// você está lendo...

ACTIVE DIRECTORY

Definir DC secundário como principal em caso de desastres

PUBLICADO POR BRUNO FELIPE · QUARTA-FEIRA, 16 NOVEMBRO 2011 · 5 COMENTÁRIOS

ARQUIVADO EM ACTIVE DIRECTORY, DESASTRE, DHCP, DOMAIN CONTROLLER, FSMO, METADATA CLEANUP, NTDS, NTDSUTIL, SIZE, WINDOWS SERVER 2008

Saudações pessoal, mais uma vez de volta ao blog, e dessa vez com um artigo muito interessante e ponto crítico para alguns técnicos e administradores.

Alguma vez já se passou pela cabeça (ou nos piores casos já aconteceram). O que fazer caso o meu Domain Controller principal morrer (considere morrer como um desastre, a situação em que nenhum troubleshooting resolveu, um problema físico como discos, ou nos extremos casos, roubo de equipamento e até mesmo incêndio).

Se dentro do seu ambiente você não ter uma estrutura de contingência prepare-se para uma longa lista de chamados. Para tanto existem outras maneiras de se previnir um desastre, porém as mesmas exigem um investimento maior a equipamentos (exemplificando um cenário de clustering), o que em algumas empresas não se faz jus o investimento.

Vamos exemplificar o cenário e a função de cada server nesse ambiente:
DC01 – Domain Controller Principal – Windows 2008R2 – DHCP Ativo na Rede (Esse garotão irá morrer)
DC02 – Domain Controller Adicional – Windows 2008R2 – DHCP Configurado porém não ativo (Esse está com as replicações e funcionamento normal)
FS01 – File Server – Windows 2008R2 (Esse mantém todos os compartilhamentos e políticas de File Server)
CL01 – Domain Client – Windows 7 (Client do domínio a ser usado como testes)

Reparem que nesse cenário não tenho o meu File Server junto ao meu Domain Controller, isso é uma boa prática e MUITO recomendada pela Microsoft, se você quer a integridade dos seus arquivos TENHA os mesmos em um servidor separado do seu Domain Controller.

Nesse artigo não entrarei em critérios de backups / storage, pois já sabemos o tamanho da necessidade dos mesmos, vamos nos concentrar somente na função de servidor por enquanto.

NOTA: *Após a realização desse processo, o servidor excluído não poderá ser adicionado novamente ao domínio, o mesmo deverá ser feito do zero e iniciar os procedimentos normais de adição de servidor ao domínio*

1- Iniciando o artigo já temos o DC01 fora do ar por um motivo de desastre, ao tentar logar com o nosso Client já é apresentado um erro que não há servidor disponível. Imagine os usuários da empresa congestionando o suporte técnico.

CATEGORIAS
Active Directory
Clients
Diversos
File Services
Lightweight Directory Services
Microsoft Forefront
Windows Server

ARQUIVOS
abril 2012
março 2012
fevereiro 2012
dezembro 2011
novembro 2011
outubro 2011
setembro 2011
junho 2011
maio 2011
abril 2011

LISTA DE LINKS
Facebook

META
Registrar-se
Login

Seguir

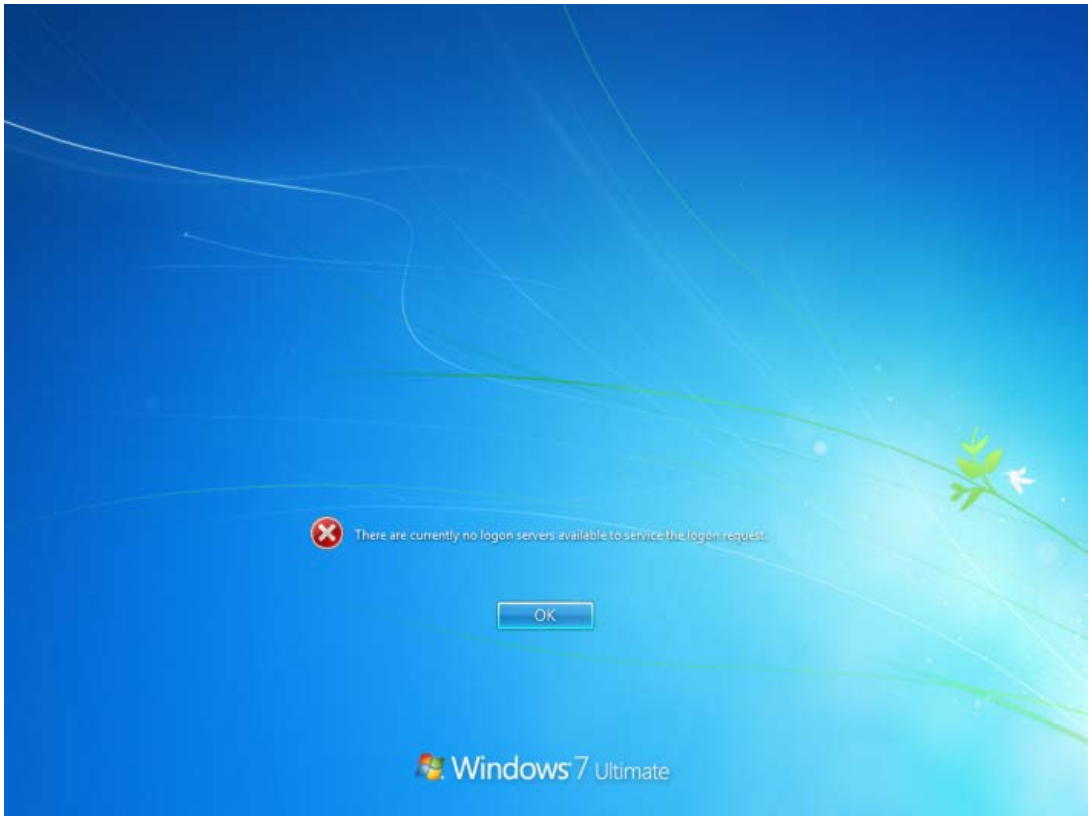
Seguir “Suporte de Rede”

Obtenha todo post novo entregue na sua caixa de entrada.

