

## 6.17 Instalação o LDAP Account Manager

O LDAP Account Manager (LAM) é um front-end Web para o gerenciamento de entradas (por exemplo: usuários, grupos e máquinas) armazenadas em um diretório LDAP. O LAM foi projetado para tornar o gerenciamento do LDAP o mais fácil possível para o usuário. Ele abstrai os detalhes técnicos do LDAP e permite, de forma mais fácil, o gerenciamento de entradas no serviço de diretórios. Se necessário, o software permite também a edição mais técnica de dados, através do navegador LDAP integrado.

Neste laboratório será instalado e configurado o LAM, para gerenciar o serviço de diretórios do Samba4 (OpenLDAP).

Para implementação do serviço, será necessário primeiramente realizar a instalação das dependências para o correto funcionamento do software.

```
root@samba4:/# apt install apache2 libapache2-mod-php7.3 javascript-common
```

Realizada a instalação das dependências, baixe a última versão do Ldap Account Manager a partir do site oficial:

```
# wget http://prdownloads.sourceforge.net/lam/ldap-account-manager_7.4-1_all.deb
```

E instale o pacote com o utilitário **dpkg**:

```
root@samba4:/# dpkg -i ldap-account-manager_7.4-1_all.deb
```

Se você receber alguma mensagem sobre dependências ausentes, execute o comando "apt" com a opção "-f" para forçar a instalação das dependências:

```
root@samba4:/# apt -f install
```

E execute novamente a instalação via **dpkg**:

```
root@samba4:/# dpkg -i ldap-account-manager_7.4-1_all.deb
```

Acesse através do navegador do cliente Windows o endereço <http://172.16.1.5/lam>:

**LAM Login**

User name

Password

Language

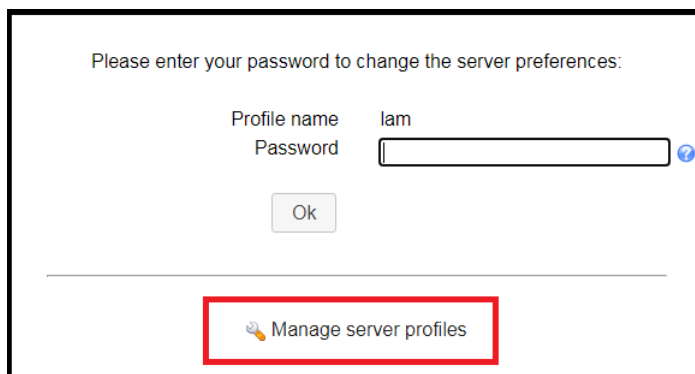
---

LDAP server

Server profile

### 6.17.1 Criando um perfil para acesso ao AD do Samba4

Instalado o LAM, agora será necessário criar um perfil para acesso ao OpenLDAP do Samba4, para isso, clique em "**LAM Configuration**" (canto superior direito), posteriormente em "**Edit server profiles**" e por fim em "**Manage server profiles**":



Please enter your password to change the server preferences:

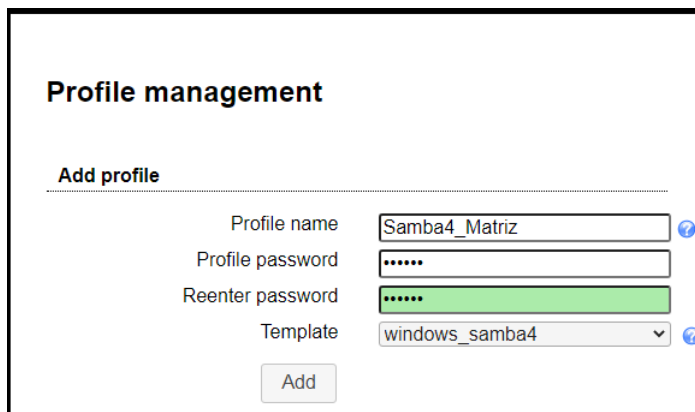
Profile name: lam

Password:

Ok

**Manage server profiles**

Na tela "**profile Management**", preencha os campos: Profile name, Profile password (defina uma senha para o perfil) e Template (deverá ser selecionado o Template **windows\_samba4**).



