,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: Empresa Ltda
dc: empresa
```

Cadastrando dados

SAVANT Tecnologia

- Com o arquivo ldif pronto, basta inserir os dados na base do Diretório:

```
ldapadd -x -D cn=manager,dc=empresa,dc=com,dc=br -W \
    -f empresa.ldif
```

- Você deve criar, ao menos, a estrutura básica do Diretório por meio dos arquivos ldif.
- Tendo criado os arquivos com a estrutura inicial (dc e ou), os outros dados (usuários, grupos, etc) podem ser inseridos no Diretório utilizando ferramentas como luma, phpLDAPadmin, phpQLadmin, ldap-admin, ldap-account-manager, etc.

Cadastrando dados

SAVANT Tecnologia

- Laboratórios 1 e 2

SAVANT

Tecnologia

Marcos Sungaila
marcos@savant.com.br
(11) 5071-3112