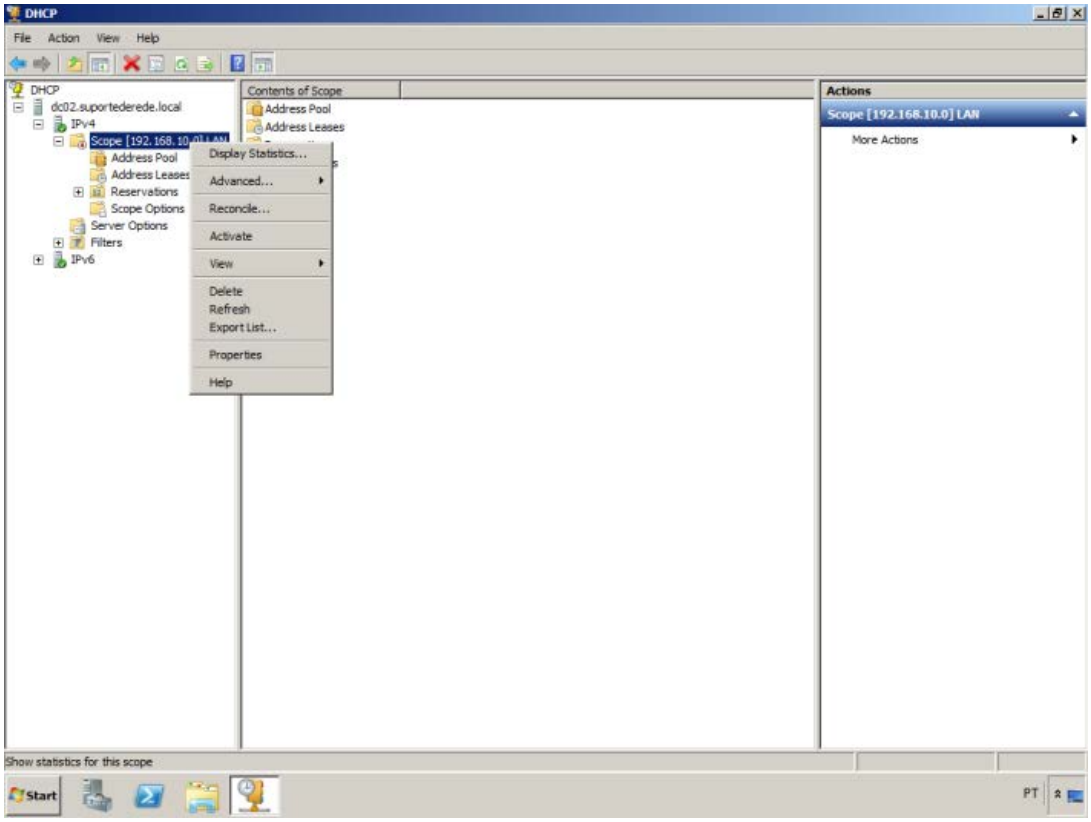
Insira seu endereço de e-mail

Cadastre-me

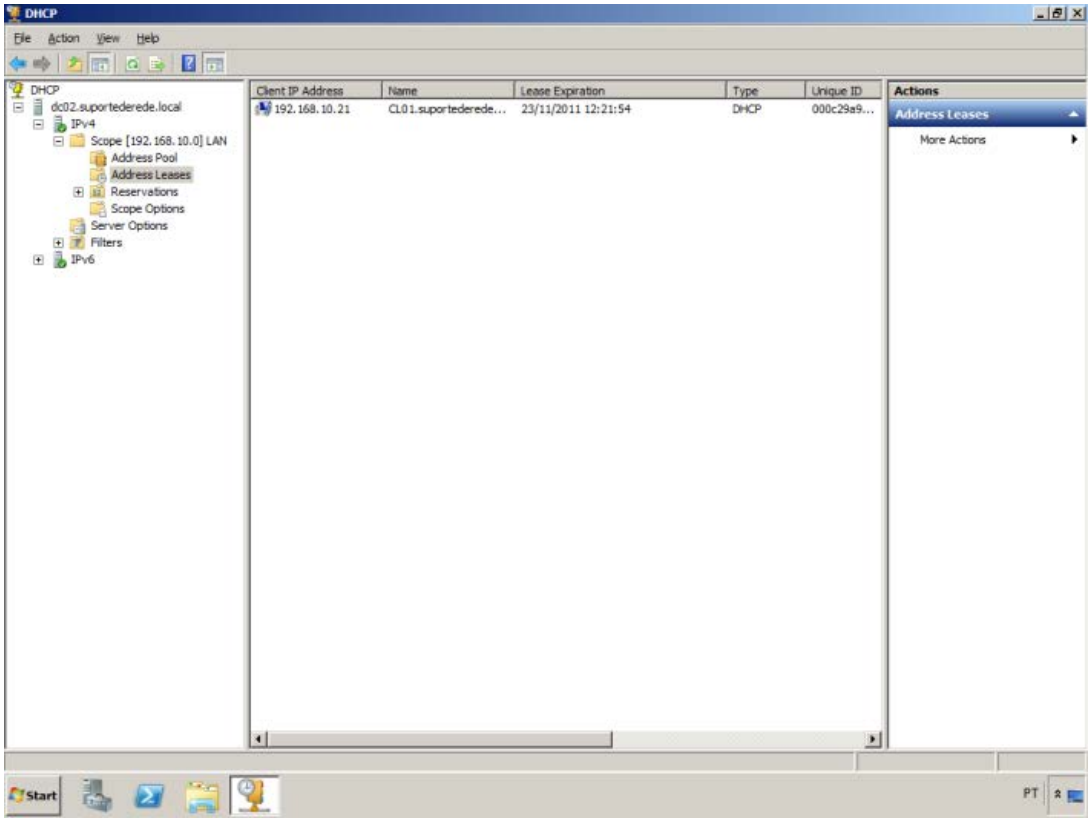
Tecnologia WordPress.com



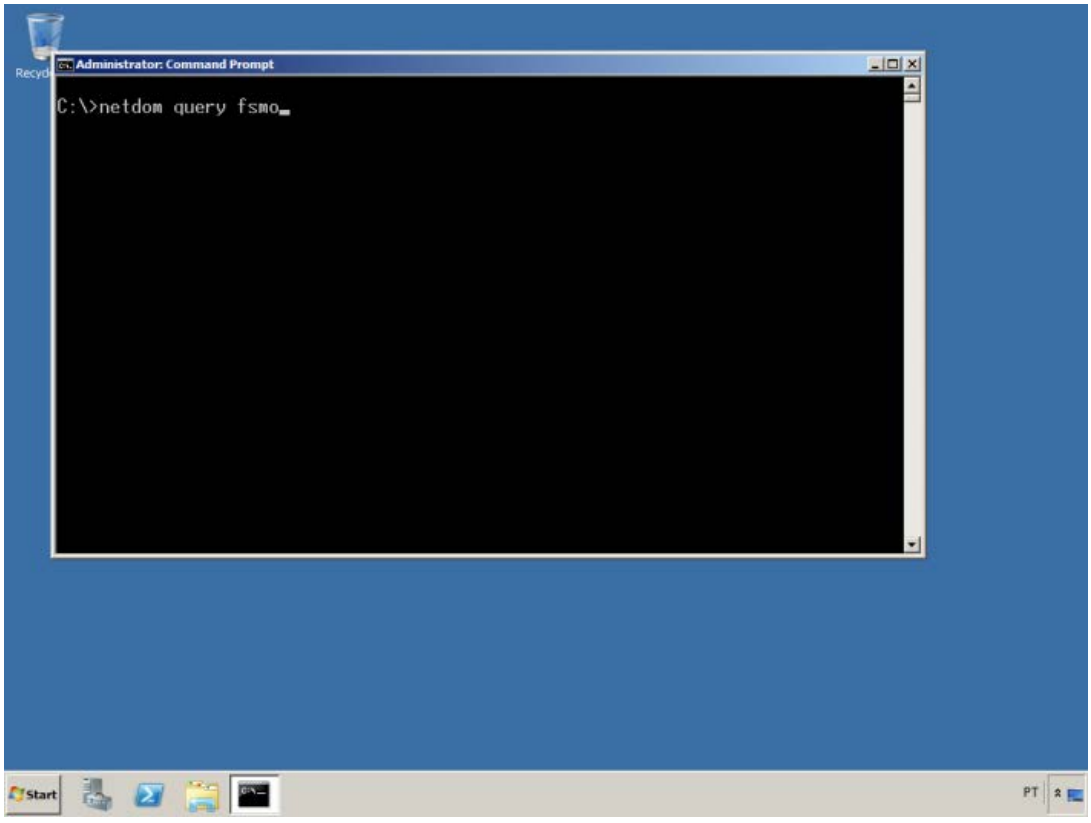
2- Nosso primeiro passo no DC02 é ativar o DHCP que já estava “pré configurado” (a configuração é simples, porém não mantenha ativo para que não haja conflito com o DHCP primário). O importante a se reparar é o range a ser distribuído se não irá conflitar com alguma atribuição fixa já existente, e também se não há nenhuma referência DNS ao servidor antigo. Para ativação, clique com o botão direito sobre o escopo e depois em “Activate”.



