Configurando O Samba Como Um Controlador De Domínio Do Active Directory

...

A partir da versão 4.0, o Samba pode ser executado como um controlador de domínio do Active Directory (AD) (DC). Se você estiver instalando o Samba em um ambiente de produção, recomenda-se que execute dois ou mais DCs por motivos de failover.

Checklist

- Preparar o ambiente
- Provisionar
- Modo Interativo
- Modo não interativo
- Configurar resolução de Nomes
- Configurar Kerberos
- Verificar DNS
- Verificar Kerberos
- Testar o Samba AD

Preparando o ambiente

- Selecione um nome de host para o AD DC.
- Não use termos NT4 como nome do host, como PDC ou BDC. Esses modos não existem em um AD e causam confusão.
- Selecione um domínio DNS para sua floresta AD. O nome também será usado como o domínio do AD Kerberos.
- Use um endereço IP estático na DC.
- Desative ferramentas, como `resolvconf`, que atualizem automaticamente seu /etc/resolv.conf

- Verifique se nenhum processo do Samba está sendo executado:

```
ps ax | egrep "samba|smbd|nmbd|winbindd"
```

- Verifique se o arquivo /etc/hosts no DC resolve corretamente o nome de domínio totalmente qualificado (FQDN) e o nome do host curto para o endereço IP da LAN do DC. Por exemplo:

```
127.0.0.1       localhost localhost.localdomain

192.168.0.1     DC1.seudominio.lan      DC1
```

- O nome do host e FQDN não devem ser resolvidos para o endereço IP `127.0.0.1` ou qualquer outro endereço IP do que o usado na interface LAN do DC.

- Se você executou anteriormente uma instalação do Samba neste host, Remova o arquivo smb.conf existente . Para listar o caminho para o arquivo execute :

```
smbd -b | grep "CONFIGFILE"
```

(saida) `CONFIGFILE: /usr/local/samba/etc/samba/smb.conf`

- Remova todos os arquivos de banco de dados do Samba, como `*.tdbe` `*.ldb`. Para listar as pastas que contêm bases de dados do Samba execute:

```
smbd -b | egrep "LOCKDIR|STATEDIR|CACHEDIR|PRIVATE_DIR"
```

Remova o /etc/krb5.conf existente execute :

```
rm /etc/krb5.conf
```

Provisionando um Samba Active Directory

- O processo de provisionamento AD do Samba executa 3 tarefas:
    - Cria os bancos de dados AD
    - Adiciona registros iniciais, como a conta de administrador do domínio
    - adiciona Entradas DNS necessárias.

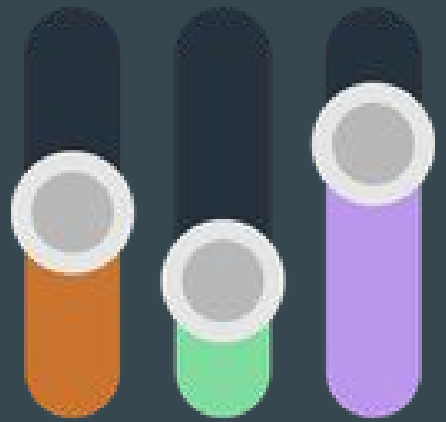
O provisionamento do AD requer permissões de root para criar arquivos e definir permissões.

samba-tool domain provision

- O comando `samba-tool domain provision` fornece vários parâmetros .
- Pode trabalhar no modo interativo e não interativo.

Para detalhes, execute :

```
samba-tool domain provision --help
```



parâmetros do comando

Configuração do modo interativo	Parâmetro do modo não interativo	Explicação
`--use-rfc2307`	`--use-rfc2307`	Permite as extensões NIS.
`Realm`	`--realm`	Reino de Kerberos. Isso também é usado como o domínio do DNS AD. Por exemplo: samba4.tux.
`Server Role`	`--server-role`	Instala a DCfunção de controlador de domínio .
`DNS backend`	`--dns-backend`	Define o back end do DNS. O primeiro DC em um AD deve ser instalado usando um back end de DNS.

