GT Diretórios

Noemi Rodriguez

PUC-Rio

Motivação

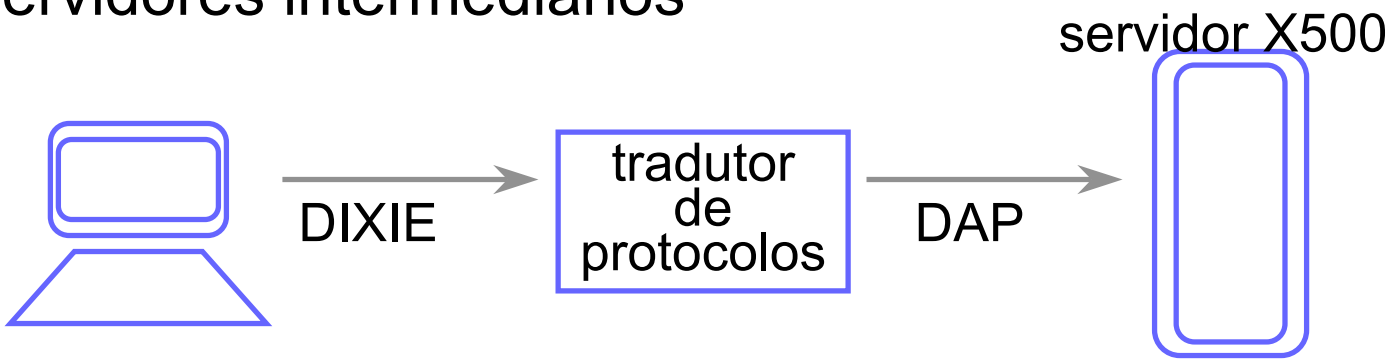
- unificação de gerência de informações
- serviço de catálogo
- diretório de pessoas ou usuários
  - uso mais explorado
  - iniciativas como directory of directories (DoDHE)
- outros usos crescendo
  - autorizações
  - controle de recursos computacionais
  - informações sobre equipamentos e redes
  - informações sobre informações

interação com aplicações

- vídeo digital
  - informações sobre os vídeos
- voip
  - localização de usuários
- aplicações educacionais
  - autorizações
  - armazenamento

histórico

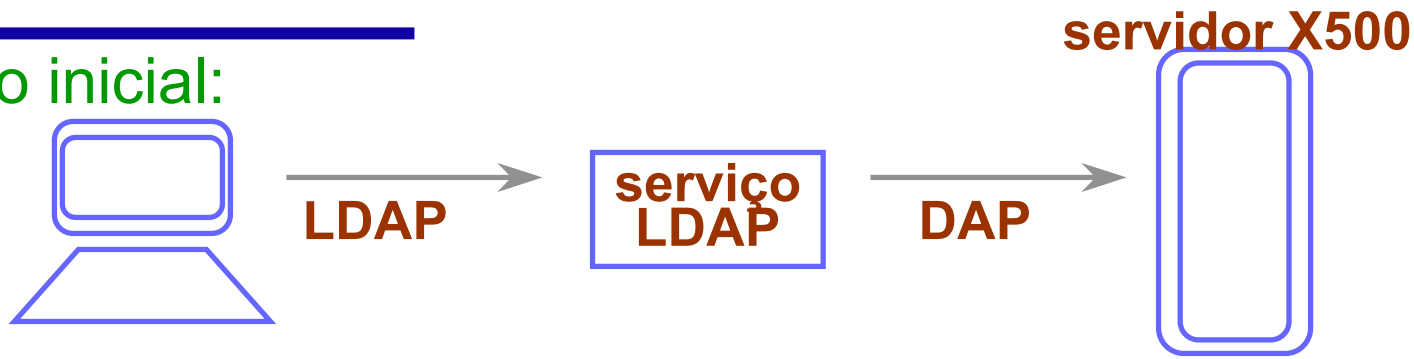
- X500: proposta OSI para serviço
- servidores intermediários



