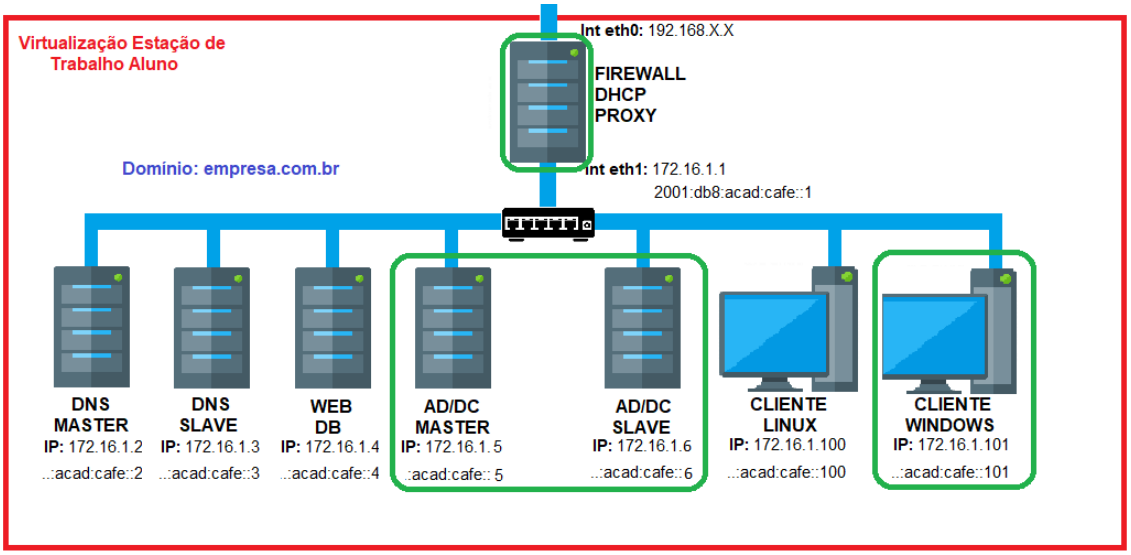
6.18 Adicionando um Controlador de Domínio Samba4 secundário

Neste laboratório, será provisionando um segundo AD/DC com Samba4, a fim de tornar o referido serviço redundante. Para isso, serão utilizadas as seguintes Máquinas Virtuais:

- Appl-Debian10-Firewall - Firewall, DHCP e Compartilhamento da internet para rede interna
- Appl-Debian10-SMB4 - Servidor AD/DC
- Appl-Debian10-SMB4-Slave - Servidor AD/DC Slave
- Appl-Windows7-Client - Testes e administração do AD/DC



6.18.1 Ajustes iniciais

Teste a conexão com o servidor Samba4 a partir do servidor Samba4-slave. O endereço IP do servidor Samba4-slave deve estar configurado com IP 172.16.1.6 (já configurado da VM disponibilizada pelo Professor):

```
root@samba4-slave:/# ip addr list
root@samba4-slave:/# ping 172.16.1.5
```

Verifique se o resolver da máquina virtual Samba4-slave está apontado para o servidor Samba4:

```
root@samba4-slave:/# vim /etc/resolv.conf
```

```
domain empresa.com.br
search empresa.com.br
nameserver 172.16.1.5
```

Verifique a partir da máquina virtual samba4-slave se o nome **samba4.empresax.com.br** está resolvendo:

```
root@samba4-slave:~# host -t A samba4.empresax.com.br
samba4.empresax.com.br has address 172.16.1.5
root@samba4-slave:~#
```

Outro ponto importante é certificar que nos dois servidores foram instaladas a mesma versão do Samba4, para isso, basta executar o comando "samba -V" em ambos os servidores como nos exemplos abaixo:

```
root@samba4:~# samba -V
Version 4.14.4
root@samba4:~#
```

```
root@samba4-slave:~# samba -V
Version 4.14.4
root@samba4-slave:~#
```

A VM Appl-Debian10-SMB4-Slave, disponibilizada pelo professor, já possui o samba4 instalado, em caso de divergência entre versões, consulte o professor quanto a possibilidade de incompatibilidade ou não do serviço.

