Instalação e personalização do Debian Etch para servidores LDAP e Shibboleth.

Éverton Foscarini, Leandro Rey, Francisco Fialho, Carolina Nogueira

[1]Universidade Federal do Rio Grande do Sul
Centro de Processamento de Dados
Rua Ramiro Barcelos, 2574 – Portão K – Porto Alegre – RS

foscarini@foscarini.biz, {leandro,francisco,carol}@cpd.ufrgs.br

Resumo. *Este artigo descreve a solução criada pela UFRGS para a implantação de servidores LDAP em Instituições Federais de Ensino Superior como parte do Projeto Diretórios da RNP. Após uma breve descrição dos objetivos do Projeto Diretórios são listados os procedimentos que são seguidos pelo instalador para a configuração dos softwares, assim como as interações que são feitas com o usuário durante os passos da instalação.*

1. Projeto Diretórios

O Projeto Diretórios da RNP foi criado com o objetivo de incentivar a instalação de diretórios LDAP nas instituições federais de ensino superior (IFES), assim como a padronização das informações institucionais através da criação de um esquema LDAP unificado, o brEduPerson. Uma das formas de acelerar essa implantação é com a criação de uma federação entre as IFES, de forma a possibilitar o compartilhamento de aplicações web e de informações dos usuários entre essas aplicações.

As atividades do Projeto Diretórios compreendem:

- Definição esquema EduPerson - RNP
- Definição técnica para implantação de uma federação - RNP
- Criação de uma ferramenta de importação de dados (EID) que facilite o povoamento do diretório das instituições - UFMG
- Criação de uma metodologia de implantação para os serviços definidos pelo projeto - UFRGS, testes pela UFF, CEFET-MG e UFC
- Desenvolvimento de uma aplicação que use os recursos da federação - UFC e CEFET-MG
- Criação de material de treinamento para capacitação de pessoal - UFMG
- Implantação da solucão - RNP

O software servidor de diretórios escolhido pelo projeto foi o OpenLDAP [OpenLDAP 2008], por ser um software livre e muito utilizado, inclusive já em produção em algumas das IFES participantes do projeto. O esquema brEduPerson é baseado no eduPerson [eduPerson 2008], com algumas modificações implementadas pelo Projeto Diretórios de forma a contemplar os vínculos de usuários existentes nas IFES brasileiras. A federação é baseada no software Shibboleth [Shibboleth 2008], que permite que serviços distribuídos possam efetuar a autenticação no domínio da universidade de origem do usuário. A figura 1 mostra um esquema básico de autenticação Shibboleth em uma plataforma de ensino à distância:

Descrição das interações da autenticação Shibboleth:

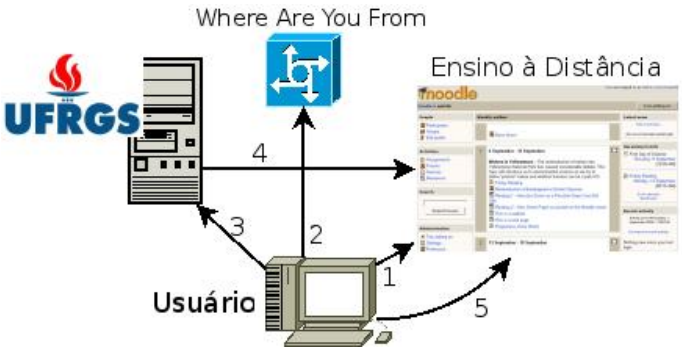

Figure 1. Arquitetura do Shibboleth

1. Usuário acessa plataforma de ensino à distância de qualquer IFES e solicita autenticação Shibboleth.
2. Usuário é redirecionado ao WAYF e deve informar em qual IFES deseja autenticar.
3. Usuário autentica-se em página de login do domínio da sua instituição.
4. Servidor da IFES informa ao servidor de EAD que o usuário é legítimo.
5. Usuário completa acesso à plataforma de ensino à distância.

2. Metodologia de Implantação

Um dos objetivos do projeto é a instalação de um servidor com os softwares OpenLDAP e Shibboleth-IDP em cada IFES, de forma que todas tenham um servidor de diretórios contendo os dados de seus usuários para fim de autenticação e por conseqüência participem da federação. Entretanto o projeto não pode partir do pressuposto que todas as instituições tenham em seu quadro de pessoal equipes com experiência de instalação e gerenciamento de servidores GNU/Linux.

Para contornar esse problema, ficou a cargo da UFRGS estabelecer uma metodologia de implantação dos softwares necessários para que as instituições fizessem parte do projeto. Essa metodologia deve conter mecanismos que facilitem a implantação da solução por pessoal menos especializado.

De forma a atender essa demanda, foram criados scripts que facilitam e até automatizam certos aspectos da instalação do sistema operacional e dos softwares escolhidos pelo projeto, realizando inclusive a criação das chaves criptográficas e dos arquivos de configuração. Também foi criada documentação que guia a instalação do sistema utilizando esses scripts. No próximo capítulo será apresentada a arquitetura da solução e serão listados os passos da instalação que foram automatizados, com um breve relato das configurações utilizadas para cada software.

3. Arquitetura da solução

A solução implementada pela UFRGS consiste em criar um conjunto de scripts de automatização da instalação do *Debian Etch* e armazená-los no servidor web *pacotes.ufrgs.br*, para que sejam acessados durante a instalação do sistema operacional. A figura 2 exemplifica o esquema utilizado. Seguem as descrições dos scripts que são utilizados durante a instalação:

- **preseed.cfg**: Contém configurações que devem ser usadas pelo instalador do Debian (ver seção 3.1).

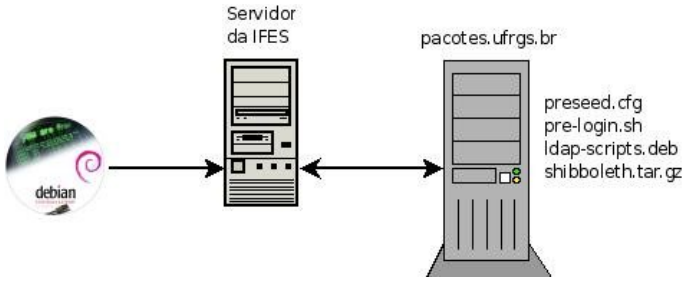

Figure 2. Seqüência de instalação

- **sources.list**: Lista de repositórios dos pacotes do Debian.
- **pre-login.sh**: Script que contém toda a automatização da instalação dos softwares (ver seção 3.2).

3.1. Instalação do Debian Etch

Ao iniciar a instalação do Debian o usuário deve informar ao instalador a URL do arquivo *preseed.cfg*. Logo após à configuração de rede, o programa de instalação do Debian busca o arquivo no servidor web *pacotes.ufrgs.br*. Este arquivo contém configurações pré-definidas para parâmetros do programa de instalação do Debian.

As principais pré-definições são as seguintes:

- **Particionamento:** É apresentado ao usuário um esquema de particionamento personalizado, contendo partições separadas para os dados do OpenLDAP, arquivos de log e arquivos de sistema. Este esquema de particionamento é otimizado para o uso de servidor de diretórios. O esquema pode ser modificado pelo usuário antes de ser gravado no disco.
- **Seleção de pacotes:** O perfil do sistema é escolhido automaticamente, instalando apenas os pacotes básicos do Debian. Um perfil mais enxuto é preferido pois os softwares que seriam instalados por padrão pelo Debian teriam de ser excluídos posteriormente, aumentando o tempo da instalação e a sua complexidade.
- **Preparação para o primeiro boot:** O último passo realizado pelo instalador do Debian consiste em preparar a execução do script *pre-login.sh* no primeiro boot do sistema. Este script guiará o usuário durante a instalação dos softwares necessários para tornar o *host* um servidor OpenLDAP, Shibboleth ou outros.

3.2. Instalação dos serviços

No primeiro boot do sistema operacional é executado o script *pre-login.sh*, que automatiza a instalação e configuração de diversos softwares. Segue a lista de softwares instalados e uma descrição detalhada das configurações específicas.

3.2.1. Servidor de email e de hora

- **postfix:** As telas de configuração do servidor de email são suprimidas e é escolhido o perfil de instalação simplificado. Além disso, é solicitado que o usuário informe ao programa de instalação um endereço de email para o qual serão enviados alarmes ou mensagens de erro.