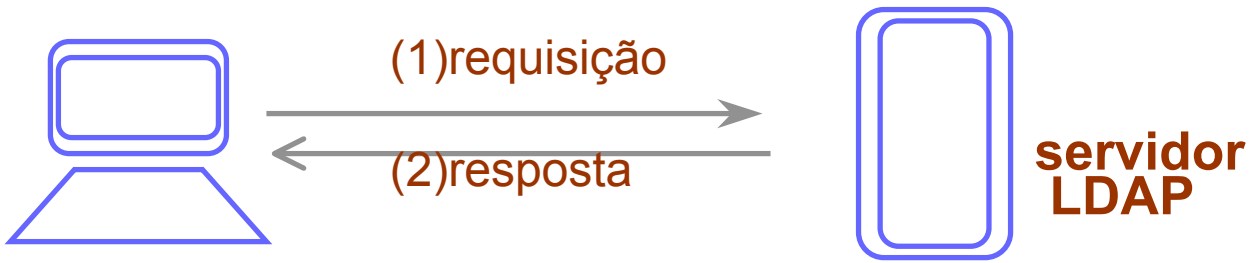
- LDAP: lightweight directory access protocol
  - iniciativa IETF + OSI-DS
  - originalmente como tradutor
  - desenvolvimento inicial na Universidade de Michigan

LDAP como serviço autônomo

uso inicial:

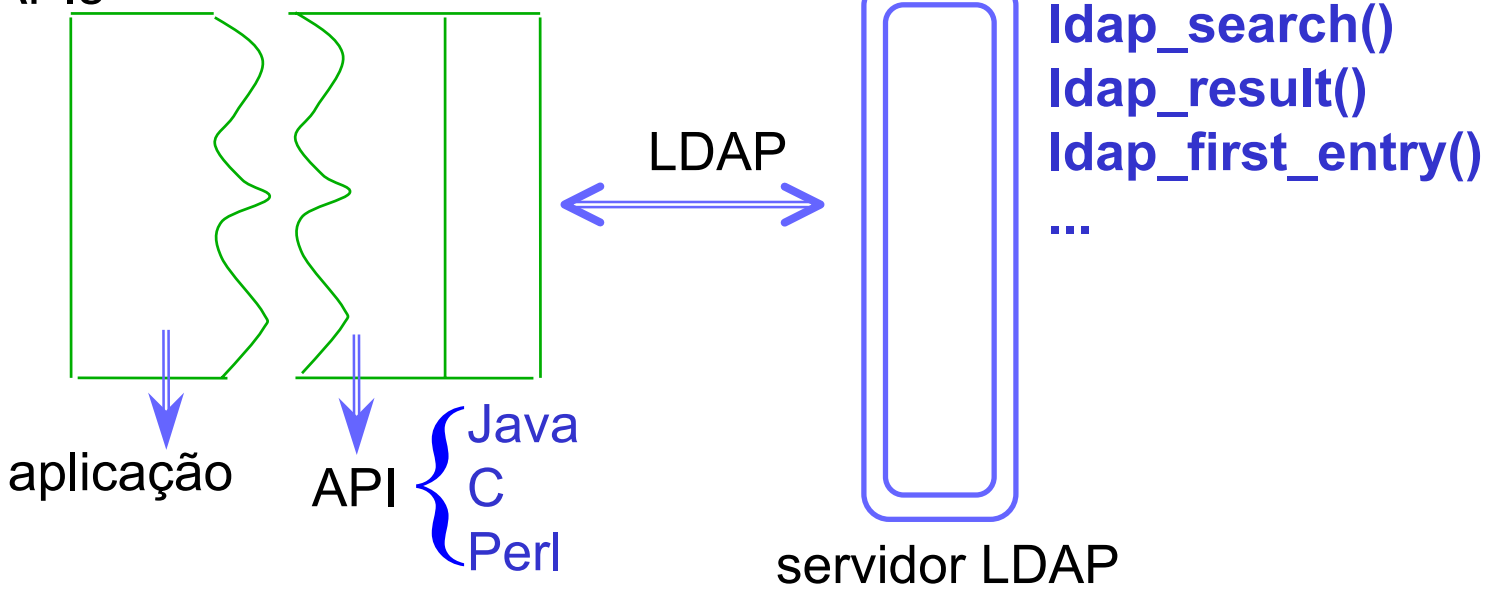


- grande uso vinha através do LDAP
- decisão de tornar o serviço autônomo:



ldap x google

- servidor de informações com protocolo de acesso padrão
- acesso por aplicações
  - APIs



modelo de informação ldap

- diretório *populado* com entradas
- entrada contém pares (atributo, valor)
- atributos:
  - usuário
    - » "todos"...
  - operacionais
    - » data de modificação, quem modificou, ...