6.18.2 Promovendo o samba como controlador de domínio

Realizado os ajustes iniciais, agora é possível promover o Samba4 como controlador de domínio secundário, para isso é necessário realizar a instalação do Samba. Na máquina virtual Samba4-slave o samba já encontra-se instalado, necessitando apenas executar o provisionamento com o comando a seguir:

```
root@samba4-slave:/# samba-tool domain join empresax.com.br DC
-U"EMPRESAX\administrator" --dns-backend=SAMBA_INTERNAL
```

No comando executado definimos que a máquina Samba4-slave ingressará no domínio **empresax.com.br** e que o usuário administrador do domínio é o usuário **Administrator**. Por fim, é indicado que será utilizado o DNS interno do Samba4.

Durante o processo de ingresso no domínio, será solicitada a senha do usuário Administrator.

Após o ingresso no domínio **empresax.com.br**, será necessário verificar se o servidor primário já consegue resolver o nome do servidor secundário samba4-slave.empresax.com.br.

```
root@samba4-slave:~# host -t A samba4-slave.empresax.com.br
samba4-slave.empresax.com.br has address 172.16.1.6
root@samba4-slave:~#
```

Também podemos testar se o ObjectGUID (atributo de identificação) está resolvendo com o comando a seguir:

```
root@samba4-Slave:/# ldbsearch -H /usr/local/samba/private/sam.ldb '(invocationid= * )'
--cross-ncs objectguid
```

Na resposta do comando deverá retornar o ObjectGUID dos dois servidores associados: record 1 (servidor primário) e record 2 (servidor secundário).

```
root@samba4-slave:~# host -t A samba4-slave.empresax.com.br
samba4-slave.empresax.com.br has address 172.16.1.6
root@samba4-slave:~# ldbsearch -H /usr/local/samba/private/sam.ldb '(invocationid= * )' --cross-ncs objectguid
# record 1
dn: CN=NTDS Settings,CN=SAMBA4-SLAVE,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=empresax,DC=com,DC=br
objectGUID: 94b559b1-b800-42c4-aa7d-1cff22ee71e2

# record 2
dn: CN=NTDS Settings,CN=SAMBA4,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=empresax,DC=com,DC=br
objectGUID: 8d49bbfc-5b51-407f-bb09-c5940f1a30ac

# returned 2 records
# 2 entries
# 0 referrals
```

Observe o ObjectGUID do servidor secundário (record 2) e teste a resolução de nome, para isso utilize o comando a seguir, substituindo o ID (em vermelho) pelo ID retornado pelo comando.

> ***root@samba4-Slave:/#host -t CNAME id._msdcs.empresax.com.br***

A resposta deverá ser parecida a apresentada na figura abaixo:

```
root@samba4-slave:~# host -t CNAME 8d49bbfc-5b51-407f-bb09-c5940f1a30ac._msdcs.empresax.com.br
8d49bbfc-5b51-407f-bb09-c5940f1a30ac._msdcs.empresax.com.br is an alias for samba4.empresax.com.br.
root@samba4-slave:~#
```

6.18.3 Configuração do Kerberos

Reinicie o serviço Samba4. É importante destacar que na máquina virtual disponibilizada o script Samba4 já está configurado.

> ***root@samba4-Slave:/#systemctl restart samba4***
> ***root@samba4-Slave:/#systemctl status samba4***

O Kerberos do controlador de domínio secundário deverá ser ajustado igualmente ao kerberos do controlador primário (configurado no primeiro laboratório). Para tornar a configuração mais simples, copiaremos com o utilitário SCP do OpensSSH Server o arquivo krb5.conf da máquina Samba4 para a Samba4-slave.

