Controlador de Domínio Adicional Samba 4

...

Introdução

- Executar um controlador de domínio (DC) é suficiente para uma floresta ativa do Active Directory (AD).
- No entanto, para motivos de failover e balanceamento de carga, você deve adicionar outros DCs à sua floresta do AD.
- Unir um Samba DC adicional a um AD existente é diferente do provisionamento do primeiro DC em uma floresta.

Cenário

- DC Samba 4 > DC Windows Server
- DC Samba 4 > DC Samba 4

Sistemas Windows suportados

- Windows 2003
- Windows 2003 R2
- Windows 2008
- Windows 2008 R2
- Windows 2012 (sem suporte)
- Windows 2016 (sem suporte)

- Um domínio NT4 usa apenas um Controlador de Domínio Primário (PDC) e, opcionalmente, Controladores de Domínio de Backup (BDC) adicionais. Em uma floresta de AD , não há diferença entre DCs, além das *funções de FSMO* .
- Use apenas o termo "controlador de domínio" ou "DC" ao falar sobre o AD para evitar qualquer possibilidade de confusão.

Instalar o Samba

- Nesse passo siga as instruções normais para a instalação do Samba compilado.
- Não faça mais nada do que isso
- Se você tiver um template de máquina virtual com apenas o samba instalado pode ser usado , ou pode também ser usando snapshots

- Depois de Instalar o Samba é necessário preparar o host que será o DC adicional

Servidor DNS local

- Por padrão, o primeiro controlador de domínio (DC) em uma floresta executa um servidor DNS para zonas baseadas no Active Directory (AD).
- Por motivos de failover, é recomendável executar vários DCs atuando como um servidor DNS em uma rede.
- Se você considerar fornecer um serviço DNS no novo DC então:
- Para o BIND9_DLZ back-end, temos que instalar e configurar o bind 9.
- Para o DNS interno, nenhuma ação adicional é necessária.

- O 'nameserver' que você definiu em '/etc/resolv.conf' deve ser um AD DC, caso contrário a junção não poderá encontrar o KDC.

```
nameserver 192.168.1.1
search seudominio.lan
```

Kerberos

- Defina as seguintes configurações no arquivo de configuração do cliente Kerberos /etc/krb5.conf:

```
[libdefaults]
    dns_lookup_realm = false
    dns_lookup_kdc = true
    default_realm = SEUDOMINIO.LAN
```

- Para verificar as configurações, use o comando kinit para solicitar um tíquete do Kerberos para o administrador do domínio:

```
# kinit administrator
Password for administrator@SEUDOMINIO.LAN:
```

- Para listar os tickets do Kerberos:

```
# klist

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SEUDOMINIO.LAN

Valid starting       Expires              Service principal
24.09.2015        19:56:55                25.09.2015        05:56:55
krbtgt/SEUDOMINIO.LAN@SEUDOMINIO.LAN
    renew until 25.09.2015 19:56:53
```

Inserido como controlador de domínio

- Use o comando `samba-tool domain join` para ingressar o DC adicional como no exemplo :

```
samba-tool domain join seudominio.lan DC -U"SEUDOMINIO\administrator" --dns-backend=SAMBA_INTERNAL
```

- Veja a `samba-tool domain join --help` para mais informações.
- Outros parâmetros freqüentemente usados com o comando samba-tool domain join:
- `--site=SITE:` Escolha o site que o DC será ingressado .
- `--option="interfaces=lo eth0" --option="bind interfaces only=yes"` : Se o servidor tem várias interfaces de rede

Pulo do gato I

- Se os outros controladores de domínio são Samba DC e foram provisionados com `--use-rfc2307`, você deve adicionar `--option='idmap_ldb:use rfc2307 = yes'` ao comando.

Verificando as entradas de DNS

- Se estiver usando Samba DC que executa o Samba 4.7 e posterior, samba-tool cria todas as entradas de DNS necessárias automaticamente quando o backend DNS é Internal .
- Caso esteja usando BIND9_DLZ configurações adicionais de DNS terão que de serem feitas.