esquemas

- definições de atributos
  - sintaxe
  - descrição
  - ...
- definições de classes de objetos
  - atributos permitidos
  - atributos obrigatórios
- espaço de atributos é plano

definição de esquema

- diferentes servidores lêem esquemas em diferentes formatos
- ldapv3: formato padronizado
- atributos, classes de objetos e outros devem ser identificados por um OID (identificador de objeto) único
  - OIDs: como os utilizados em MIBs SNMP
  - obtenção junto à IANA

definição de atributos

```
attributetype ( 2.5.4.41 NAME 'name'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {322768} )

attributetype ( 1.3.6.1.4.1.15996.1.1.84
        NAME 'midiaDuracao'
        DESC 'Duracao do video'
        EQUALITY caseIgnoreMatch
        SYNTAX  1.3.6.1.4.1.1466.115.121.1.15
        ORDERING caseIgnoreOrderingMatch
        SINGLE-VALUE )
```

definição de classe de objeto

```
objectclass ( 1.3.6.1.4.1.15996.1.2.5 NAME 'objMidia'
        DESC 'Midia'
        SUP top STRUCTURAL
        MUST ( midiaNomeArquivo $ midiaTipoArquivo $
                midiaTamanhoArquivo $ midiaQualidade $
                midiaLocalizacao $ midiaDuracao) )
```

