

Cenários de FSMO do Active Directory e Global Catalog

Este artigo tem por objetivo não só promover uma explicação sobre as FSMO (Flexible Single-Master Operations) e Global Catalog do Active Directory, mas também centralizar informações diversas obtidas através de pesquisas em artigos e materiais oficiais da Microsoft, demonstrando através de cenários as recomendações realizadas sobre o assunto.

Introdução

No Windows NT 4.0 havia o conceito de PDC (Primary Domain Controller) que era responsável por processar e disponibilizar todas as informações do domínio e também existia o chamado BDC (Backup Domain Controller) que possuía uma cópia de leitura das informações do domínio. Este modelo era também conhecido por 'Single-Master'. Quando ocorria algum problema com o PDC havia necessidade de se promover manualmente algum dos BDC para a função do PDC.

A partir do Windows 2000, surgiu o conceito de 'Multi-Master', pois todos os controladores de domínio passaram a armazenar uma cópia do diretório ativo que pode ser modificada. O gerenciamento destas alterações passou a ser mais complexo, exigindo controles especiais para tratar os possíveis conflitos. Um exemplo de conflito seria a alteração de senha por um usuário enquanto um administrador excluiria este usuário. Para prevenir que ocorram problemas em função de alterações como essa foram criadas as regras do FSMO (Flexible Single-Master Operations). Para mudanças como essas, um controlador de domínio chamado de Mestre de Operações irá centralizar e processar as atualizações. Esta operação, realizada com base de modelo single-master irá prevenir os possíveis conflitos de atualizações na base do AD.

FSMO

Existem cinco FSMO, duas exclusivas para a floresta e três para o domínio, conforme abaixo:

Floresta

- ❖ Schema Master: Controla todas as atualizações no SCHEMA que contém a lista máster de classes de objetos e atributos que são usados para a criação de objetos como usuários, impressoras e etc.
- ❖ Domain Naming Master: Esta regra é responsável por controlar a adição e remoção de domínios na floresta, evitando conflito de nomes.

Domínio

- ❖ PDC Emulator: Atua como um PDC de Windows NT 4.0 para suportar todos os BDCs Windows NT 4.0 quando o domínio está em 'mixed-mode'. Também é responsável por tratar alterações de contas de usuários, "lockouts" de contas, relações de confiança com outros domínios e pelo sincronismo do relógio no domínio.
- ❖ RID Master. Cada objeto deve possuir um identificador único, conhecido como SID. O SID do objeto é construído usando o SID do domínio, mais um ID relativo (RID). O RID

Master aloca blocos de RIDs para cada controlador de domínio que atribui os RIDs aos objetos criados.

- ❖ Infrastructure Master. Quando um objeto é movido de um domínio para outro, o mestre de infra-estrutura atualiza no domínio as referências a objetos que apontam para o objeto em outro domínio. A referência a objetos contém o identificador global exclusivo (GUID, globally unique identifier), o nome distinto e um SID. O Active Directory atualiza o nome distinto e o SID periodicamente na referência do objeto para refletir as alterações feitas ao objeto real, como as movimentações dentro do domínio e entre domínios, além da exclusão do objeto ¹.

Uma forma rápida de se identificar onde estão alocadas as FSMO em sua rede:

```
netdom query fsmo
```

O utilitário 'Netdom.exe' está disponível no "Support Tools" do Windows (CD do Windows - SUPPORT\TOOLS\SUPTOOLS.MSI)

Global Catalog

"Os recursos no Active Directory podem ser compartilhados por domínios e florestas. O recurso GC do Active Directory torna transparente para o usuário a procura de recursos em domínios e florestas. Por exemplo, se você procurar todas as impressoras em uma floresta, um servidor de GC processará a consulta no catálogo global e retornará os resultados. Sem um servidor de catálogo global, seria necessário procurar em cada domínio na floresta" ². O Global Catalog torna possível localizar objetos dos domínios sem a necessidade de conhecer o nome destes domínios.

O Global Catalog é um controlador que possui uma réplica alterável de seu domínio e uma cópia de leitura parcial de todos os demais domínios da floresta.

Em uma floresta com múltiplos domínios o GC é consultado no processo de logon, pois ele é responsável por repassar as informações de grupos universais do usuário para poder permitir ou negar os acessos.

Uma forma rápida de se identificar os servidores com função de Catalogo Global em uma rede:

```
nltest /dsgetdc:corp /GC
```

O utilitário 'nltest' está disponível no "Support Tools" do Windows (CD do Windows - SUPPORT\TOOLS\SUPTOOLS.MSI)

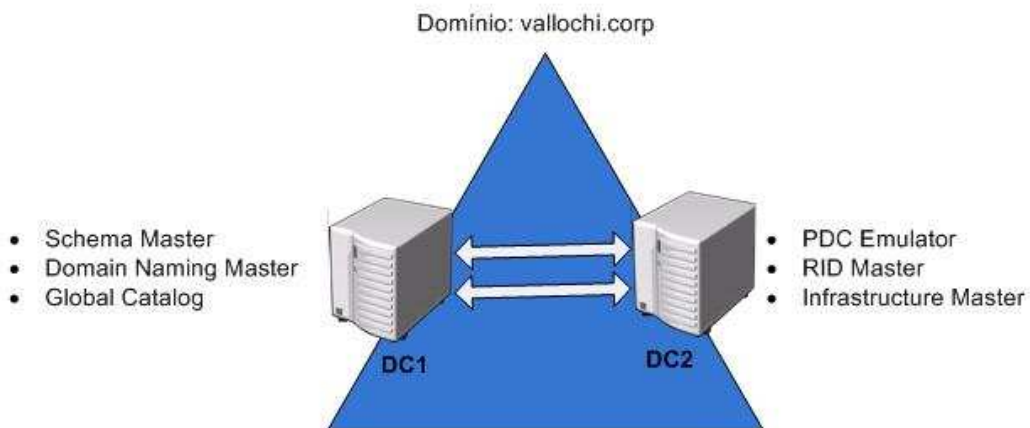
Recomendações

Baseado em algumas recomendações da Microsoft construí alguns cenários para distribuição das Operações Masters na implantação do Active Directory em sua organização.

- ❖ PDC Emulator e RID Master devem estar na mesma máquina, pois o PDC Emulator é grande consumidor de RID's.
- ❖ Infrastructure Master não deve estar em um DC que também é Global Catalog. Isso acontece, pois o Infrastructure Master quando tem algum objeto desatualizado, contata o Global Catalog em busca das informações atuais. Estando no mesmo controlador, ele não tem como saber se as informações na sua base de dados já estão atualizadas ou não, então nunca irá buscar novas atualizações.
- ❖ Para um gerenciamento facilitado, Schema Master e Domain Naming Master podem estar na mesma máquina, que deve ser também um Global Catalog.
- ❖ O Global Catalog desempenha um importante papel em ambientes que utilizam o Microsoft Exchange Server, portanto, é recomendado que ambos estejam na mesma LAN.

Cenários

Cenário 1 – Single-Domain Forest

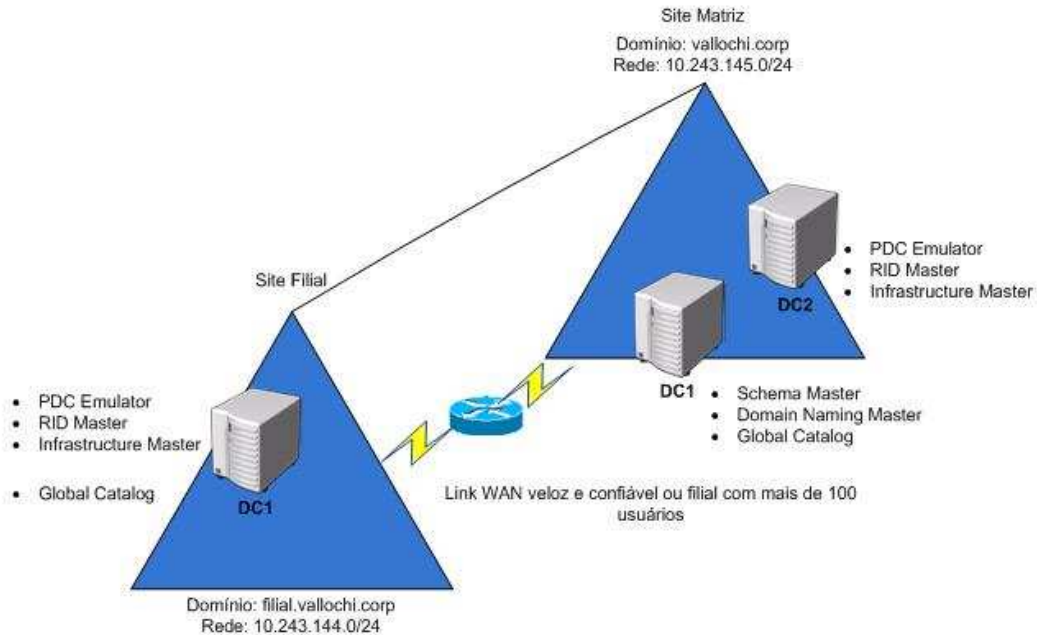


Uma citação importante é que embora o Global Catalog seja automaticamente habilitado no processo de promoção do primeiro controlador de domínio da floresta, neste cenário, ele não é utilizado no logon. Isto ocorre por se tratar de uma Floresta com domínio único, por não haver outros domínios para serem consultados pelo GC e pelos controladores de domínio conhecerem todas as informações de seu próprio domínio.

Conforme citado anteriormente, o Infrastructure Master não pode ser alocado no mesmo controlador que o Catalogo Global, todavia existem algumas exceções:

- ❖ Em uma floresta com um único domínio não existem “phantoms”, por esta razão o Infrastructure Master não tem trabalho a fazer, então será indiferente estar com o Catalogo Global ou não.
- ❖ Em uma Floresta com múltiplos domínios, se todos os controladores de domínio estiverem com o Global Catalog habilitado, não haverá “phantoms” e mais uma vez não haverá trabalho para o Infrastructure Master.

Cenário 2 – Multidomain Forest – Link WAN veloz e confiável

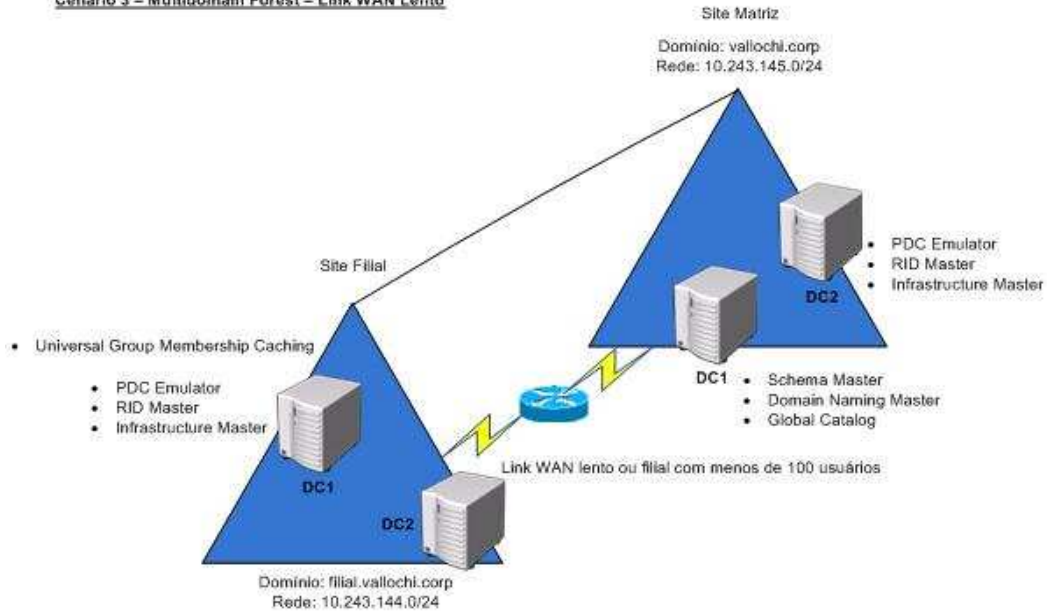


Por se tratar de um link veloz e confiável entre os dois sites apresentados é altamente recomendável a utilização de um Global Catalog na filial para evitar que todo o tráfego de login seja direcionado para a matriz e sobrecarregue o link. Neste caso permaneceria o tráfego de replicação dos controladores de domínio e dos GCs.

Na hipótese de haverem múltiplos sites com múltiplos domínios interligados através de links rápidos, talvez não seja recomendável habilitar um GC em cada localidade por não compensar o tráfego de replicação entre eles. Neste caso o recomendável é uma monitoração e melhor avaliação.

No site Matriz, todas as recomendações para as FSMO puderam ser atendidas, pois as funções foram distribuídas e equilibradas. Já na filial, por haver apenas um servidor controlador de domínio, o Global Catalog teve que ser habilitado com a função de Infrastructure Master, neste caso seria importante modificar a estrutura e tentar copiar a mesma configuração da matriz, tornando-a ideal. Ideal também pelo fato de gerar redundância para o domínio filial.vallochi.corp que no exemplo acima não há.

Cenário 3 – Multidomain Forest – Link WAN Lento



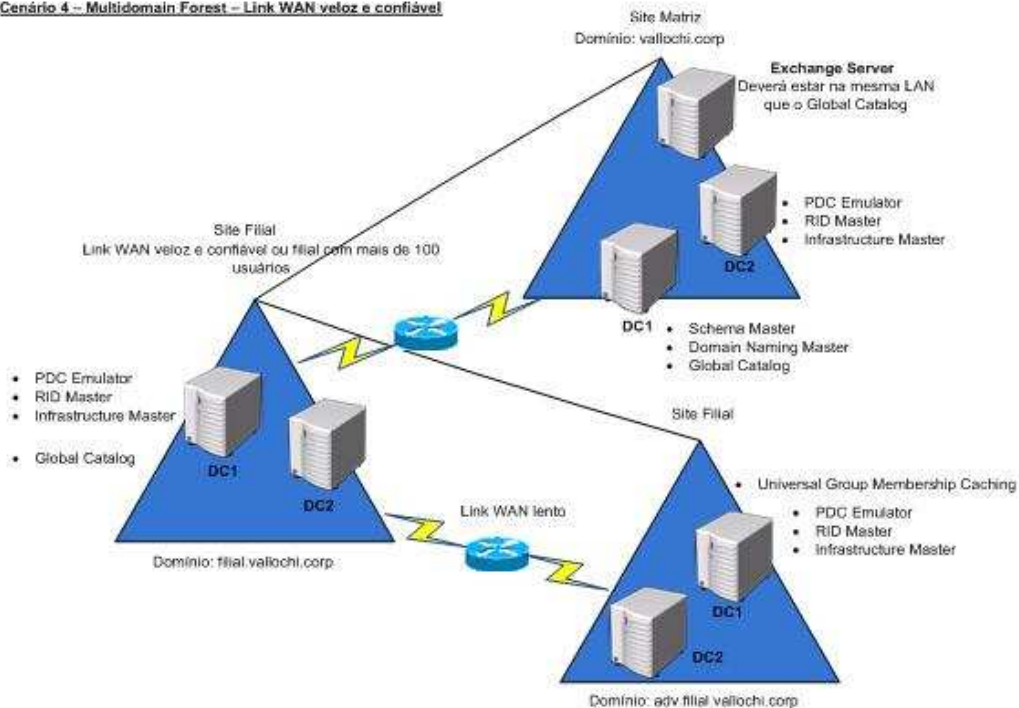
Neste cenário, por se tratar de um link lento a opção de Universal Group Caching seria a mais indicada. Através do 'caching', as informações SIDs de grupos globais e universais são armazenadas localmente no controlador, evitando que o GC seja consultado a cada logon.

Benefícios gerados pelo uso do 'caching':

- ❖ Tempo de logon mais rápido, pois a autenticação não irá requer o contato ao GC para obter os membros dos grupos universais.
- ❖ Maior disponibilidade no logon, pois será possível realizar logon no caso do link entre os sites falhar.
- ❖ Evita necessidade de upgrade de hardware dos controladores de domínio em função dos requerimentos e consumo de recursos gerados pelos GCs.
- ❖ Minimiza o uso do link, pois também não haverá o tráfego de replicação entre os GCs.

Há uma discussão ou recomendação para o uso de um GC no site que tiver mais de 100 usuários em função do tráfego gerado pelas demais consultas que os controladores fazem aos GCs em busca de objetos de outros domínios. Neste caso vale melhor análise/avaliação.

Cenário 4 – Multidomain Forest – Link WAN veloz e confiável



Trouxe este cenário como exemplo de combinação das soluções apresentadas anteriormente e para reforçar o conceito de se colocar o GC na mesma rede LAN do Exchange Server. O GC é utilizado pelos servidores de email na localização de usuários, contatos e do Global Address List. Isto evita inclusive que haja problema de envio e recebimento de email quando houver queda de link entre duas localidades.

Referências

1- Planejando, implementando e fazendo a manutenção de uma infra-estrutura do Active Directory® do Microsoft® Windows Server. 2003, Módulo 1, página 9.

2- Planejando, implementando e fazendo a manutenção de uma infra-estrutura do Active Directory® do Microsoft® Windows Server. 2003, Módulo 1, página 23.

<http://www.microsoft.com/brasil/technet/Colunas/DaniloBordini/GlobalCatalog.mspix>, acesso em 23/07/2008, 18:00 horas.

<http://www.microsoft.com/brasil/technet/Colunas/DaniloBordini/operacoesmestres.mspix>, acesso em 23/07/2008, 18:45 horas.

<http://technet2.microsoft.com/windowsserver/en/library/440e44ab-ea05-4bd8-a68c-12cf8fb1af501033.mspix?mfr=true>, acesso em 23/07/2008, 21:00 horas.

<http://blogs.dirteam.com/blogs/jorge/archive/2006/05/25/1040.aspx>, acesso em 25/07/2008, 22:30 horas.

Autor: Savio Talamoni Vallochi

Profissional com larga experiência na área de Tecnologia com foco em Redes e Segurança da Informação, trabalhando atualmente na CPM Braxis, uma das maiores consultorias de TI brasileiras, atuando em grandes clientes do setor financeiro, formado em Ciências Jurídicas, Pós-Graduado em Segurança da Informação, com certificações Microsoft MCP, MCSA, MCSE e ITIL Foundation.

Visite meu blog em <http://saviovallochi.spaces.live.com/>