Mapeamentos internos de IDs de grupos e usuários

- Atualmente, a replicação de SYSVOL não é suportada no Samba.
- Para usar uma solução alternativa de Replicação Sysvol , todos os controladores de domínio (DC) devem usar os mesmos mapeamentos de ID para usuários e grupos internos.
- Por padrão, um Samba DC armazena os IDs de usuário e grupo nos atributos 'xidNumber' em 'idmap.ldb'.
- Por causa da maneira como o 'idmap.ldb' funciona, você não pode garantir que cada DC use o mesmo ID para um determinado usuário ou grupo.

- Crie um hot-backup do arquivo /opt/samba/private/idmap.ldb no DC existente:

```
tdbbackup -s .bak /usr/local/samba/private/idmap.ldb
```

Isso cria um arquivo de backup /opt/samba/private/idmap.ldb.bak.

- Mova o arquivo de backup para a pasta /opt/samba/private/ no novo DC adicional e remova o sufixo .bak para substituir o arquivo existente.
- Redefinir as listas de controle de acesso (ACL) do sistema de arquivos da pasta Sysvol no novo DC:

```
samba-tool ntacl sysvolreset
```

Configure o Samba no boot e inicie o Samba

- Configure o `systemd` para que gerencie o serviço samba e o inicie com o comando:

```
systemctl start samba-ad-dc
```

Verificando a replicação de diretório

- Depois que o controlador de domínio (DC) foi iniciado, o `knowledge consistency checker` (KCC) no DC do Samba cria acordos de replicação para outros DCs na floresta do Active Directory (AD). Pode levar até 15 minutos até que o KCC crie as conexões de replicação geradas automaticamente.
- A replicação de diretório é importante em uma floresta do Active Directory (AD) com vários controladores de domínio (DC) para failover e balanceamento de carga.

- Para os acordos de replicação que os KCCs criam automaticamente, os seguintes contêineres são replicados por padrão:

```
DC=Forest_Root_Domain

CN=Configuration,DC=Forest_Root_Domain

CN=Schema,CN=Configuration,DC=Forest_Root_Domain

DC=ForestDnsZones,DC=Forest_Root_Domain

DC=DomainDnsZones,DC=Forest_Root_Domain
```

- Exibindo os Status de Replicação em um Samba DC , o comando abaixo exibe os acordos de replicação de entrada e saída com outro controlador de domínio na floresta do AD. **A saída é relatada do ponto de vista do DC do Samba, no qual você executa o comando.**

```
samba-tool drs showrepl
```

Exibindo os status de replicação em um DC do Windows

- Replicação de entrada ,Para exibir a replicação de entrada em um DC do Windows:
- Abra um prompt de comando.
- Use o utilitário `repadmin` para exibir os status de conexão de entrada:

```
repadmin /showrepl
```

Pulo do gato 2

- O que `Warning: No NC replicated for Connection !` significa?

Ao executar o comando `samba-tool drs showrepl`, o seguinte aviso é exibido no final da saída:

`Warning: No NC replicated for Connection!`

O aviso aparece porque o Samba define incorretamente alguns sinalizadores ao registrar o controlador de domínio para replicação. **O aviso é inofensivo e pode ser ignorado.**

Verificar os compartilhamentos

- Listar todos os compartilhamentos fornecidos pelo DC:

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

- Os compartilhamentos netlogon e os sysvol foram criados automaticamente durante o provisionamento e devem existir em um DC.
- Para verificar a autenticação, conecte-se ao compartilhamento netlogon usando a conta de administrador do domínio:

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

Testando o servidor DNS local

- Consultar o servidor DNS local para resolver o nome do domínio `minhaempresa.lan`

```
host -t A minhaempresa.lan localhost
```

- O DNS local resolve o nome de domínio para os endereços IP de todos os controladores de domínio (DC).
- Caso você receba nenhum ou um resultado diferente, revise os passos e verifique:
- os arquivos de log do sistema,
- os arquivos de log do Samba,
- os arquivos de log do BIND, se o BIND9_DLZ for usado.