- hierarquia permite herança de atributos

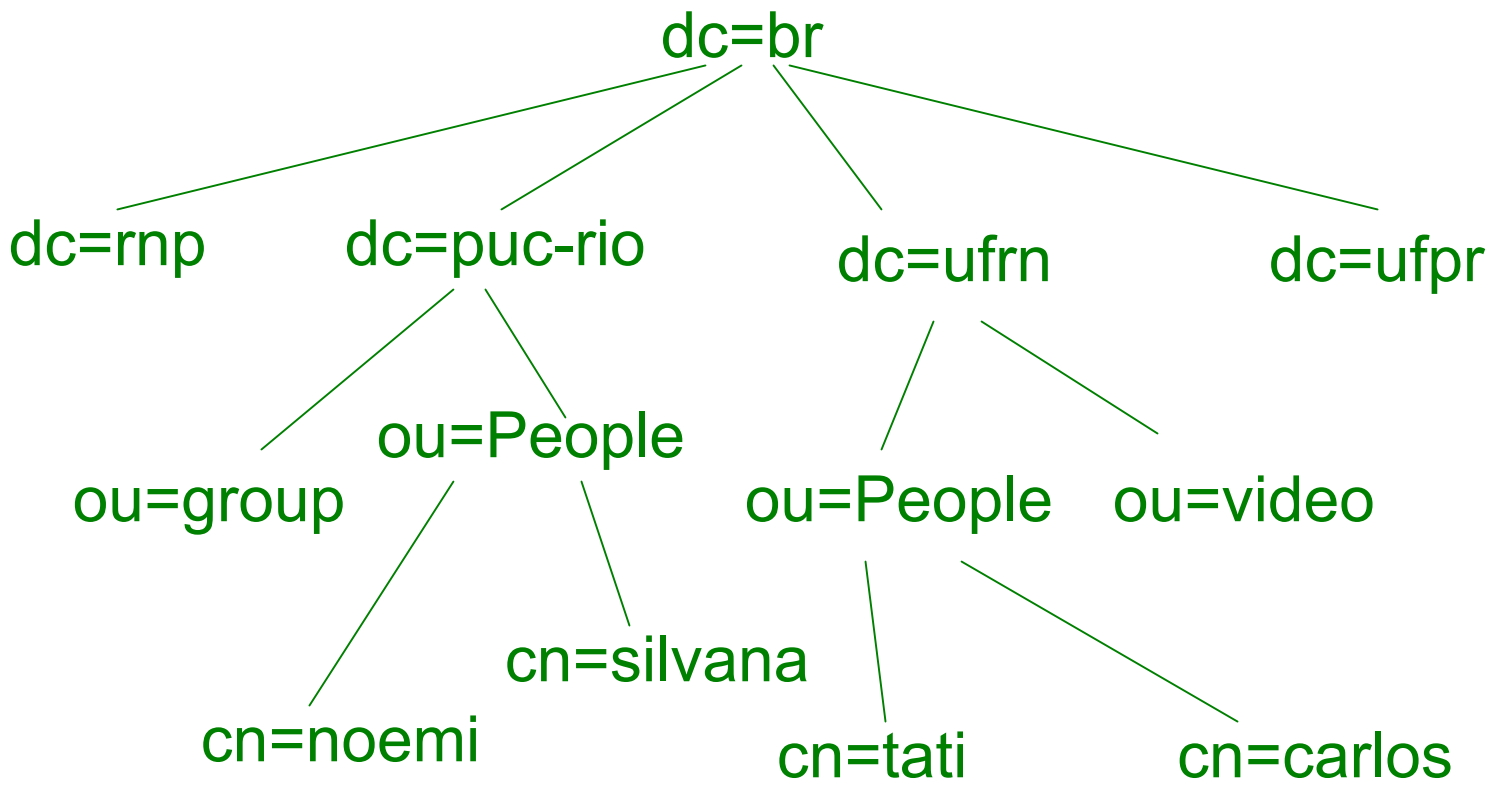
exemplo de entrada

dn: cn=Barbara J Jensen, dc=example, dc=com
cn: Barbara J Jensen
cn: Babs Jensen
objectClass: person
sn: Jensen

} atributos podem ter vários valores

- uma entrada pode pertencer a várias classes de objetos

modelo de nomes



hierarquia

- escolha do número de níveis é livre
- estrutura do diretório é definida através de entradas
  - não há relação com o esquema
- entradas especiais com objectClass: dcObject definem os níveis da árvore
- atributo especial dn indica lugar da entrada na estrutura de árvore

  dn: dc=puc-rio, dc=br

dn: dc=puc-rio, dc=br
objectClass: dcObject
objectClass: organization
dc: puc-rio

openldap

- projeto sucessor da implementação de UMich
  - software aberto
  - servidor ldap
  - bibliotecas para clientes
  - documentação incompleta...
  - www..openldap.org

gt diretórios

- falta de grupos no Brasil trabalhando em questões ligadas a diretórios multi-institucionais
- proposta da RNP: grupo que estudasse serviço e implantasse um piloto envolvendo algumas instituições

gt diretórios

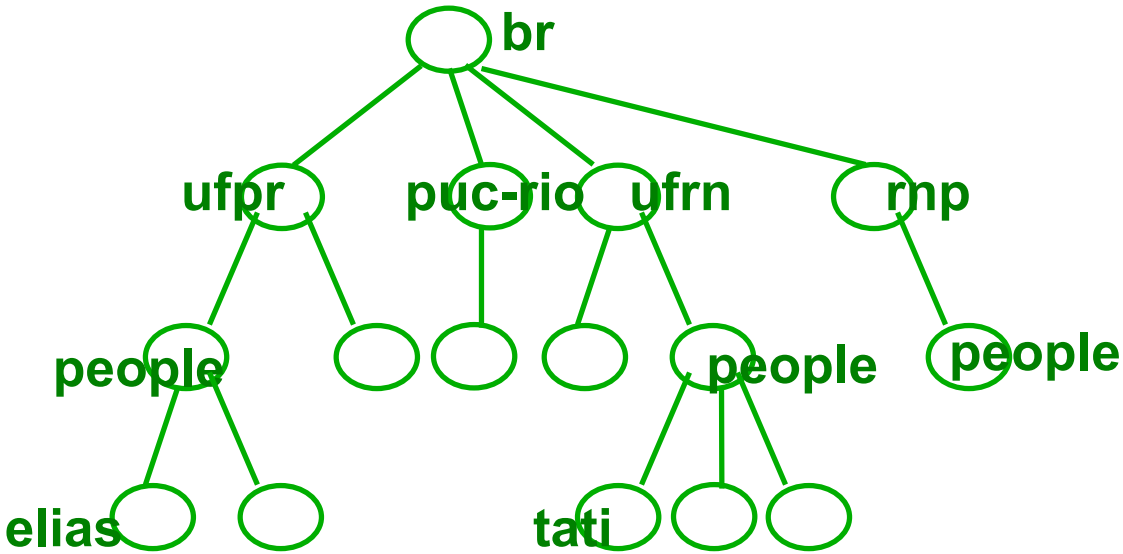
- equipe
  - coordenação: Noemi Rodriguez
  - analistas: Leticia Nogueira
    Silvana Rossetto
- localização
  - laboratório telemídia, PUC-Rio
  - gtdir.inf.puc-rio.br

gt diretórios

- estudo do serviço e acesso
  - servidor
  - interfaces para clientes
  - segurança
  - distribuição
- piloto multiinstitucional
- levantamento de trabalhos em diretórios