Configuração do modo interativo	Parâmetro do modo não interativo	Explicação
`DNS forwarder IP address`	`não disponível`	Esta configuração só está disponível quando se usa o SAMBA_INTERNALback end do DNS.
`Administrator password`	`--adminpass`	Define a senha do administrador do domínio. Se a senha não corresponder aos requisitos de complexidade, o provisionamento falhará. Para obter detalhes
`Não disponível`	`--function-level`	Define o nível funcional

Exemplos interativo e Não Interativo

- Modo Interativo

```
samba-tool domain provision --use-rfc2307 --interactive
```

- Modo NÃO Interativo

```
samba-tool domain provision --server-role=dc --use-rfc2307
--dns-backend=SAMBA_INTERNAL --realm=SUAEMPRESA.COM
--domain=SUAEMPRESA --adminpass=Passw0rd
```

Configurar Resolução de Nomes

- Os membros do domínio em um AD usam DNS para localizar serviços, como LDAP e Kerberos.
- Para isso, eles precisam usar um servidor de DNS que seja capaz de resolver a zona do DNS AD.
- Você precisa configurar o arquivo /etc/resolv.conf no DC como abaixo :

```
domain suaempresa.com

nameserver 127.0.0.1
```

Configurar Kerberos

- Em um AD, o Kerberos é usado para autenticar usuários, máquinas e serviços.
- Durante o provisionamento, o Samba cria um arquivo de configuração Kerberos para o seu DC.
- A configuração Kerberos pré-criada usa registros de recursos do serviço DNS (SRV) para localizar o KDC.
- Para usar, crie um link simbólico para a configuração Kerberos pré-configurada:

```
ln -sf /usr/local/samba/private/krb5.conf /etc/krb5.conf
```

Testando o Samba AD

- Para iniciar o serviço samba manualmente, use o comando:

```
/caminho/do/executável/samba
```

- Teste os compartilhamentos padrão (sysvol e netlogon)

```
smbclient -L localhost -U%
```

- Testar autenticação, conecte-se ao compartilhamento netlogon como administrador do domínio:

```
smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

- Verificar registro SRV `_ldap` baseado em tcp no domínio:

```
host -t SRV _ldap._tcp.samdom.example.com.
```

```
_ldap._tcp.samdom.example.com has SRV record 0 100 389
dc1.samdom.example.com.
```

- Verificar registro SRV `_kerberos` no domínio:

```
host -t SRV _kerberos._udp.samdom.example.com.
```

```
_kerberos._udp.samdom.example.com has SRV record 0 100 88
dc1.samdom.example.com.
```

- Verificar registro A do controlador de domínio:

```
host -t A dc1.samdom.example.com.
```

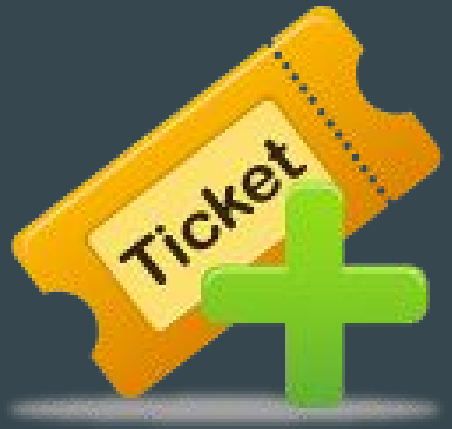
```
dc1.samdom.example.com has address 10.99.0.1
```

Testando ticket kerberos (TGT)

- O Kerberos trabalha baseado em Tickets, que identificam os usuários.
- Para testar se o kerberos está emitindo tickets execute :

```
kinit administrator
```

```
Password for administrator@SAMDOM.EXAMPLE.COM:
```



- O domínio Kerberos é anexado automaticamente, se você não passar no formato user@REALM para o comando kinit.
- Defina realm Kerberos sempre em maiúscula.
- Para listar os tickets em cache execute :

```
klist
```

```
Ticket cache: FILE:/tmp/krb5cc_0

Default principal: administrator@SAMDOM.EXAMPLE.COM

Valid starting       Expires              Service principal

01.11.2016 08:45:00  12.11.2016 18:45:00  krbtgt/SAMDOM.EXAMPLE.COM@SAMDOM.EXAMPLE.COM

      renew until 02.11.2016 08:44:59
```

Links úteis

...

Mais informações

- Documentação oficial - https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller