

Integrando serviços de email Linux ao Active Directory

Alexandro Silva
alexos@ngsecurity.com.br
<http://penguim.wordpress.com>

- **Apresentação**
- **Escopo do Projeto**
- **Clusterização**
- **Antes e Depois**
- **Desafios**
- **Conceitos Básicos**
- **Solução**
 - **Postfix (SMTP)**
 - **Dovecot (IMAP e POP3)**

Who I am?

- **Hacker**
- **Professor da Graduação e Pós-Graduação da Unijorge;**
- **Fundador da célula de Software Livre da Unijorge;**
- **Coordenador do Núcleo de Soluções Tecnológicas da Unijorge;**
- **Consultor em Segurança da Informação e Tecnologias OpenSource.**
- **Membro oficial do Ubuntu Internacional**

Escopo do projeto

- **Implantação de uma solução robusta e completa de groupware livre numa infraestrutura clusterizada totalmente integrada ao ambiente proprietário de autenticação.**

Clusterização

- Ambiente Red Hat usando o Red Hat Cluster Suite e o GFS, permitindo assim um ambiente de alta disponibilidade com os arquivos disponíveis numa infraestrutura de storage.

Antes

- Lotus Notes
- Sem autenticação integrada:
 - Duplicação de usuários e senhas;
 - Sem padronização;
 - Difícil manutenção.

Depois

- **Egroupware**
- **Autenticação centralizada:**
 - Base única de usuários e senhas;
 - Padronização;
 - Fácil manutenção.

Desafios

- Como fazer a integração dos serviços com o Active Directory?
- Como fazer a manutenção dos usuários de forma centralizada?
- Como manter alta disponibilidade em conexões não persistentes?

Conceitos Básicos

- **LDAP**
 - Protocolo utilizado para atualizar e pesquisar diretórios rodando sobre TCP/IP.
- **Kerberos**
 - Protocolo desenvolvido para fornecer poderosa autenticação em aplicações usuário/servidor
- **PAM**
 - Conjunto de bibliotecas usadas para fazer autenticação, gerenciamento de contas, controle de recursos dos usuários no sistema.

Solução

- Configurando o Postfix (SMTP)
 - LDAP
 - /etc/postfix/ldap-users.cf

server_host = 10.x.x.x

search_base = dc=acme,dc=local

version = 3

query_filter = (&(objectclass=person)(mail=%s))

result_attribute = sAMAccountName

result_format = %s/Maildir/

bind = yes

bind_dn = postfix@acme.local

bind_pw = postfix

Solução

- Configurando o Postfix (SMTP)

- Postfix

- /etc/postfix/main.cf

`virtual_mailbox_domains = lion.acme.local`

`virtual_mailbox_base = /home/vmail/`

`virtual_mailbox_maps = ldap:/etc/postfix/ldap-users.cf`

`virtual_uid_maps = static:507`

`virtual_gid_maps = static:507`

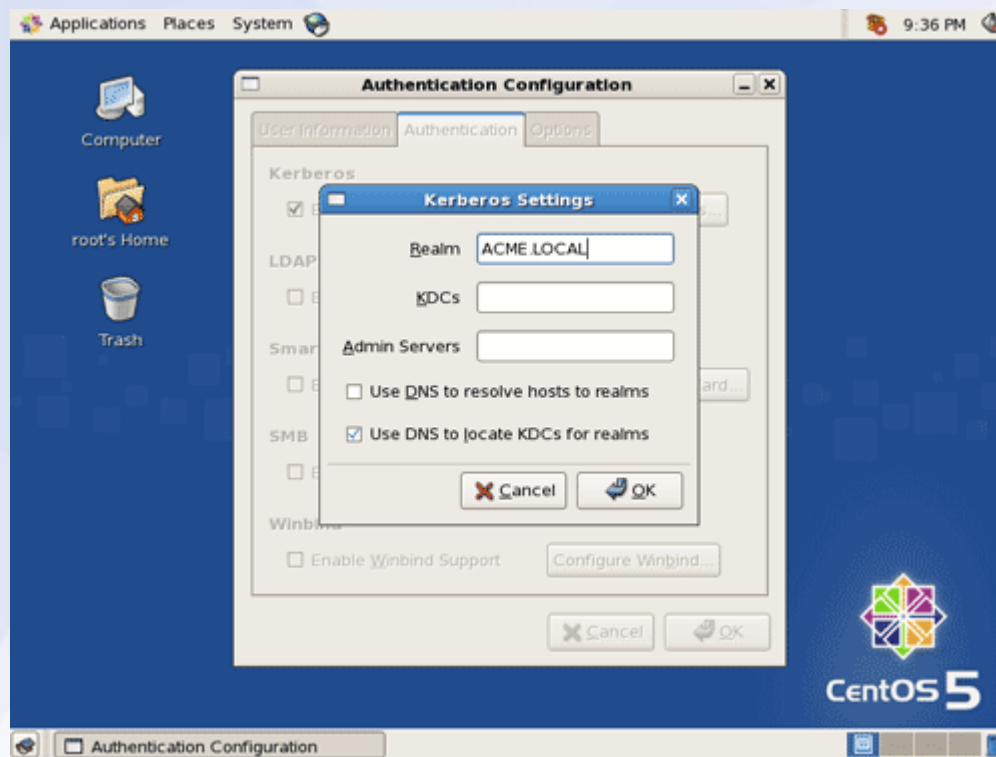
`append_at_myorigin = no`

- Testando:

- `postmap -q bugsbunny@acme.local ldap:/etc/postfix/ldap-users.cf1`

Solução

- Configurando o Dovecot (Imap e Pop3)
 - Kerberos
 - Authconfig



Solução

- Configurando o Dovecot (Imap e Pop3)
 - Kerberos

- /etc/pam.d/dovecot

```
auth sufficient pam_krb5.so no_user_check validate
```

```
account sufficient pam_permit.so
```

- /etc/dovecot.conf

```
passdb pam {
```

```
}
```

```
userdb static {
```

```
args = uid=501 gid=501 home=/home/vmail/%Lu
```

```
}
```

Conclusão

- **Está solução mostrou-se:**
 - **Robusta;**
 - **Permitindo alta disponibilidade;**
 - **Completa;**
 - **Fácil de manter e gerenciar**

Dúvidas????

Contatos

- Email:
 - alexos@ngsecurity.com.br
 - penguim@ubuntu.com
- Site:
 - <http://penguim.wordpress.com>