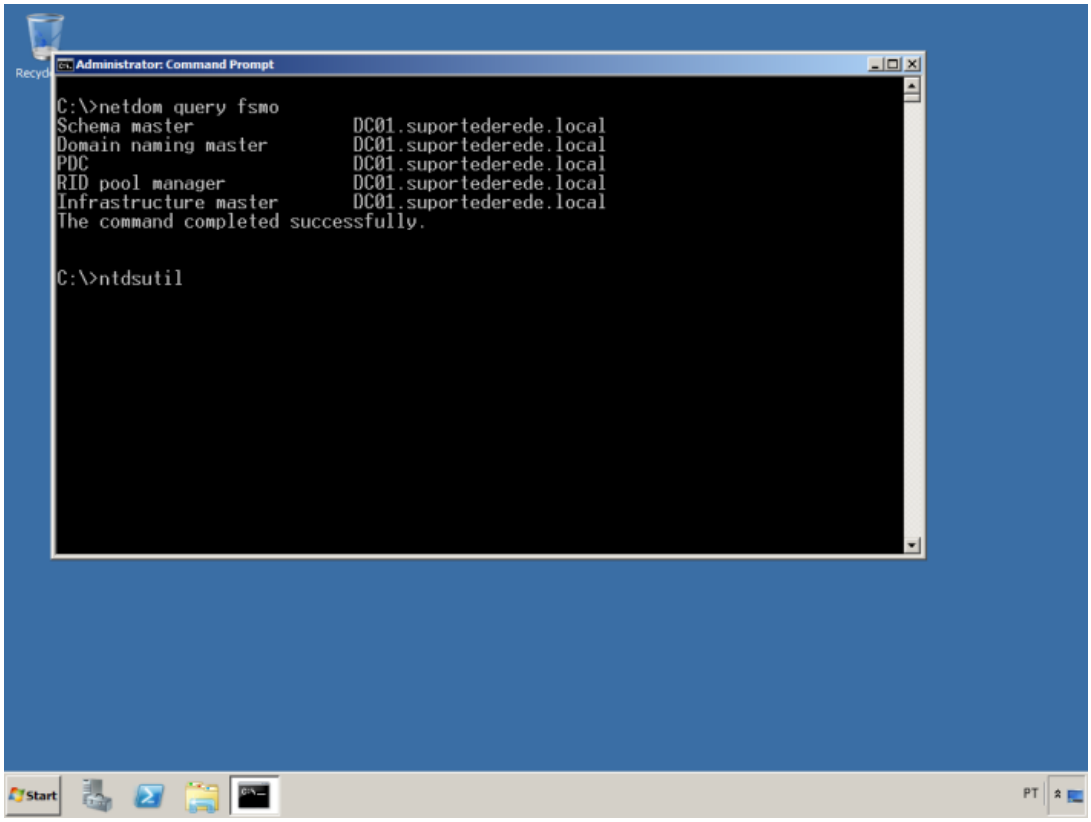
3- Após reiniciar o meu client (CL01), acompanhando pela opção “Address Leases” já reparo que o IP foi atribuído com sucesso ao meu client.



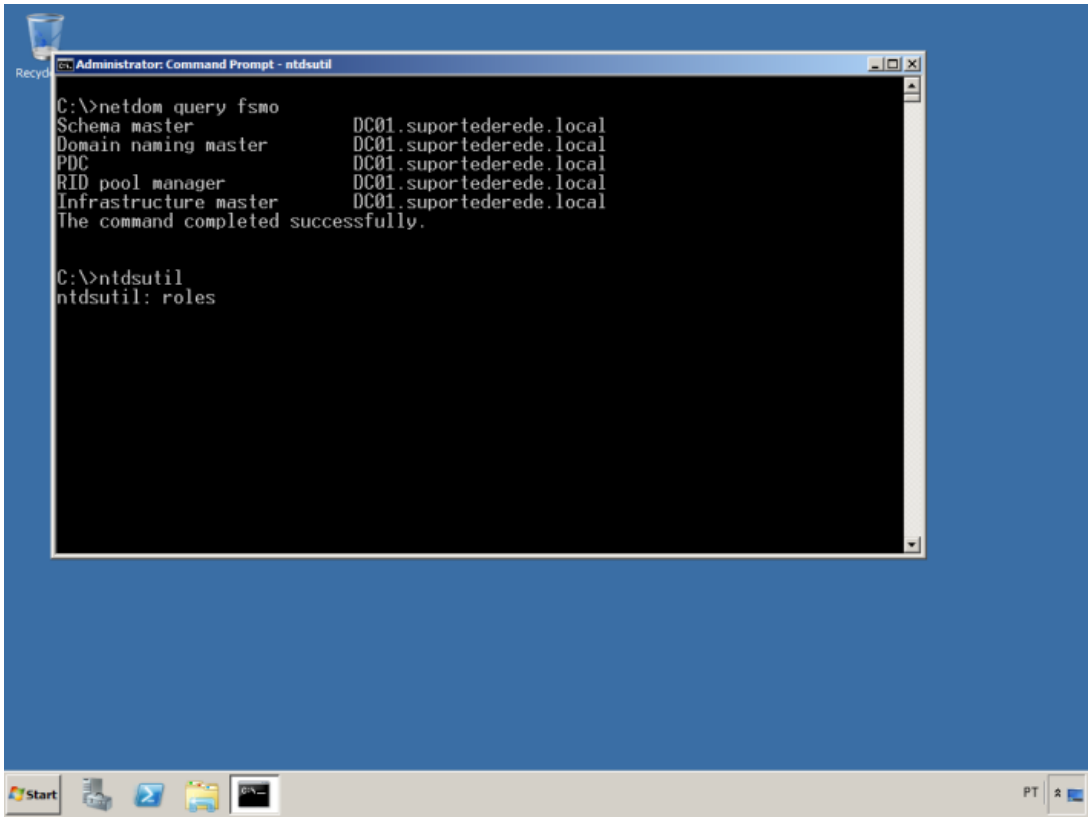
4- Agora vamos iniciar o processos para migração das FSMO (Flexible Single Master Operation), primeiro precisamos consultar quem são os mestres de operação, para isso abra o prompt de comando e digite: **netdom query fsmo**