> ***root@samba4-slave:/# scp aluno@172.16.1.5:/etc/krb5.conf /etc/***

Agora inicialize um ticket do kerberos para o usuário administrator, a senha utilizada será a mesma que definimos anteriormente no controlador primário: (Pa$$w0rd).

> ***root@samba4-Slave:/# kinit administrator***

```
root@samba4-slave:~# kinit administrator
Password for administrator@EMPRESAX.COM.BR:
Warning: Your password will expire in 36 days on sáb 10 jul 2021 11:25:54 -03
root@samba4-slave:~#
```

Liste o ticket criado:

> ***root@samba4-Slave:/# klist***

```
root@samba4-slave:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@EMPRESAX.COM.BR

Valid starting       Expires              Service principal
03/06/2021 21:58:00  04/06/2021 07:58:00  krbtgt/EMPRESAX.COM.BR@EMPRESAX.COM.BR
        renew until 04/06/2021 21:57:55
root@samba4-slave:~#
```

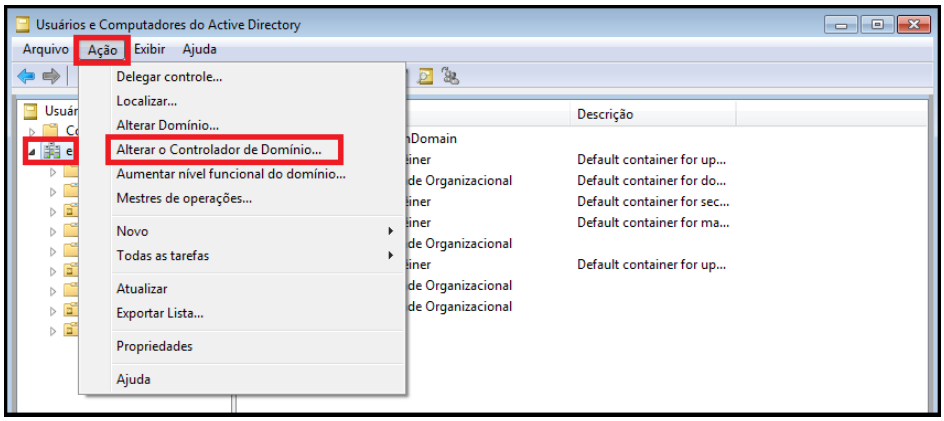
Agora será testada a replicação para no controlador de domínio secundário. Sempre que realizada qualquer alteração em um dos controladores o mesmo deve refletir sobre o outro controlador. Para verificar isto basta usar o comando a baixo:

> ***root@samba4-Slave:/# samba-tool drs showrepl***

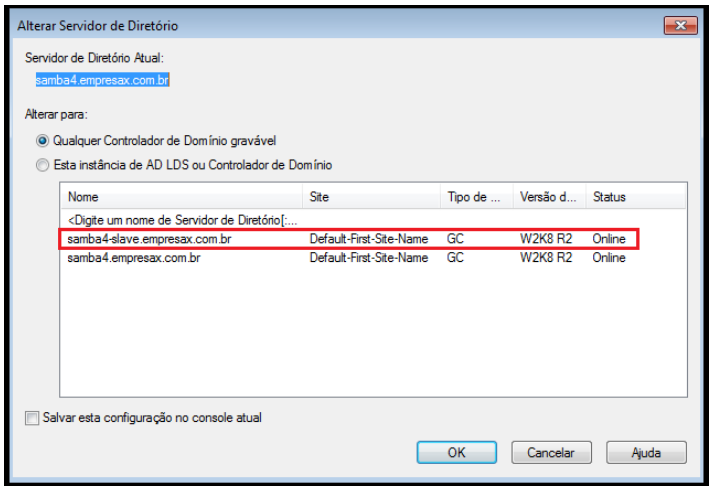
```
root@samba4-slave:~# samba-tool drs showrepl
Default-First-Site-Name\SAMBA4-SLAVE
DSA Options: 0x00000001
DSA object GUID: 94b559b1-b800-42c4-aa7d-1cff22ee71e2
DSA invocationId: f163ed4a-d047-4e00-904e-d8f0814c6cf3

==== INBOUND NEIGHBORS ====

DC=ForestDnsZones,DC=empresax,DC=com,DC=br
        Default-First-Site-Name\SAMBA4 via RPC
                DSA object GUID: 8d49bbfc-5b51-407f-bb09-c5940f1a30ac
                Last attempt @ Thu Jun  3 22:03:21 2021 -03 was successful
                0 consecutive failure(s).
                Last success @ Thu Jun  3 22:03:21 2021 -03

DC=DomainDnsZones,DC=empresax,DC=com,DC=br
        Default-First-Site-Name\SAMBA4 via RPC
                DSA object GUID: 8d49bbfc-5b51-407f-bb09-c5940f1a30ac
                Last attempt @ Thu Jun  3 22:03:21 2021 -03 was successful
                0 consecutive failure(s).
                Last success @ Thu Jun  3 22:03:21 2021 -03

CN=Schema,CN=Configuration,DC=empresax,DC=com,DC=br
        Default-First-Site-Name\SAMBA4 via RPC
                DSA object GUID: 8d49bbfc-5b51-407f-bb09-c5940f1a30ac
                Last attempt @ Thu Jun  3 22:03:21 2021 -03 was successful
                0 consecutive failure(s).
                Last success @ Thu Jun  3 22:03:21 2021 -03

DC=empresax,DC=com,DC=br
        Default-First-Site-Name\SAMBA4 via RPC
                DSA object GUID: 8d49bbfc-5b51-407f-bb09-c5940f1a30ac
                Last attempt @ Thu Jun  3 22:03:21 2021 -03 was successful
                0 consecutive failure(s).
                Last success @ Thu Jun  3 22:03:21 2021 -03

CN=Configuration,DC=empresax,DC=com,DC=br
        Default-First-Site-Name\SAMBA4 via RPC
                DSA object GUID: 8d49bbfc-5b51-407f-bb09-c5940f1a30ac
                Last attempt @ Thu Jun  3 22:03:21 2021 -03 was successful
                0 consecutive failure(s).
                Last success @ Thu Jun  3 22:03:21 2021 -03
```

6.18.4 Gerenciando o servidor secundário a partir do RSAT

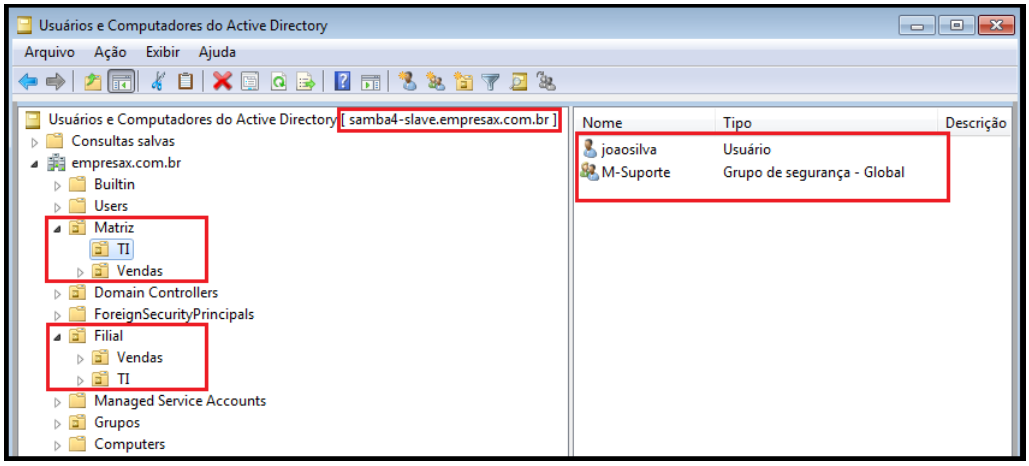
Na máquina virtual Windows, caso você deseje gerenciar o servidor secundário a partir do RSAT, abra o Console de gerenciamento do Active Directory, selecione o domínio "empresax.com.br", clique em "Ação" e selecione "Alterar controlador de domínio" como apresentado na figura abaixo:



Na janela "Alterar Servidor de Diretório Atual" deverão aparecer os dois servidores e apresentar para ambos o status "Online", para gerenciar qualquer um dos dois, basta clicar no escolhido e posteriormente em "OK".



