# Pam com LDAP

Autoria de Giancarlo Rubio
04/04/2008
Última Atualização 06/04/2008

FreeBSD e PAM

O FreeBSD suporta a autenticação do PAM no LDAP desde a versão 5.1. A minha necessidade foi quando um servidor de e-mail, necessitava da permissão de leitura e escrita no home do usuário e sendo que o servidor LDAP não estava na mesma máquina.

Porque usarei PAM?

O PAM permite que inúmeras aplicações (squid,apache,postfix,etc..) autentiquem em sua base de usuários sem ter que configurar cada uma delas para a autenticação, no meu caso na base LDAP.

FreeBSD e PAM

O FreeBSD suporta a autenticação do PAM no LDAP desde a versão 5.1. A minha necessidade foi quando um servidor de e-mail, necessitava da permissão de leitura e escrita no home do usuário e sendo que o servidor LDAP não estava na mesma máquina.

Instalando os pacotes necessários

* Pressuponho que você já tenha uma base LDAP configurada e populada.
Adicionamos os pacotes nss_ldap e pam_ldap
#pkg_add -rv nss_ldap pam_ldap

Ou se preferir via ports
# cd /usr/ports/net/nss_ldap/
# make install clean
# cd /usr/ports/security/pam_ldap/
# make install clean

Configurando

Devemos agora configurar nosso ldap.conf e nss_ldap.conf. Copie os originais
#cp /usr/local/etc/nss_ldap.conf.dist /usr/local/etc/nss_ldap.conf
#cp /usr/local/etc/ldap.conf.dist /usr/local/etc/ldap.conf

Abra ele com seu editor preferido e altere as seguintes linhas de acordo com suas configurações dos 2 arquivos (nss_ldap.conf e ldap.conf

- host 127.0.0.1
- base dc=padl,dc=com
- rootbinddn cn=manager,dc=padl,dc=com ( Esta tem que ser descomentada)

Crie o arquivo ldap.secret com a senha do seu "Manager ou Admin" da sua base ldap e de permissão de leitura e escrita somente para o root
# echo 'minhasenha' > /usr/local/etc/ldap.secret
# chmod 600 /usr/local/etc/ldap.secret

Abra seu arquivo /etc/pam.d/system e adicione a linha abaixo
auth sufficient /usr/local/lib/pam_ldap.so no_warn try_first_pass
antes desta "auth required pam_unix.so no_warn try_first_pass nullok".

Edite agora seu /etc/nsswitch.conf alterando as linhas
group: compat -> group: files ldap
passwd: compra -> passwd: files ldap

Testando

Para verificar se tudo ocorreu bem um simples id deverá retornar seu usuário da base ldap
#id nomedousuario

Se não funcionar verefique seu messages a caça de algum erro.
Se mesmo assim não funcionar, rode seu ldap em modo debug provavelmente seu ldap está "bindando de forma errada" (usuário, senha, base).

Problemas e Soluções

Ao reiniciar a máquina o slapd demorava quase 2 minutos para subir.O que acontecia?? Percebi que o daemon ao iniciar sobe com o usuário slapd, a minha configuração do pam manda ele procurar no ldap mais se ele não está de pé como vai achar?? Após muitas horas de google cheguei a solução.

Troquei no meu nss_ldap.conf a opção bind_policy de hard para soft. Logo se o ldap falhar ele não tentará conectar várias vezes e retorna um erro de conexão.

Referências
Quick and dirty FreeBSD 5.x and nss_ldap mini-HOWTO