Verificando o Kerberos

- Solicite um tíquete Kerberos para a conta de administrador do domínio:

```
$ kinit administrator
Password for administrator@SEUDOMINIO.LAN:
```

- Listar os tickets do Kerberos em cache:

```
klist
```

Configuração de DNS em controladores de domínio

- A configuração do DNS em controladores de domínio (DC) é importante, porque se não conseguir localizar outros DCs, a replicação falhará.
- Defina o IP local do DC como o servidor de nomes principal.
- Por exemplo:
- No novo DC, use o IP local 10.99.0.2como entrada nameserver principal :

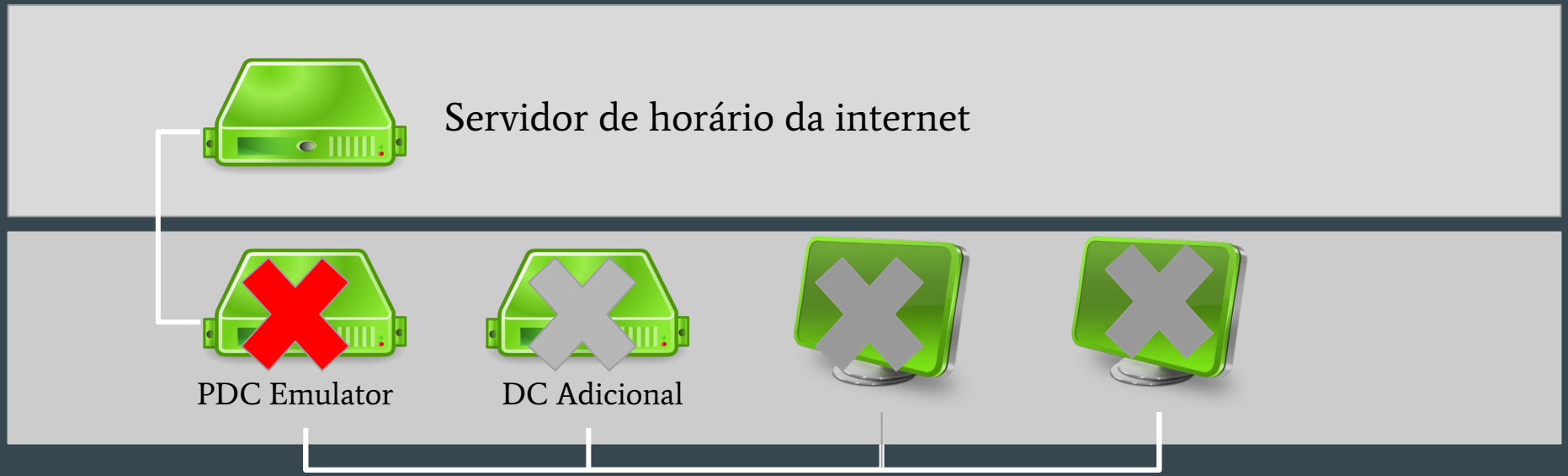
```
nameserver 10.99.0.2
nameserver 10.99.0.1
search seudominio.lan
```

Configurando a Sincronização de Horário

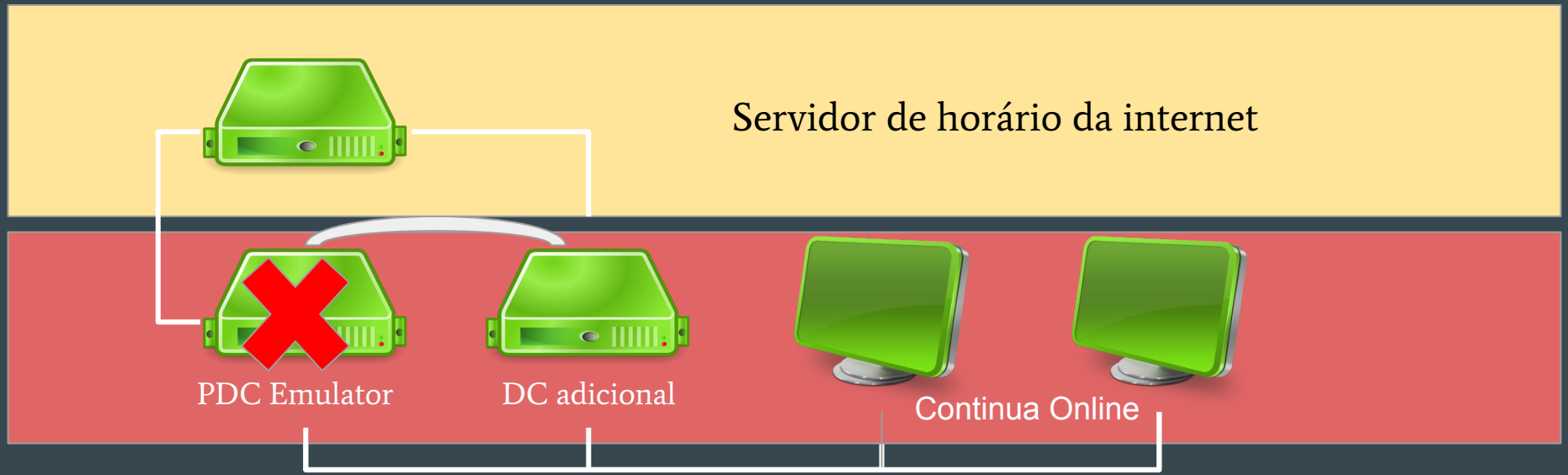
- O Kerberos requer um tempo sincronizado em todos os membros do domínio.
- Em um Active Directory (AD), você deve ter uma sincronização de tempo precisa.
- Por exemplo, o Kerberos requer carimbos de hora corretos para evitar ataques de repetição e o AD usa o tempo para resolver conflitos de replicação.
- O desvio de tempo máximo permitido padrão em um AD é de 5 minutos.
- Se um membro de domínio ou controlador de domínio (DC) tiver uma diferença de horário maior ou menor, o acesso será negado.
- Como resultado, um usuário não pode acessar compartilhamentos ou consultar o diretório.

- O Samba suporta a ntpd, o daemon sincroniza o horário com origens externas e permite que os clientes recuperem o horário do servidor que está executando o daemon.

Cenário a observar



Prática recomendada recomendada



Configurando a Sincronização de Horário

- Siga esses passos para configurar o servidor NTP de hora - http://astreinamentos.com.br/samba2.0/servidor-ntp.txt
- Se você estiver executando o controlador de domínio em uma VM, considere adicionar `tinker panic 0` ao final do ntp.conf.
- Isso diz ao NTP para não entrar em pânico e sair, não importa qual seja o deslocamento de tempo. Isso é recomendado porque as máquinas virtuais não têm relógio físico e podem ser pausadas a qualquer momento e iniciar horas mais tarde.

Pulo do Gato 3

- Os membros do domínio do Windows AD usarão qualquer DC como fonte de tempo padrão geralmente não é necessário reconfigurar os clientes.
- Para obter mais informações sobre a sincronização de horário e a hierarquia em um AD, consulte http://technet.microsoft.com/pt-br/library/cc773013%28v=ws.10%29.aspx#w2k3tr_times_how_izcr .
- Mas também pode ser configuradas via GPO - http://www.sysadminlab.net/windows/configuring-ntp-on-windows-using-gpo

Replicação da pasta sysvol

- Atualmente, o Samba não suporta replicação Sysvol.
- Se houver mais do que os GPOs padrão no Sysvol no outro DC (s), você deve sincronizar Sysvol para o novo controlador de domínio, `samba-tool ntacl sysvolreset` lançará um erro se você não o fizer.
- Você pode usar 4 alternativas para tal
- Baseada em **Rsync** Unidirecional (apenas DCs do Samba): Característica : Configuração rápida, fácil de configurar.
- Baseada em **Rsync / Unison** bidirecional (somente DCs do Samba): **Característica:** Mais complexa, requer script de terceiros, cada DC requer um cron job uns contra os outros.

- Baseada em **Rsync / osync** bidirecional (somente DCs do Samba): Característica: Mais complexa, requer script de terceiros, cada DC requer um cron job uns contra os outros.
- Baseada em Robocopy unidirecional (DCs do Windows -> DC Samba): **Característica**: Configuração rápida, fácil de configurar, usa MS robocopy

Testando a replicação

- Para testar se a replicação de diretório funciona corretamente, adicione, por exemplo, um usuário em um DC existente e verifique se ele aparece automaticamente no DC recém adicionado.
- Opcionalmente, use o utilitário `ldapcmp` para comparar dois diretórios.

Prática

...