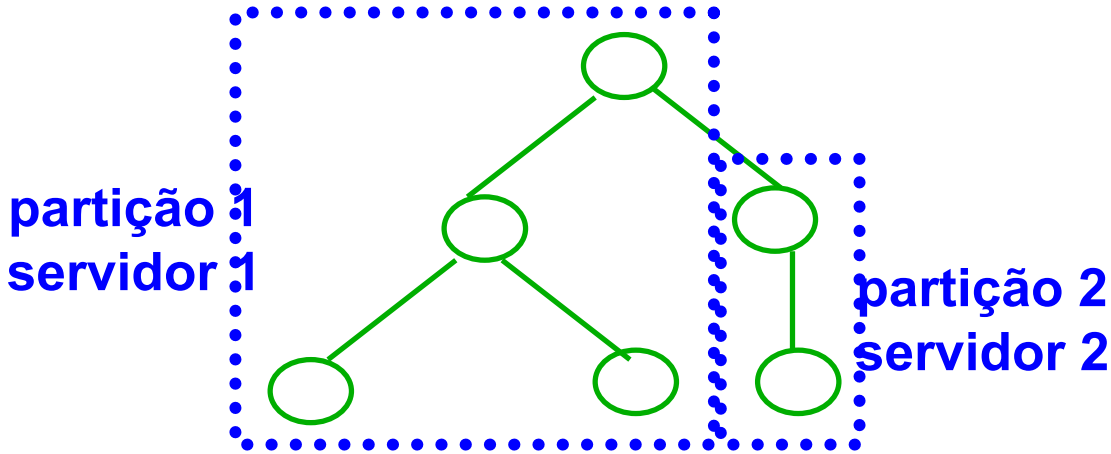
projeto piloto - 1

- experimento com eduPerson e diretório de diretórios
  - diretório único com dados de pesquisadores e professores
  - esquema utilizado: eduPerson



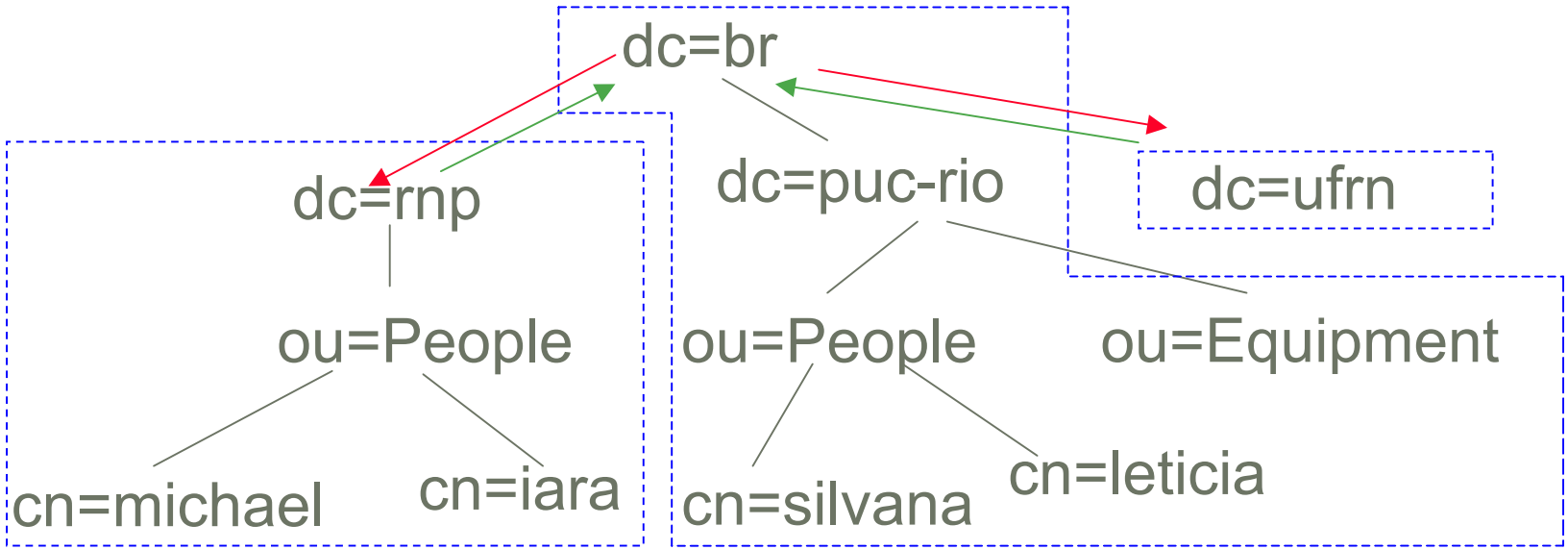
suporte para distribuição

- distribuição de informação (referrals)



unindo as partições

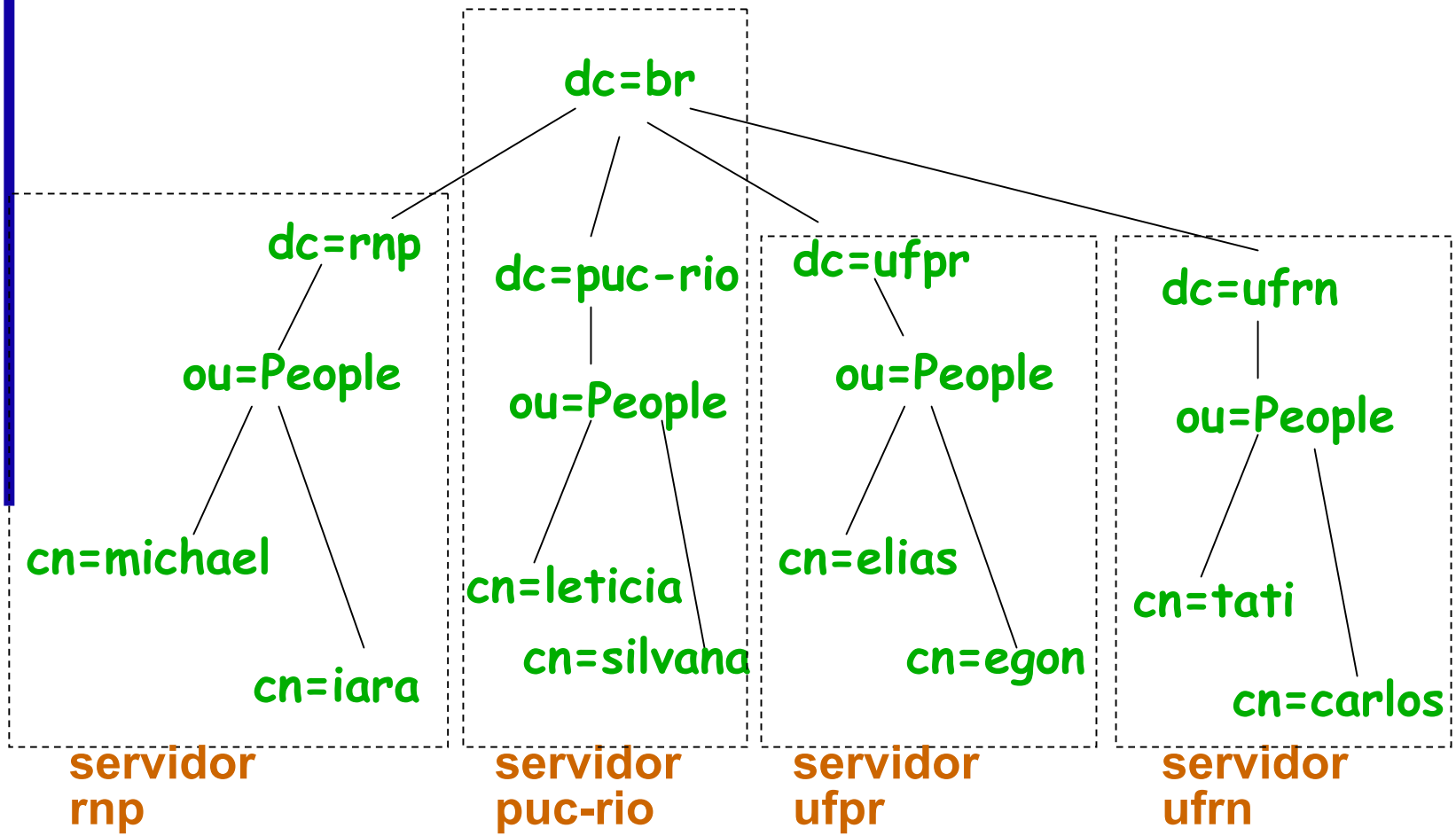
- Referências de conhecimento imediatamente superior
- Referências subordinadas