**Profile management**

**Add profile**

Profile name: Samba4\_Matriz

Profile password:

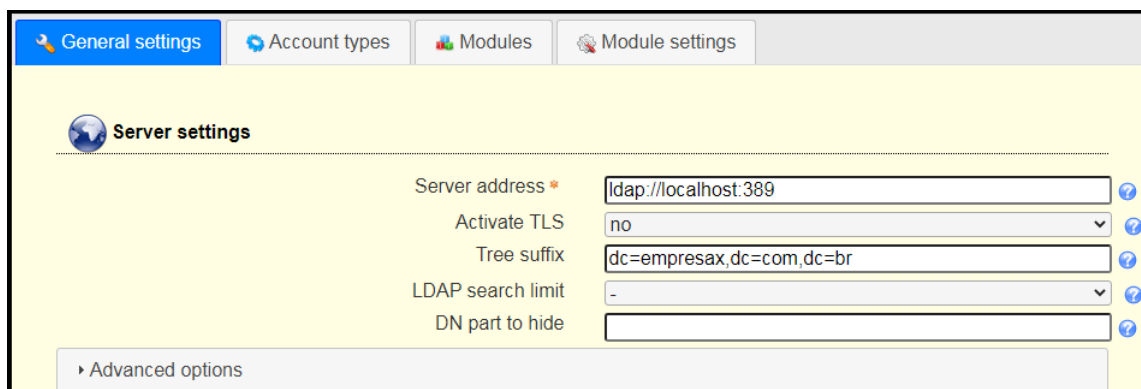
Reenter password:

Template: windows\_samba4

Add

Após preencher os campos, ao clicar em "Add" será solicitada a senha Master default do LAM, a senha padrão é **lam**. Vale ressaltar, que em um ambiente de produção, é importante alterar a senha default de administrador.

Criado o perfil, agora é necessário configurar a conexão do LAM com o OpenLDAP. Inicialmente serão inseridas as configurações gerais, preenchendo os campos: Server address (endereço do servidor samba4) e Tree suffix (sufixo utilizado na estrutura de AD):



**General settings** | **Account types** | **Modules** | **Module settings**

**Server settings**

Server address: ldap://localhost:389

Activate TLS: no

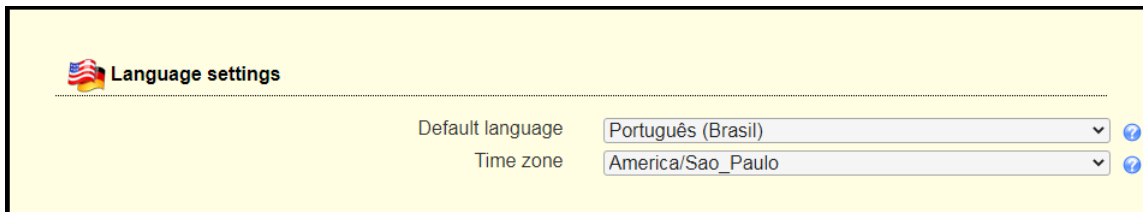
Tree suffix: dc=empresax,dc=com,dc=br

LDAP search limit: -

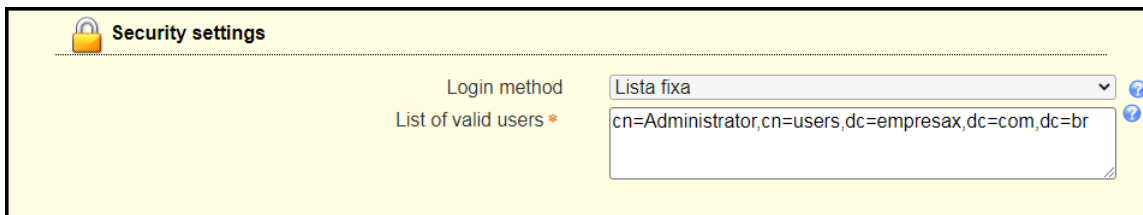
DN part to hide:

Advanced options

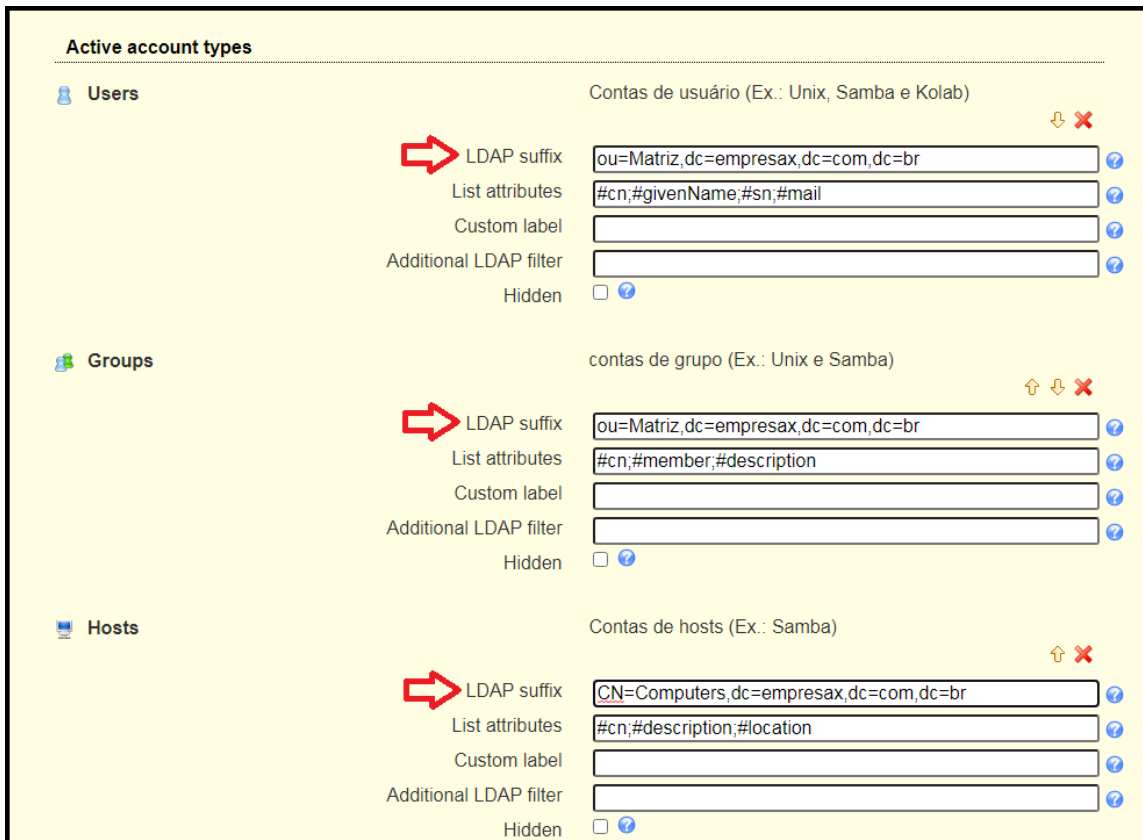
Um pouco mais abaixo, configure o idioma padrão do LDAP Account Manager para Português (Brasil) e o Time Zone para América/Saopaulo :



Ainda em "General settings", configure as credenciais de acesso ao OpenLDAP do Samba4 configurando o "List of valid users" e definindo a senha de acesso ao perfil. A conexão ao LDAP será realizada pelo usuário Administrator do Samba4, atenção para o ajuste do sufixo (cn=users,dc=empresax,dc=com,dc=br):

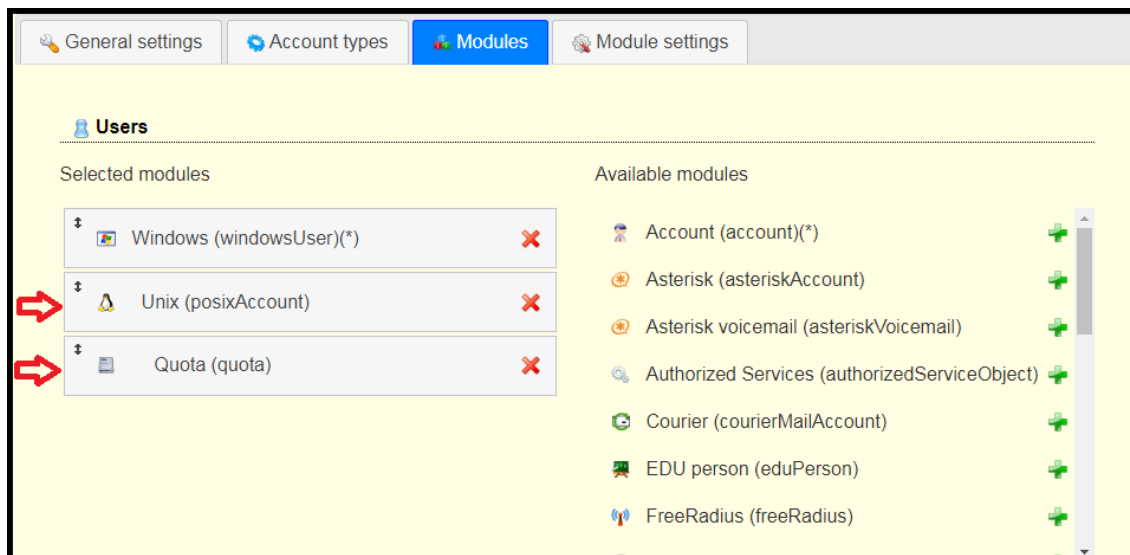


Agora, volte ao topo do formulário e acesse na aba "Account types", configure os acessos aos usuários, grupos e máquinas da Unidade Organizacional Matriz, ajustando os campos "LDAP suffix" de cada um dos objetos:

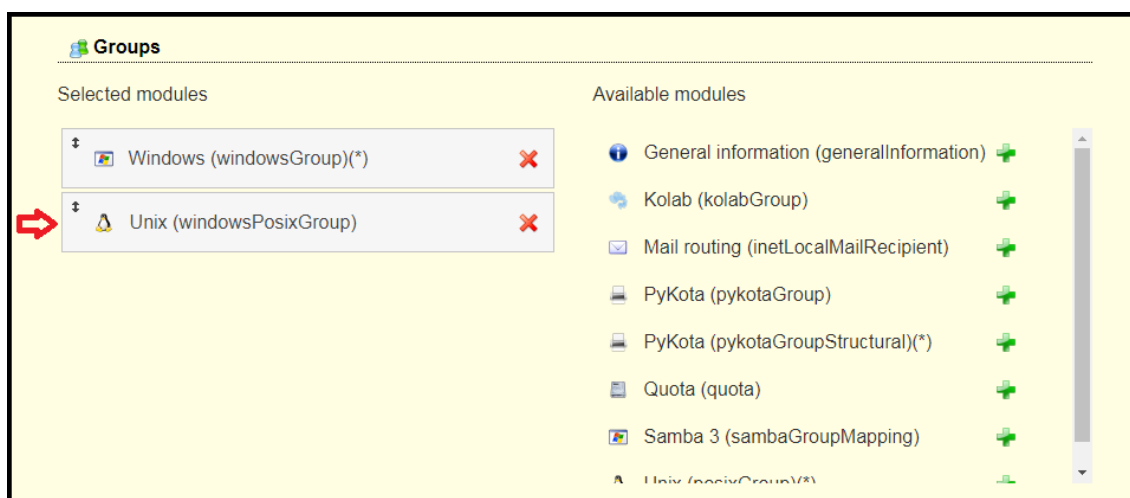


Agora será necessário ativar os módulos que serão utilizados para administração do AD (Aba Modules). Os módulos quando ativados, permitem uma experiência mais amigável com o gerenciamento do AD, pois acrescenta campos para que vários tipos de atributos possam ser adicionados por meio da interface do LAM. É possível ativar módulos para usuários, grupos e hosts.

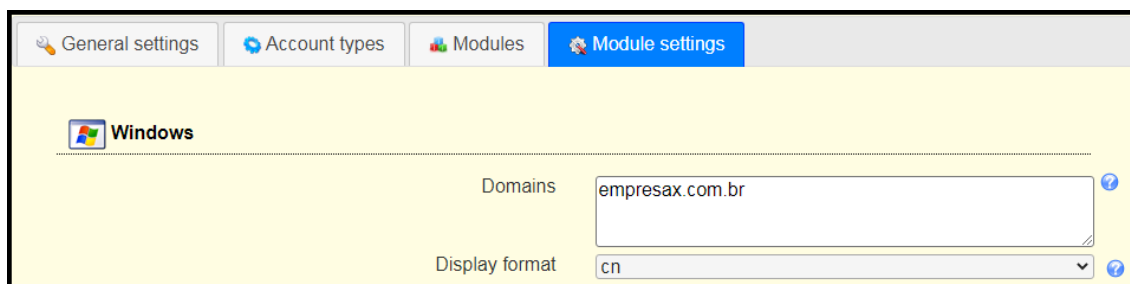
Para os usuários, serão adicionados os módulos Quota (quota) e Unix (posixAccount), esses módulo se referem respectivamente ao gerenciamento de cotas de usuários e as contas de usuário para o linux. Para adicioná-los clique no ícone + ao lado do módulo:



Nos módulos de Grupos, adicione o módulo "Unix (windowPosixGroup)":



Por fim, na aba "**Modules Settings**", adicione o domínio "empresax.com.br" como segue:



Após o término das configurações, clique no botão **Save**, disponível na parte inferior da página.

### 6.17.2 Ajuste do Samba4 para acesso ao LAM

Possivelmente na primeira tentativa de acesso ao OpenLDAP via LAM, o seguinte erro ocorrerá LDAP\_STRONG\_AUTH\_REQUIRED. Este erro ocorre devido o servidor LDAP ainda não possuir uma opção para impor uma autenticação forte.



The screenshot shows the LAM Login web interface. On the left, the text "LAM Login" is written vertically in blue. The main form has fields for "Nome do usuário" (set to "Administrator"), "Senha", and "Idioma" (set to "Português (Brasil)"). Below these is an "Início de sessão" button. A red error box in the center contains the text: "Não foi possível conectar-se ao servidor LDAP especificado. Por favor tente novamente. (8) Erro LDAP , servidor reportou: Strong(er) authentication required - BindSimple: Transport encryption required." At the bottom, there are fields for "servidor LDAP" (set to "ldap://localhost:389") and "Perfil de servidor" (set to "Samba4\_Matriz").

Como o comportamento padrão anterior era "não", para solucionar este problema pode ser necessário que você altere explicitamente a opção "*ldap server require strong auth*" no arquivo `smb.conf`, até que todos os clientes tenham sido ajustados. Clientes Windows e servidores membros do Samba já usam proteção de integridade.

Para isso edite o arquivo `smb.conf`:

```
root@samba4:/# vim /usr/local/samba/etc/smb.conf
```

E insira a seguinte linha na seção global do arquivo:

```
ldap server require strong auth = no
```

```
# Global parameters
[global]
bind interfaces only = Yes
dns forwarder = 8.8.8.8
interfaces = lo enp0s3
netbios name = SAMBA4
realm = EMPRESAX.COM.BR
server role = active directory domain controller
workgroup = EMPRESAX
idmap_ldb:use rfc2307 = yes
allow dns updates = nonsecure and secure
ldap server require strong auth = no
```

Por fim, reinicie o serviço Samba4:

```
root@samba4:/# systemctl restart samba4
```

### 6.17.3 Teste de autenticação no LAM e ajustes iniciais

Para testar a autenticação é necessário selecionar o perfil criado anteriormente no LAN no campo "Perfil de servidor" (Samba4\_Matriz). No campo "Nome do usuário" utilize o usuário administrador do domínio (Administrator) e a senha (Pa\$\$w0rd). Por fim, verifique o funcionamento da autenticação clicando em "Início de sessão".

**LAM Login**

Nome do usuário: **Administrator**

Senha:

Idioma: **Português (Brasil)**

---

servidor LDAP: **ldap://localhost:389**

Perfil de servidor: **Samba4\_Matriz** **1º**

Observe, que como criamos um perfil para a Unidade Organizacional Matriz, apenas os usuários e unidades pertencentes a Matriz serão listados no LAM. No menu superior direito é possível listar as unidades TI e Vendas:

**Usuários** | Grupos | Hosts

Conta de usuário: 2

Ações	Nome comum	Primeiro nome	Último nome	Correio Eletrônico
Ordenar sequência				
<input type="checkbox"/> Filtro	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Joao Silva	Joao	Silva	
<input type="checkbox"/>	Maria Braga	Maria	Braga	

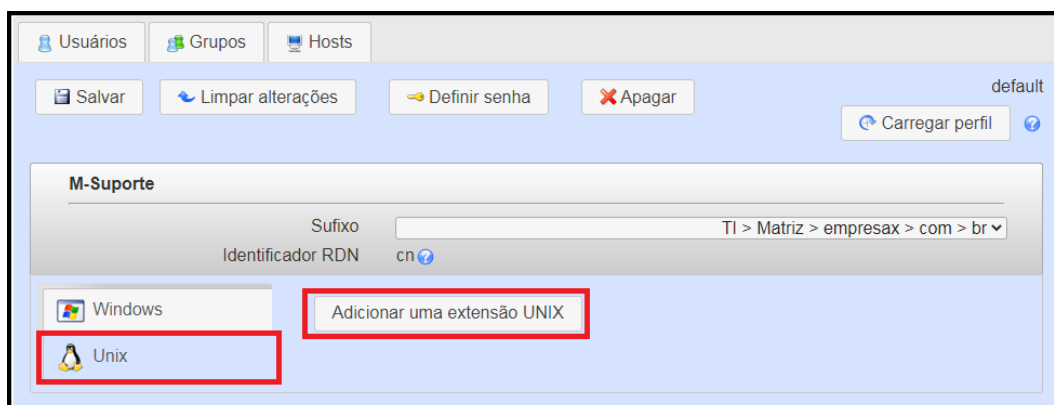
No primeiro acesso, para que seja possível administrar de forma efetiva os grupos criados no AD, é importante adicionar a extensão UNIX para cada um deles. Para isso, clique na aba "Grupos" edite os grupos "M-Suporte" e "M-Vendedores" (um de cada vez, clicando no ícone lápis)

**Usuários** | **Grupos** | Hosts

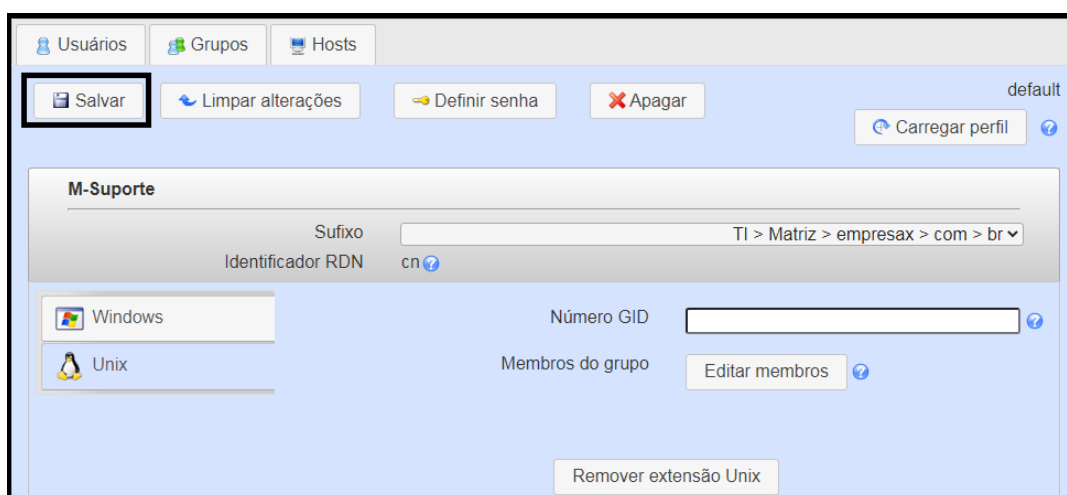
Contagem de grupos: 2

Ações	Nome do grupo	DN's membros do grupo	Descrição do grupo
Ordenar sequência			
<input type="checkbox"/> Filtro	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	M-Suporte	Joao Silva > TI > Matriz > empresax > com > br	
<input type="checkbox"/>	M-Vendedores	Maria Braga > Vendas > Matriz > empresax > com > br	

No menu lateral clique na opção Unix e posteriormente no botão "Adicionar uma extensão UNIX":



Após Adicionar a extensão, clique em salvar.



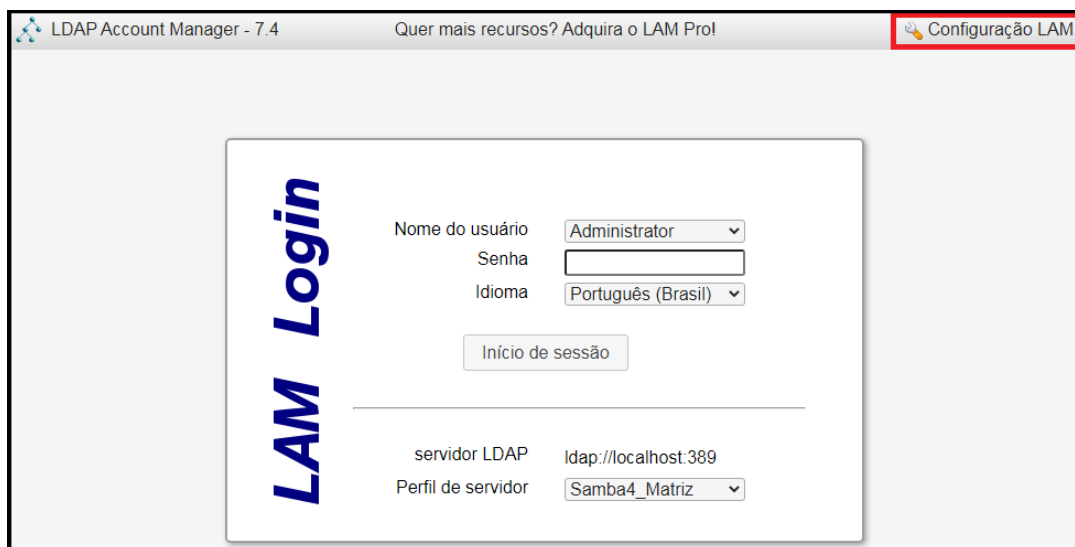
Criado o perfil para a Unidade Organizacional Matriz, repita os passos a partir do tópico "6.17.1" e crie um perfil para Unidade Organizacional Filial.

#### 6.17.4 Configuração de acesso para os usuários controladores das Unidades Organizacional

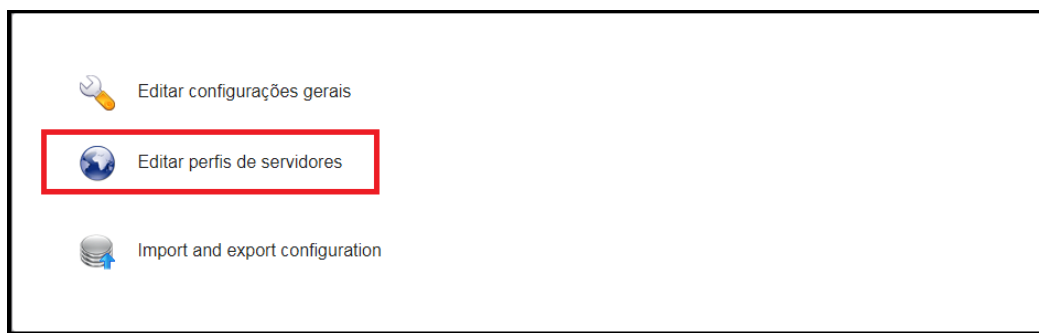
No laboratório anterior, foi delegado o controle da Unidade Organizacional Matriz para o grupo M-Suporte e da Unidade Organizacional Filial para o grupo F-Suporte. Nesta atividade, será autorizado o acesso como administrador do Active Directory do Samba4 via LAM para os usuários pertencentes a estes grupos em cada um dos perfis criados.

- **Usuário:** joaosilva / **Perfil:** Matriz
- **Usuário:** marcovaz / **Perfil:** Filial

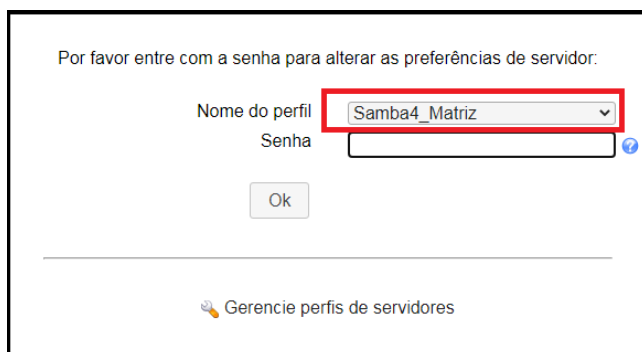
Iniciaremos pelo "perfil Matriz". Para começar a configuração, clique em "LAN Configuration" no canto superior direito:



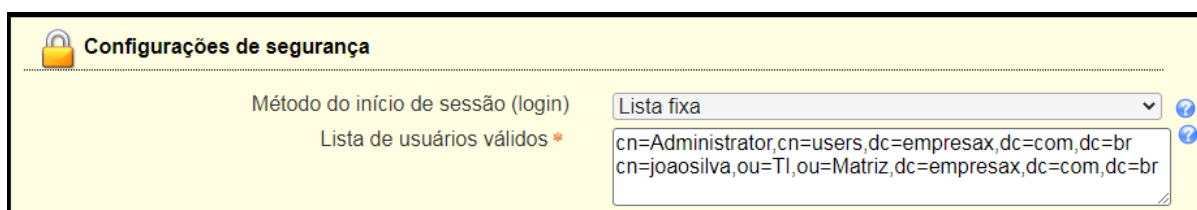
Escolha a opção "Editar perfis de servidores:



Selecione o perfil Samba4\_Matriz, criado na tarefa anterior; E, digite a senha de acesso ao perfil Samba4\_Matriz.

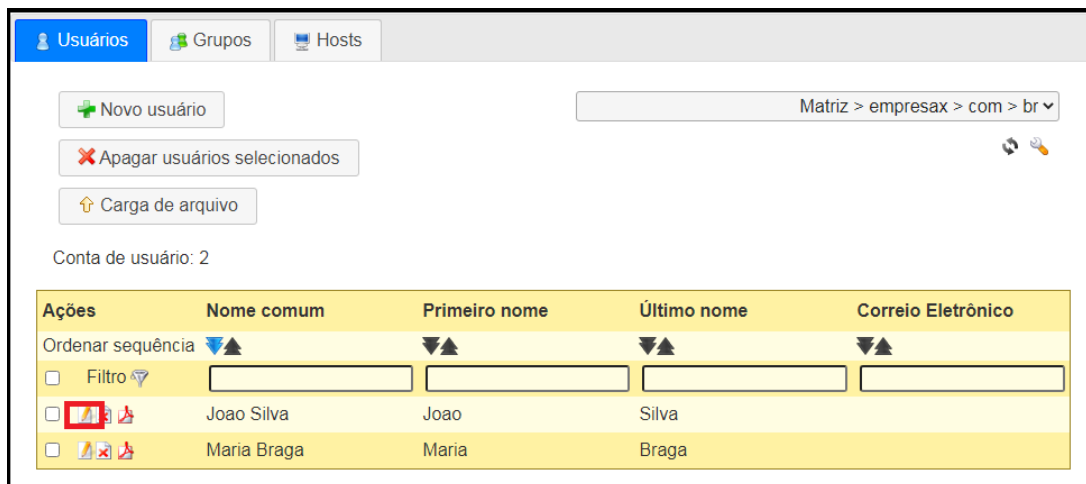


Nas "configurações gerais", desça até a seção "Configurações de segurança" e acrescente na lista de usuários válidos o usuário "**joaosilva**", conforme ilustrado na figura abaixo:

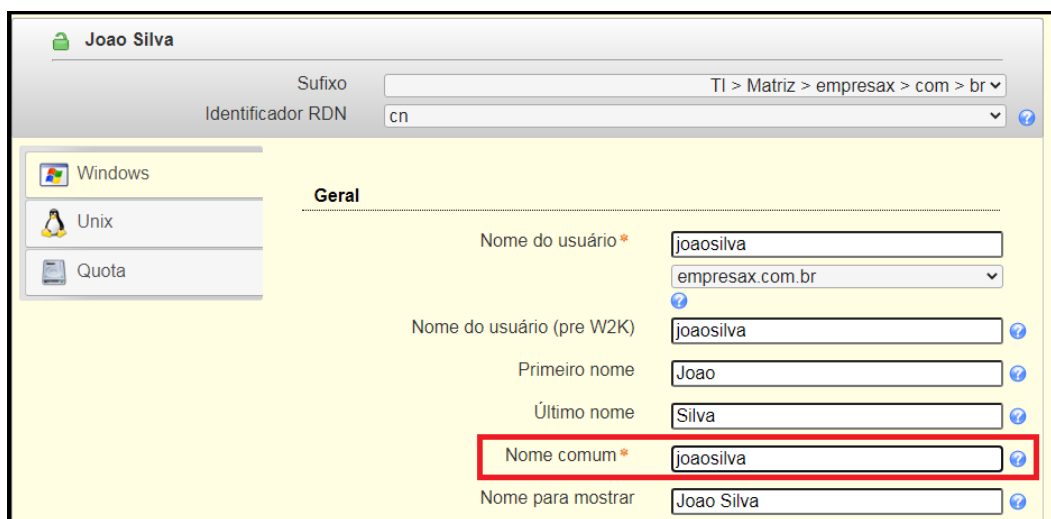




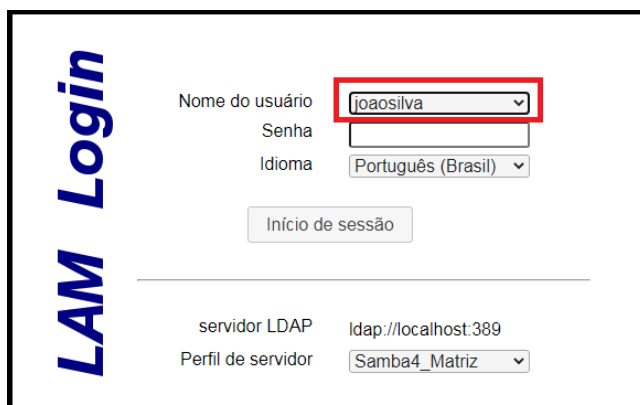
Um ponto importante, para que o usuário "**joaosilva**" consiga autenticar no LAM, é o ajuste do campo "CN" no Active Directory do Samba4, pois este campo não está no padrão que definimos, na Lista de Usuário Válidos, devido a este ter sido criado via RSAT na Estação de Trabalho Windows. Para realizar o ajuste, autentique no LAM com o usuário Administrator e edite as configurações do usuário "**joaosilva**" clicando no ícone "Lápis" ao lado do nome do usuário:



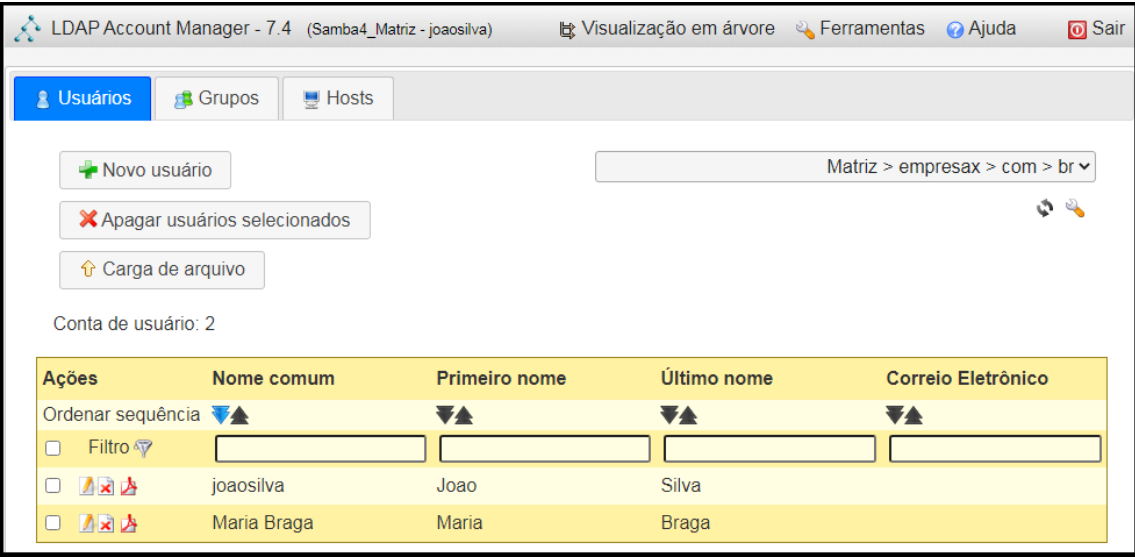
No campo "Nome comum" altere o nome do usuário para o seu login de acesso: **joaosilva**, pois este é o campo "CN" que estamos utilizando para autenticação no LAM.



Após realizar o ajuste, clique em sair e autentique no LAM com o usuário **joaosilva**:



Observe que o usuário **"joaosilva"** tem permissão para acessar a Unidade Organizacional Matriz, bem como administrá-la, criando usuário, grupos, alterando senha e configurações:



**Autorizado o usuário "joaosilva" a autenticar no perfil da Unidade Organizacional Matriz, repita os passos a partir do tópico "6.17.4" e configure o LAM de forma que o usuário "marcovaz" possa autenticar no perfil da Unidade Organizacional Filial.**