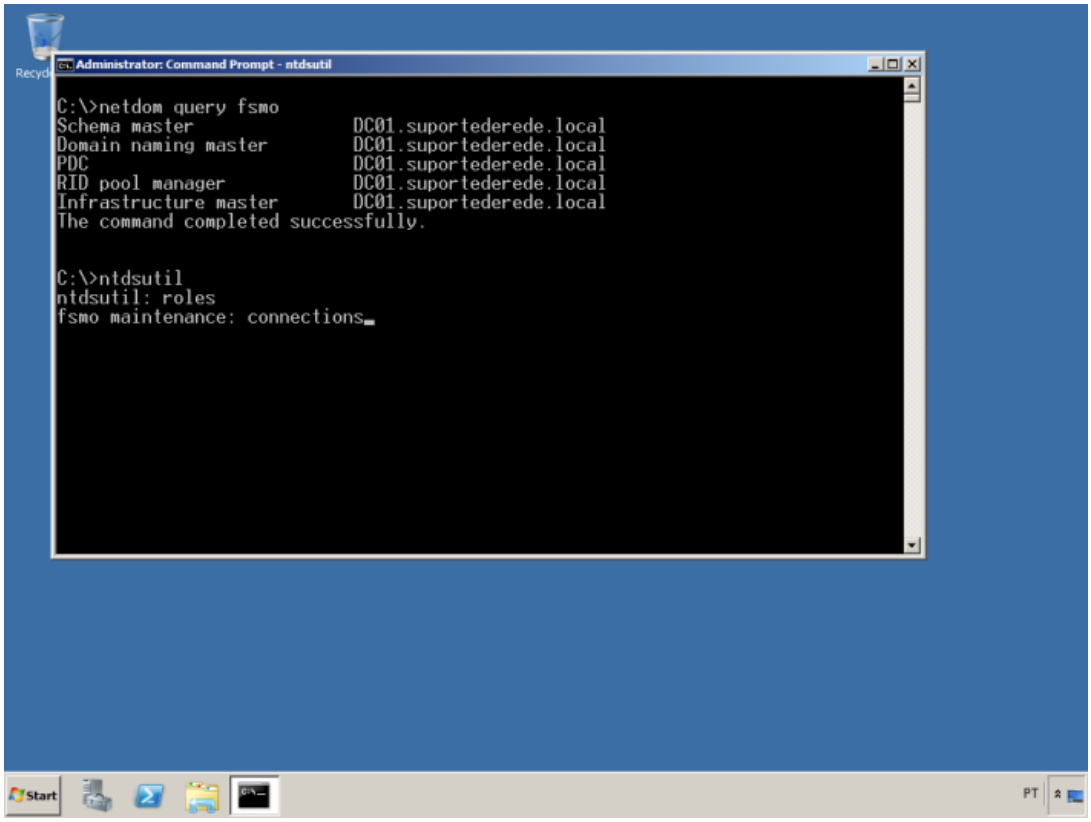
5- Verificamos que todos os operations masters apontam para o DC01 (servidor falecido rsrsrs). Precisaremos entrar na base NTDS para fazer as seguintes ações, para isso digite: **ntdsutil**



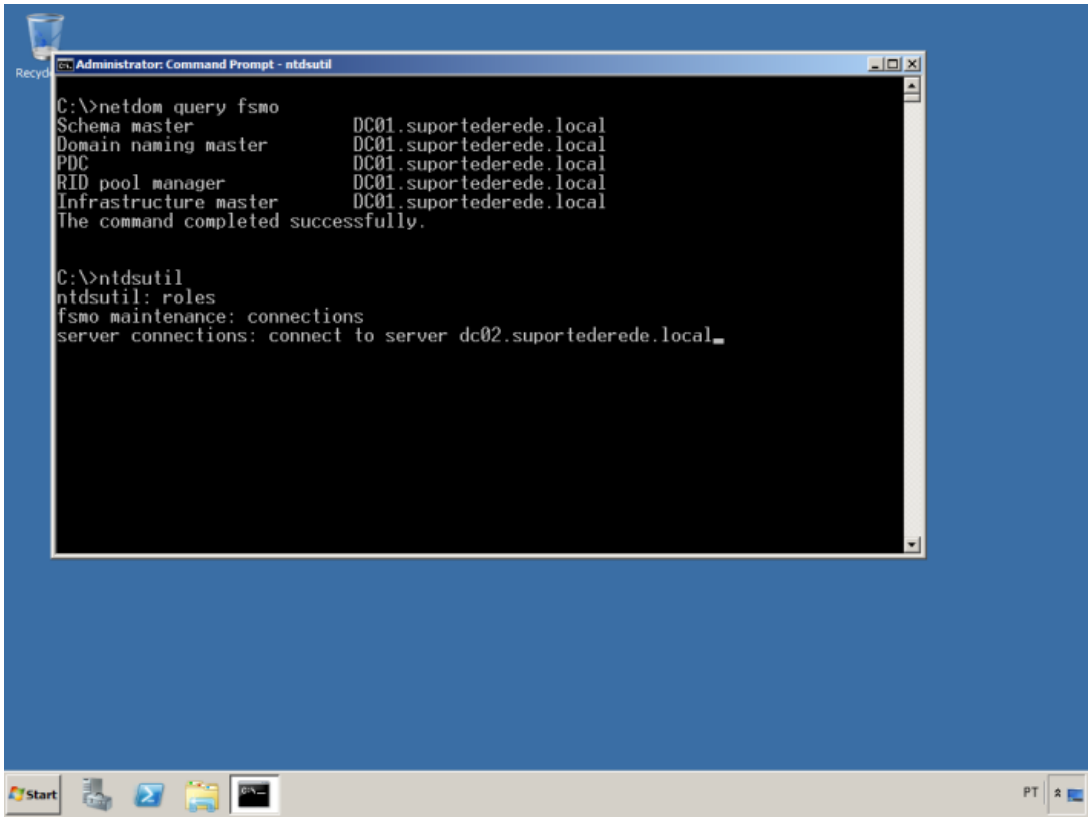
6- Em seguida digite: **roles**



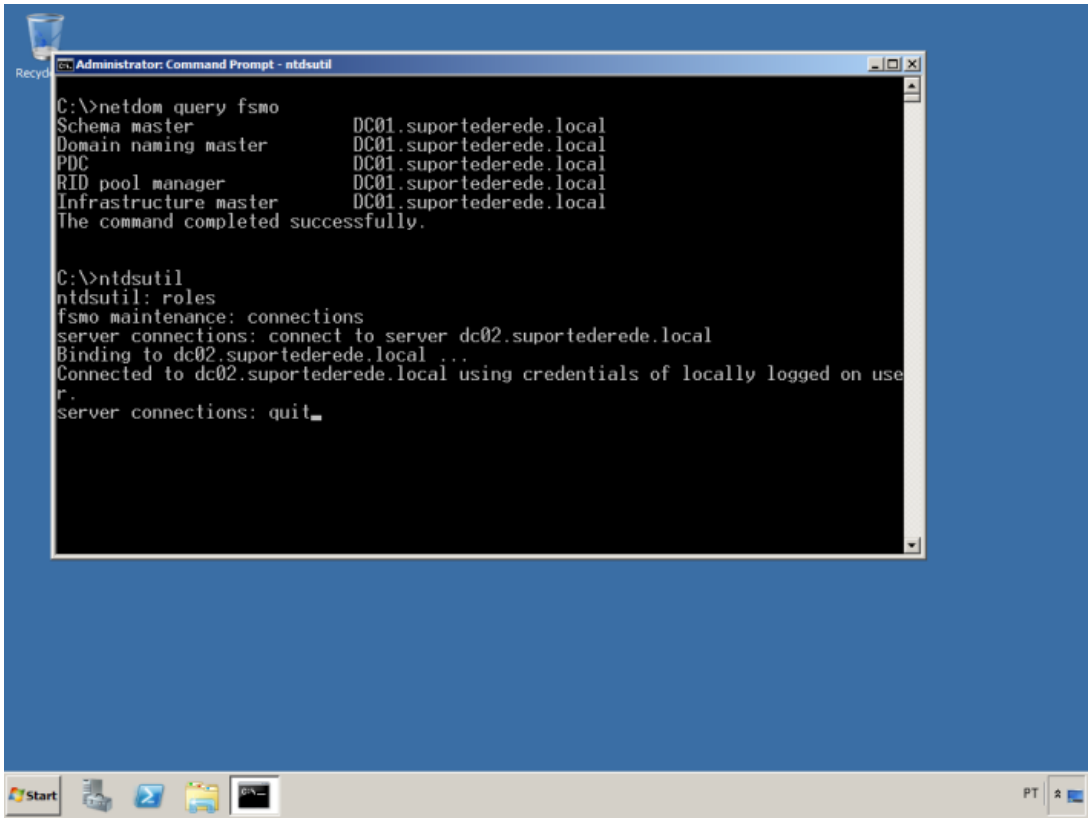
7- Em “fsmo maintenance” digite: **connections**