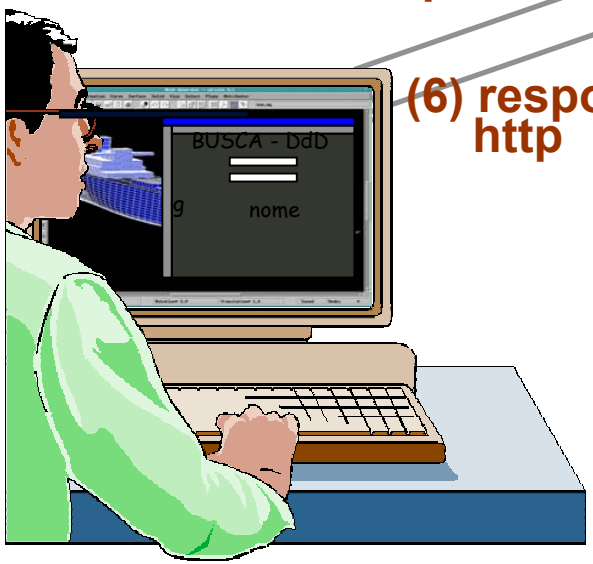
métodos para unir as partições

- Referrals
  - Indicação do próximo servidor a ser contactado é retornada ao cliente
  - funções fazem acesso aos diferentes servidores automaticamente.
- Chaining
  - Servidor entra em contato com outros servidores antes de retornar a resposta ao cliente

particionamento piloto



piloto 1 - distribuição



servidor www

servidor LDAP PUC-Rio

servidor LDAP UFPR

(1) requisição http

(2)requisição ldap

(3)referral

(4)requisição ldap

(5)resposta

(6) resposta http

aplicação Java (servlets)
api Java/LDAP

modelo de segurança

- autenticação por credenciais
  - v2: senhas ou kerberos
- v3: forma de autenticação não definida pelo padrão
  - negociação SASL
    - » senha
    - » kerberos
    - » external: ssl, tls ou ipsec
  - credenciais podem ser passadas sobre TLS ou SSL
- controle de acesso
  - padrão não define como deve ser especificado
    - » listas de controle de acesso
    - » entradas em arquivo de configuração

