

# V WSPPD 2007

Uma visão geral do OpenLDAP e Active Directory para autenticação de usuários em sistemas heterogêneos e distribuídos

Porto Alegre, Agosto de 2007.

Guilherme Matte Macedo, Rafael Bohrer Ávila e Philippe O. A. Navaux  
{gmmacedo, avila, navaux}@inf.ufrgs.br  
Instituto de Informática / UFRGS



# Sumário

- Introdução
- Diretório de Serviços
- Estrutura de um Diretório
- Protocolo DAP e LDAP
- OpenLDAP
- Active Directory
- Autenticação de Usuários
- Conclusão
- Referências
- Perguntas

# Introdução

- Sistemas heterogêneos e distribuídos estão cada vez mais presentes em nosso dia-a-dia
- Necessidade de comunicação e interoperabilidade entre diferentes sistemas
- A comunicação é essencial para todos
- Ela deve ser fácil, simples e independente de plataforma

# Diretório de Serviços

- Conjunto de aplicações que organizam informações e recursos de uma rede, tornando os transparentes para os usuários
- Pode ser visto como uma "lista telefônica"
- Por possuir uma organização genérica, prove interoperabilidade entre diferentes sistemas
- Possibilita a centralização, caso se deseje, de informações sobre os usuários (e.g., logins, senhas, dados pessoais) e recursos
- É parecido com um banco de dados, no entanto, possui grandes otimizações para consultas (leituras)

# Estrutura de um Diretório (1)

- Um diretório é uma árvore de entradas de diretórios
- Cada entrada é composta por um conjunto de atributos, cada um possui um nome e um conjunto de valores
- As entradas possuem um identificador único, o seu Distinguished Name (DN), composto por um Relative Distinguished Name (RDN) -- um atributo da entrada -- e o DN da entrada pai

# Estrutura de um Diretório (2)

- Exemplo de uma entrada em um diretório:

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
fn: John
sn: Doe
phone: 2345 6789
mail: john@example.com
```

- No exemplo acima:

- RDN da entrada: "cn=John Doe"
- DN da entrada pai: "dc=example,dc=com"
- DN da entrada (formado pelo RDN e pelo DN da entrada pai):  
"dn: cn=John Doe,dc=example,dc=com"

# Protocolo DAP e LDAP

- Directory Access Protocol
  - Protocolo para acesso à diretórios de serviços (padrão X.500 - série de padrões sobre diretórios de serviços)
- Lightweight Directory Access Protocol
  - É uma versão mais "leve" do protocolo DAP, que utiliza o protocolo TCP/IP para a comunicação
  - Permite fazer consultas e modificações sobre diretórios de serviços
  - É uma dentre várias soluções (e.g., NDS, NIS, SAMBA)

# OpenLDAP

- É uma implementação livre e de código aberto do protocolo LDAP
- É desenvolvido pelo projeto OpenLDAP
- Disponibiliza um servidor e várias ferramentas para auxiliar nas consultas, inclusão, remoção e sincronização de informações de um diretório
- Permite a interoperabilidade com diretórios rodando em outros sistemas

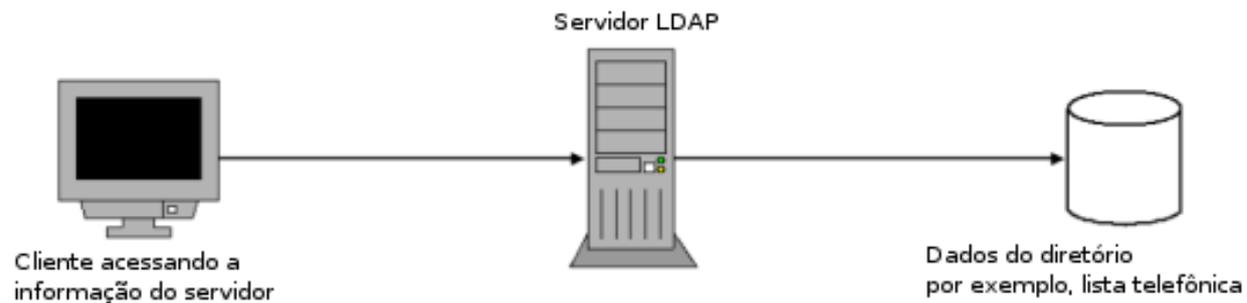
# Active Directory

- É a implementação do protocolo LDAP feita pela Microsoft
- Permite a autenticação de usuários em ambientes Windows
- Com o auxílio do pacote "Services for Unix" e plugins para autenticação, possibilita a interoperabilidade com sistemas Unix

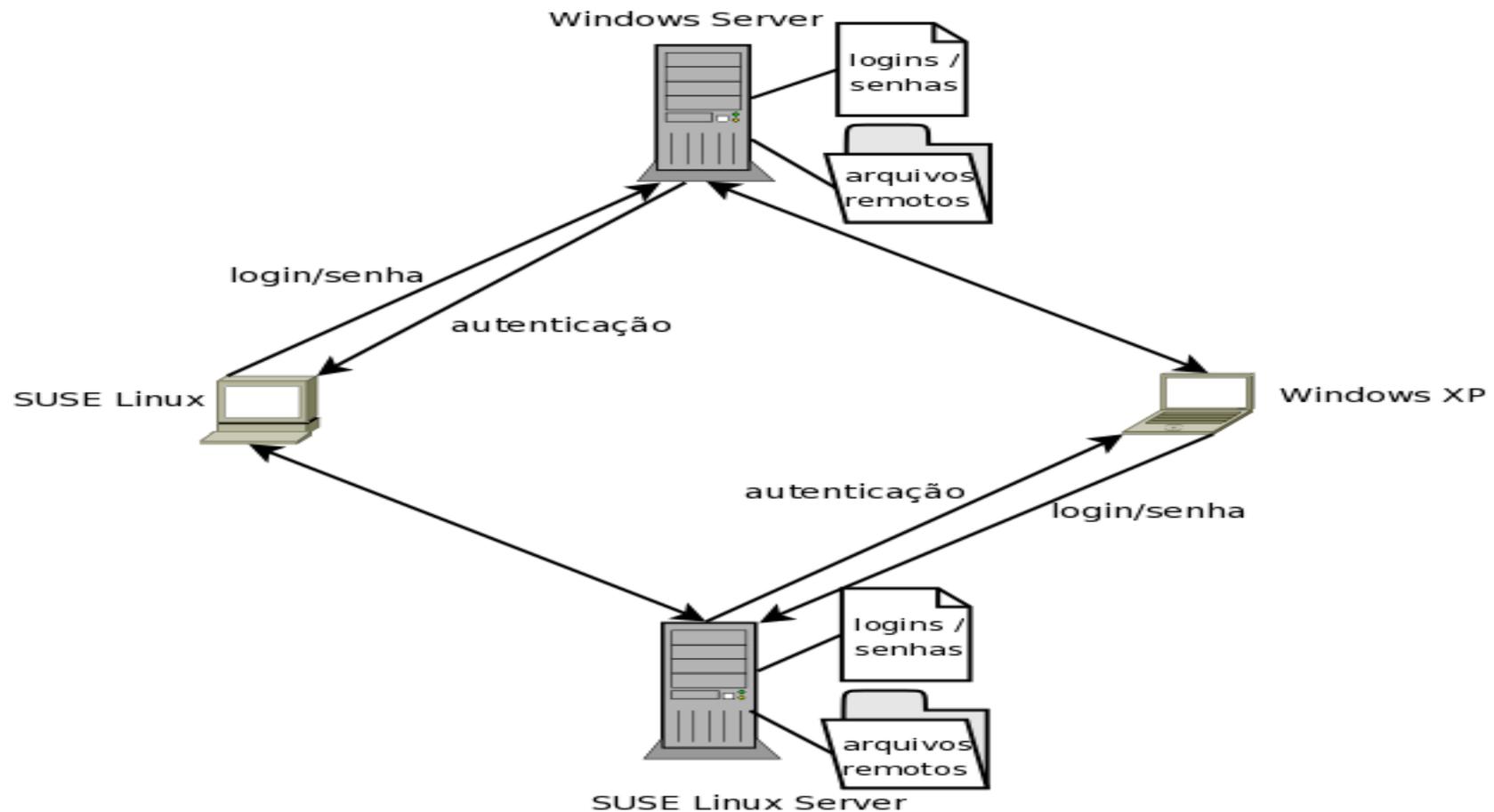
# Autenticação de Usuários (1)

- Para os testes utilizou-se o OpenLDAP, rodando sobre o SUSE Linux, e o Active Directory, sobre o Windows Server e XP, juntamente com o “Services for Unix”
- Cada cliente foi “emulado” sobre uma máquina virtual
- Configurou-se cada um para acessar o servidor de diretórios
- No servidor, criou-se os dados de cada usuário (e.g., logins e senhas)

# Autenticação de Usuários (2)



# Autenticação de Usuários (3)



# Conclusões

- É possível fazer com que sistemas distribuídos e heterogêneos se comuniquem
- A comunicação é simples e rápida
- É transparente ao usuário
- Possibilita que ele se desloque dentro de uma rede, sem ter que levar seus dados / informações juntos

# Referências

- [1] G. M. Macedo, R. B. Ávila e P. O. A. Navaux, "Uma visão geral do OpenLDAP e Active Directory para autenticação de usuários em sistemas heterogêneos e distribuídos", V WSPPD, 2007.
- [2] Wikimedia Foundation, Inc., "Directory Service", [http://en.wikipedia.org/wiki/Directory\\_service](http://en.wikipedia.org/wiki/Directory_service), acessado em Julho/2007.
- [3] Wikimedia Foundation, Inc., "LDAP Protocol", <http://en.wikipedia.org/wiki/Ldap>, acessado em Julho/2007.
- [4] Wikimedia Foundation, Inc., "Active Directory", [http://en.wikipedia.org/wiki/Active\\_directory](http://en.wikipedia.org/wiki/Active_directory), acessado em Julho/2007.
- [5] Núcleo de Desenvolvimento Open Source e Interoperabilidade, [www.codeplex.com/NDOS](http://www.codeplex.com/NDOS), acessado em Julho/2007.

# Perguntas?

Obrigado!