- **ntpd:** O programa de instalação oferece ao usuário a opção de escolher um servidor de hora personalizado. Após o fornecimento do endereço pelo usuário é efetuada uma atualização de hora para testar se o servidor está acessível. Caso o usuário não forneça nenhum servidor, é utilizado o servidor de hora do Cais (*ntp.cais.rnp.br*).

3.2.2. Servidor OpenLDAP

É realizada a instalação dos pacotes *slapd* e *ldap-scripts*. O *ldap-scripts* é um pacote criado pela UFRGS que faz o monitoramento do estado do *slapd*, reiniciando-o ou recuperando-o quando necessário, além do backup diário da base LDAP.

- **Perfil de instalação:**A instalação do OpenLDAP pode ser feita em diferentes perfis, de acordo com as necessidades de escalabilidade e tolerância à falhas. A escolha do perfil a ser usado é realizada no momento da instalação, através de telas que oferecem as opções de configuração. O arquivo de configuração do OpenLDAP é gerado automaticamente contendo as configurações necessárias para cada perfil.
  - **Único:** Deve ser escolhido no caso de ser instalado um único servidor para o domínio. Este servidor será configurado para realizar backup diário da base de dados.
  - **Múltiplos:** Abre a opção para instalar mais de um servidor para o mesmo domínio, entretanto um deles deverá ser o mestre (que recebe atualizações) e o(s) outro(s) será(ão) apenas cópia(s). Após escolher o perfil "múltiplos", deve-se decidir se aquele servidor será mestre ou escravo.
    - **Mestre:** É o servidor principal do domínio. Não realiza o backup diário (delega essa obrigação a um escravo) e é configurado para permitir que o(s) escravo(s) tenha(m) acesso à toda a base de dados. Esse acesso é controlado através de uma senha de replicação, que será cadastrada na instalação do mestre e fornecida posteriormente durante a instalação do(s) escravo(s).
    - **Escravo:** Ao instalar um escravo, o instalador solicita que seja informado o endereço do servidor mestre, assim como a senha de replicação. O instalador também pergunta ao usuário se é este escravo que deverá realizar o backup diário da base LDAP.
- **Cadastramento inicial de usuários:** O programa de instalação efetua o cadastramento de alguns usuários padrão, solicitando que sejam fornecidas as respectivas senhas.
  - **Administrador:** O administrador da base LDAP é cadastrado somente se o servidor é único ou mestre, visto que em um servidor escravo a senha é replicada diretamente do mestre.
  - **Leitores:** É cadastrado o usuário *leitor-shib*, que terá acesso aos dados dos usuários para posterior compartilhamento via Shibboleth-IDP.
  - **Usuários de teste:** Para facilitar o teste do LDAP e do Shibboleth-IDP, são criados dois usuários com senhas padrão, que podem ser apagados pelo administrador quando o sistema entrar em produção.

- **Configuração do TLS:** O instalador cria o certificado SSL e a chave criptográfica para o OpenLDAP. É sugerido que o usuário forneça os dados que farão parte do certificado, como cidade, UF, país e organização, entre outros. O programa de instalação também está preparado para criar o certificado sem esses esses dados.

3.2.3. Shibboleth-IDP

O Shibboleth-IDP é um software cuja instalação é bastante complexa, pois tem uma extensa lista de dependências e mais de 15 arquivos de configuração que devem ser criados/editados para que o serviço funcione e se integre com *Apache*, *Tomcat* e OpenLDAP. Através do programa de instalação foi possível simplificar muito o processo, resumindo as interações do usuário à 4 telas que devem ter opções preenchidas e mais algumas confirmações e telas de avisos. Seguem informações sobre as interações com o usuário e sobre os principais arquivos criados no processo.

- **Cadastramento do servidor LDAP:** O instalador solicita o endereço do servidor LDAP e a senha do usuário *leitor-shib*.
- **Configurações do Apache/Tomcat:** O programa de instalação faz a criação dos sites virtuais e a habilitação dos módulos necessários para a conexão do *Apache* ao *Tomcat*. Também são criados os arquivos de configuração do *Tomcat* e são instalados o *esup-cas-server* e o *cas-client-java*, softwares necessários para efetuar a autenticação dos usuários no LDAP.
- **Criação do certificado SSL do Apache/Shibboleth-IDP:** É utilizado o mesmo algoritmo de criação de chave usado para o OpenLDAP. Este certificado será utilizado para autenticar as conexões do servidor Shibboleth-IDP na federação.
- **Configuração do Shibboleth-IDP:** Os arquivos de configuração do Shibboleth-IDP que são automaticamente criados e configurados pelo programa de instalação são os seguintes:
  - **idp.xml:** Contém as configurações básicas do Shibboleth-IDP, tais como os nomes das federações à que faz parte, caminho para os arquivos que contém as chaves criptográficas utilizadas para autenticar os dados, nível de verbosidade dos logs, URL's de acesso ao serviço e os caminhos para os arquivos de configuração secundários.
  - **resolver.ldap.xml:** Contém as configurações para acesso ao servidor LDAP e dos atributos que devem ser buscados na base de dados.
  - **arp-site.xml:** Contém as políticas de liberação de atributos, que controlam o envio de informações dos usuários à outras instituições que fazem parte da federação.
- **Template de metadados para federação:** O instalador prepara o arquivo *federação-metadata.xml*, que contém os metadados do servidor recém instalado e que devem ser distribuídos pela federação. Esse arquivo deve ser encaminhado ao administrador da federação.

3.2.4. Shibboleth-SP

O programa de instalação criado pela UFRGS também possui um fluxo de instalação do Shibboleth-SP. Esse fluxo só poderá ser seguido caso o Shibboleth-IDP não tenha sido

instalado na máquina por questão de incompatibilidade entre as configurações. Segue um resumo do fluxo de instalação e das configurações utilizadas.

- **Configuração do Apache:** É executada a instalação do módulo *libapache2-mod-shib* no *Apache*, que provê suporte à autenticação Shibboleth. Também é criado um site virtual já com suporte à essa autenticação, para que o administrador possa testar o funcionamento do Shibboleth-SP.
- **Configuração do Shibboleth-SP:** A configuração do Shibboleth-SP é bem mais simples do que a do Shibboleth-IDP, consistindo em apenas 2 arquivos que são configurados automaticamente:
  - **shibboleth.xml:** Contém as configurações do *host*, certificado SSL, o caminho para os metadados da federação à que ele faz parte e a URL do WAYF (Where Are You From).
  - **AAP.xml:** Contém a política de aceitação de atributos, que indica quais atributos o Shibboleth-SP pode aceitar provenientes de outros domínios. Essa configuração permite o controle de acesso dos usuários Shibboleth aos serviços hospedados no site.
- **Template de metadados para federação:** Assim como ocorre na instalação do Shibboleth-IDP, o instalador gera um arquivo padrão com os metadados do servidor.

4. Conclusões

A criação dos scripts de automatização da instalação facilitou bastante o processo de instalação dos softwares, visto que grande parte das configurações são feitas de forma quase automática, demandando apenas alguma assistência por parte do usuário que está procedendo a instalação.

De acordo com um teste de instalação realizado, foi possível ter um servidor OpenLDAP + Shibboleth-IDP instalado e funcionando integrado a uma federação já existente em aproximadamente 30 minutos, contando com o tempo de instalação do sistema operacional. É importante fazer a ressalva que o download dos pacotes e dos arquivos foi feito a partir da rede local, pois é a UFRGS que mantém o repositório de pacotes.

Realizando uma análise dos fluxos de instalação, também é possível visualizar que a instalação do OpenLDAP + Shibboleth-IDP acaba por criar ou fazer alterações em 28 arquivos de configuração diferentes. Essas operações seriam maçantes e suscetíveis à erros, de forma que a automatização garante que todas serão executadas e corretas.

O resultado desse trabalho foi a criação de um instalador modular, o qual pode ser futuramente estendido para conter fluxos de instalação dos mais variados softwares. Esse instalador viabiliza a implantação dos serviços definidos pelo Projeto Diretórios nas IFES de todos os portes, simplificando o processo de configuração dos softwares necessários para integração de uma IFES à federação que será estabelecida.

References

eduPerson (2008). http://www.educause.edu/eduperson/, acesso em Mar de 2008.

OpenLDAP (2008). http://www.openldap.org/, acesso em Mar de 2008.

Shibboleth (2008). http://shibboleth.internet2.edu/, acesso em Mar de 2008.