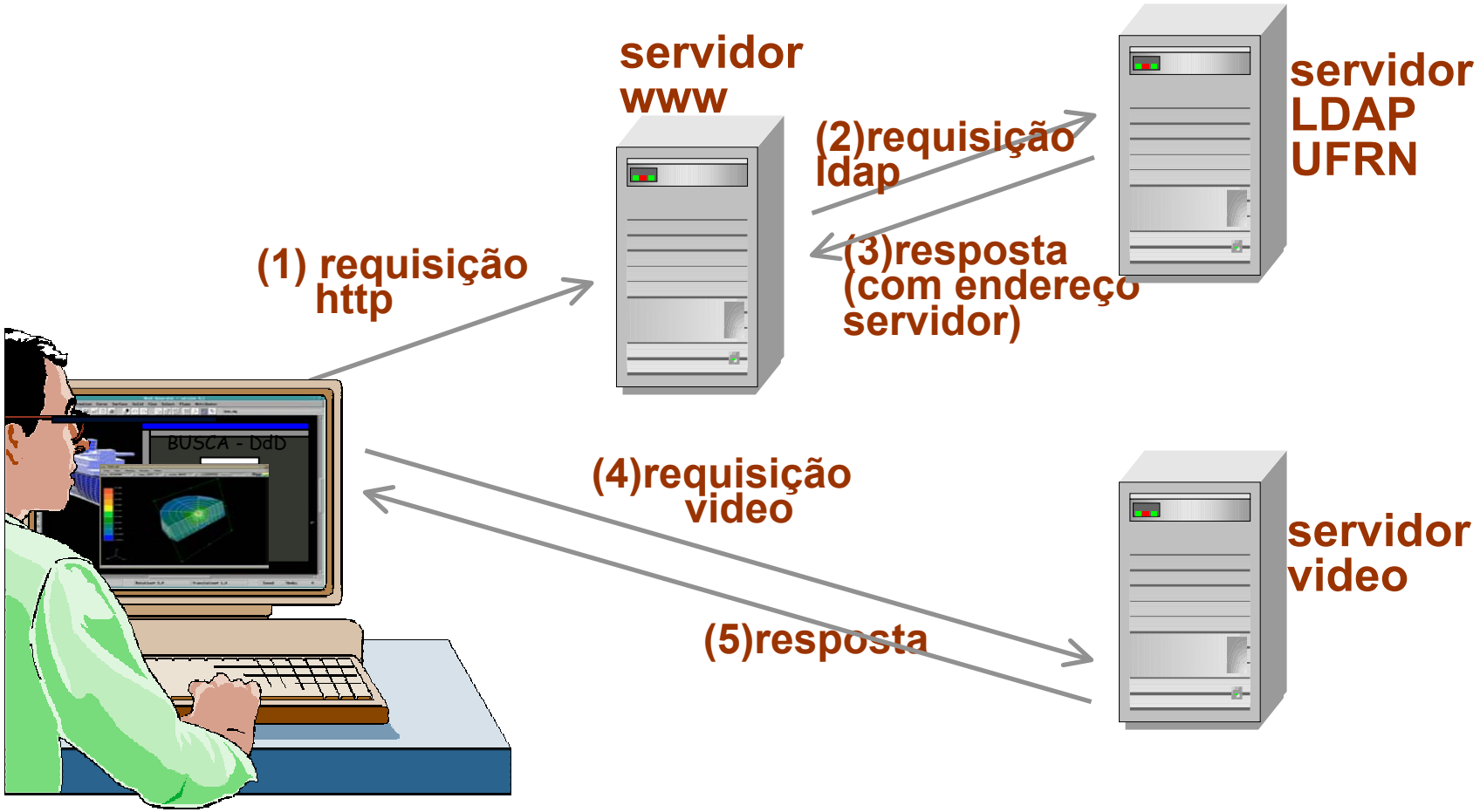
segurança no piloto

- autenticação com senhas passadas sobre TLS
  - autenticação com certificados TLS ainda não funciona
- cada servidor tem certificado assinado pelo servidor raiz
- controle de acesso: info sobre usuário
  - (no openldap por arquivo de configuração)
  - consulta: só para usuário cadastrado naquele servidor
  - alteração: só root ou o próprio usuário
- para que referrals funcionem:
  - aplicação de busca é 'usuário' cadastrado em todos os servidores

projeto piloto - 2

- diretório como apoio para serviço de video sob demanda
  - projeto integrado com o GT de vídeo
- projeto de um esquema específico
  - trabalho conjunto dos dois GTs
  - GT Video: especificação dos atributos de interesse
  - GT Diretórios: especificação do esquema
  - GT Video: população do diretório com entradas de videos
  - GT Diretórios: desenvolvimento de aplicação de consulta

piloto 2 - vídeos



próximas etapas

- envolvimento de um número maior de intituições
- discussão do esquema
  - eduPerson é realmente o adequado?
- diretório de diretórios como serviço estável
  - raiz na RNP
  - treinamento em configuração e gerência

o que se está fazendo em diretórios

- administração de sistemas computacionais
  - UFMG
  - UFBA
  - diretório como repositório de autorizações para recursos computacionais
- projetos mais específicos
  - InCor
- pouca coisa inter-institucional
  - computação em grade

resultados

- integração com outros grupos
  - experiência de trabalho integrado com GT video
  - interação com grupo UFRN
- entendimento e documentação do openldap
  - configuração
  - réplicas
  - referrals
  - proteção
- identificação de trabalhos na área

por fazer...

- estudos de configuração
  - réplicas e escalabilidade - testes de carga
  - autenticação com certificados
- interface de programação
  - interfaces simplificadas
  - crescimento de uso
  - DSML: proposta de padrão para comunicação XML
    - » dados
    - » operações