Observe que as Unidades Organizacionais, Usuários e Grupos foram replicados para o Controlador de Domínio Slave:



Para testar a replicação entre servidores, selecione o controlador de domínio "samba4-slave" e crie um novo usuário em uma das Unidades Organizacionais criadas no Active Directory do Samba4.

Para verificar a replicação, altere novamente o gerenciamento para o servidor "samba4" e verifique se o usuário criado replicou corretamente.

6.18.5 Teste de replicação LDAP via CLI

A ferramenta Samba-tool fornece um subcomando para testar a replicação do LDAP entre os controladores de domínio, independentemente de estarem executando o Samba ou Windows.

Para comparar todo o diretório no Controlador de Domínio Secundário com o Primário, execute o seguinte comando:

```
#samba-tool ldapcmp ldap://samba4.empresax.com.br ldap://localhost -Uadministrator
```

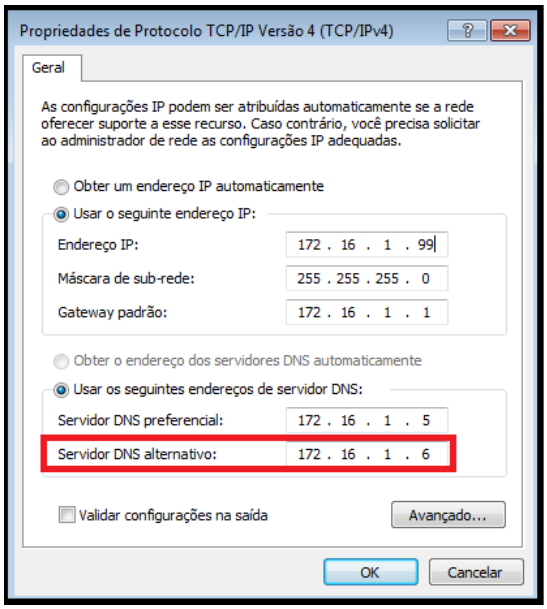
É possível ainda comparar partes dos diretórios entre os controladores de domínio:

```
#samba-tool ldapcmp ldap://samba4.empresax.com.br ldap://localhost -Uadministrator domain

#samba-tool ldapcmp ldap://samba4.empresax.com.br ldap://localhost -Uadministrator configuration

#samba-tool ldapcmp ldap://samba4.empresax.com.br ldap://localhost -Uadministrator schema

#samba-tool ldapcmp ldap://samba4.empresax.com.br ldap://localhost -Uadministrator dnsdomain

#samba-tool ldapcmp ldap://samba4.empresax.com.br ldap://localhost -Uadministrator dnsforest
```

6.18.6 Teste de Redundância

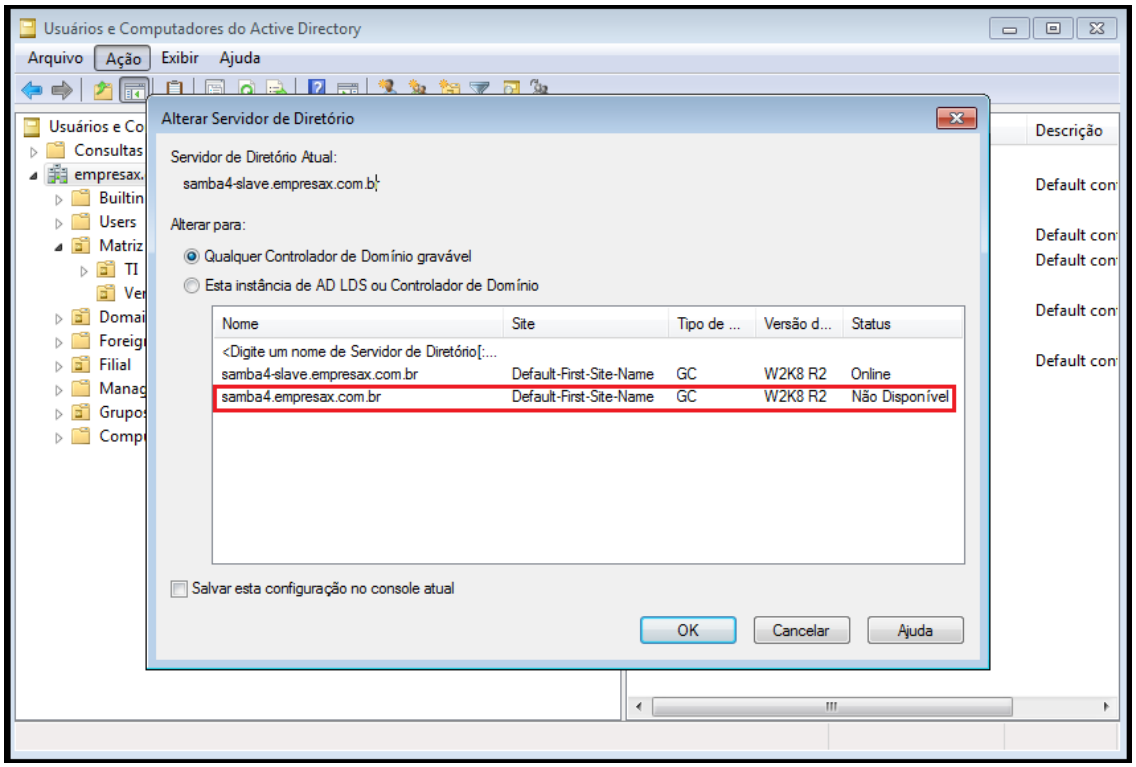
Quando o Controlador de Domínio principal não estiver disponível, seja por problemas de conectividade ou de funcionamento, uma das funções do Controlador de Domínio Slave é responder para que o serviço não fique indisponível.

Para testar a redundância do serviço, vá até as configurações de rede da estação de trabalho Windows e configure a opção "Servidor DNS alternativo" para o IP do servidor samba4-slave (172.16.1.6):



Agora, desligue o Controlador de Domínio principal (samba4) e reinicie a estação de trabalho Windows. Após a inicialização do Windows, autentique com o usuário Administrator, a fim de certificar o funcionamento do controlador de domínio secundário.

Autenticado no sistema, abra o Console de gerenciamento do Active Directory (dsa.msc), selecione o domínio "empresax.com.br", clique em "Ação" e selecione "Alterar controlador de domínio". Deverá aparecer o Controlador de Dompinio Principal como "Não disponível" e o secundário como "Online", como apresentado na figura abaixo:



Pronto, o Controlador de Domínio slave está funcionando corretamente e assumindo o controle quando o Controlador Principal está indisponível.

6.18.7 Replicação do Sysvol

O diretório Sysvol contem arquivos públicos do domino que precisam ser acessados pelas máquinas clientes, esse diretório é composto pelos seguintes subdiretórios: Policies: as pastas desse diretório têm como nome GUIDs das políticas de grupos. Por padrão já possui os subdiretórios contendo as Políticas de Domínio Padrão e Políticas de Controladores de Domínio Padrão.

Scripts: por padrão estará vazia, essa é o compartilhamento netlogon na qual pode armazenar scripts que necessitam de replicação para todos os DCs.

O Samba atualmente não suporta replicação Sysvol, em sua documentação pode ser consultadas alternativas para replicação do diretório: https://wiki.samba.org/index.php/SysVol_replication_(DFS-R).