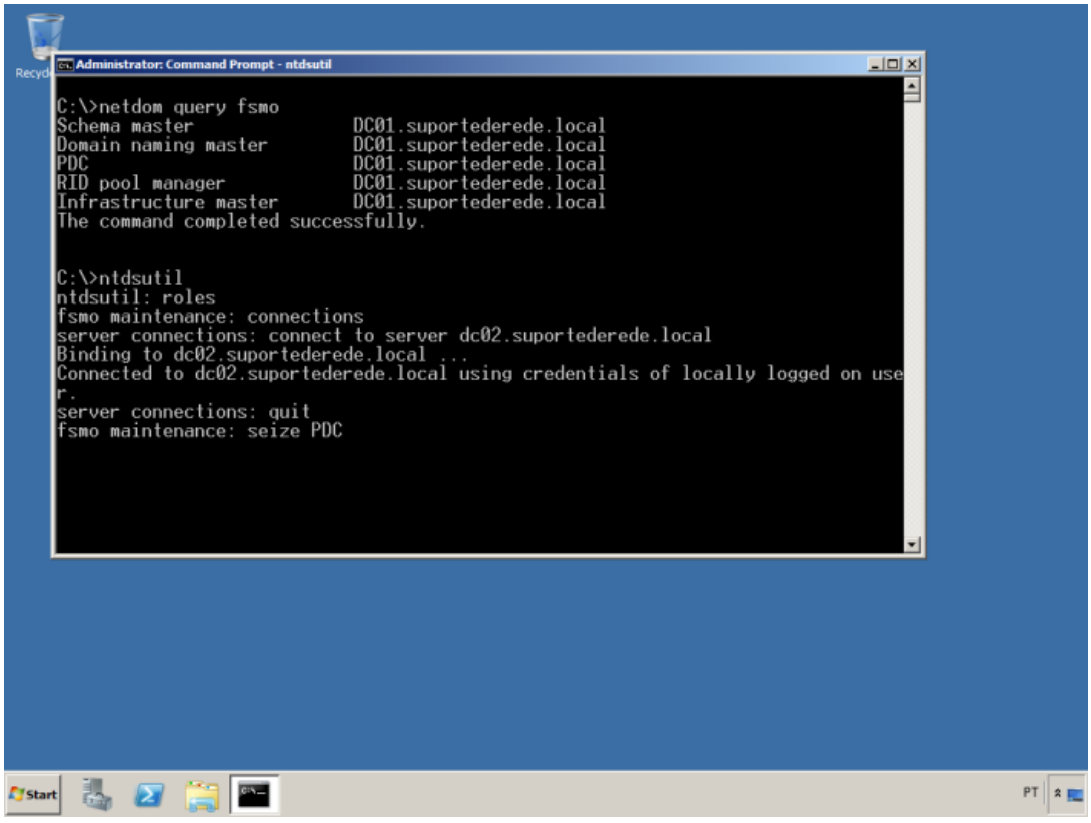
8- Em “server connections” digite: **connect to server *nome_do_dc_ativo*** (No nosso caso dc02.suportederede.local)



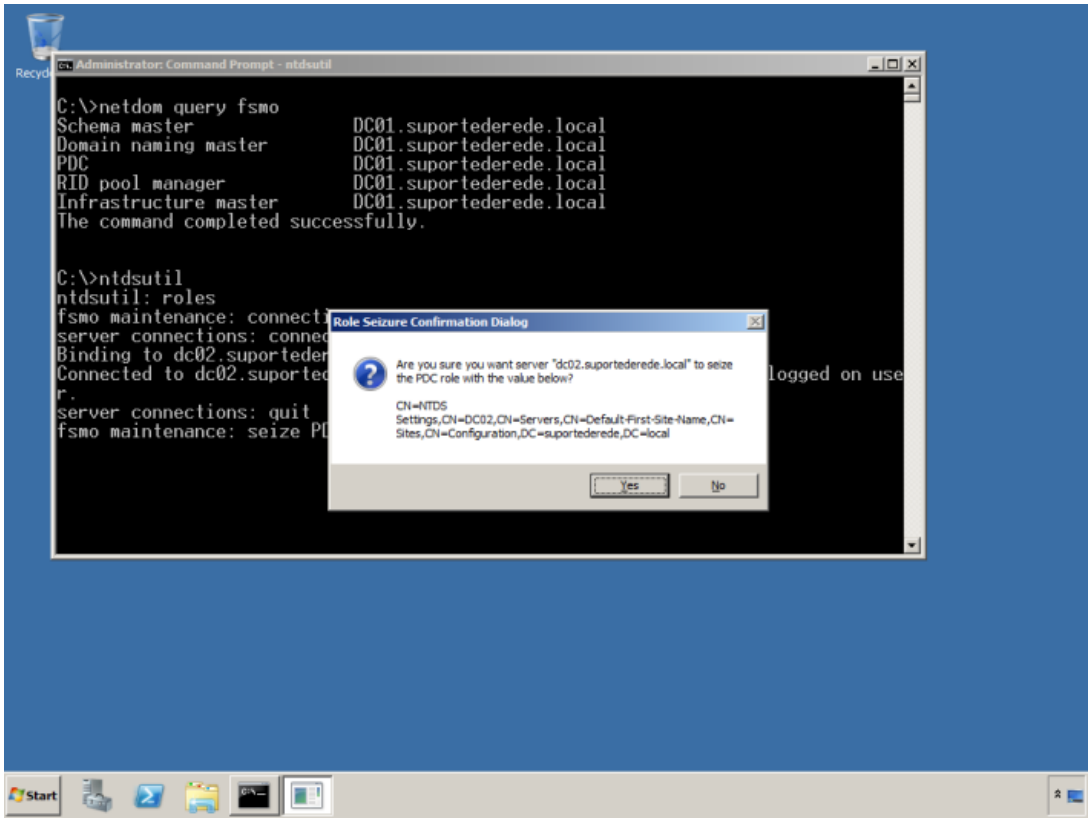
9- Será usada as credenciais administrativas locais, em “server connections” digite: **quit**



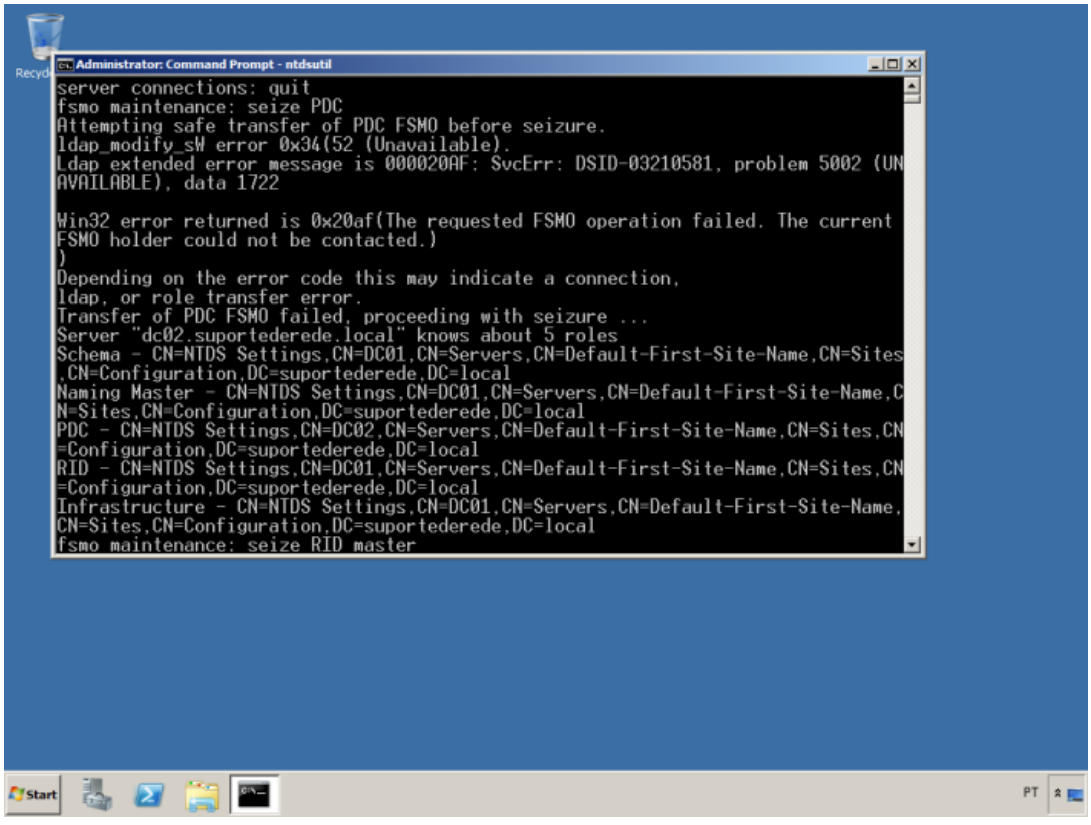
10- Agora novamente em “fsmo maintenance” digite: **seize PDC**



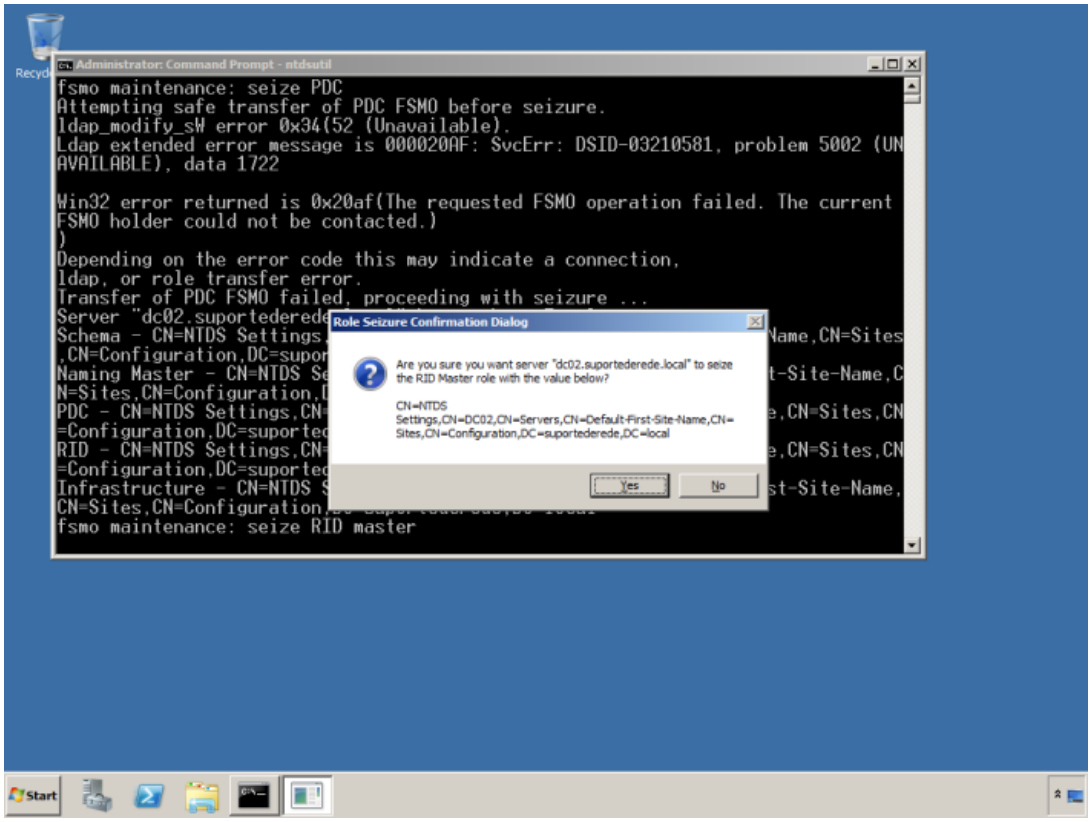
11- Confirme com **Yes** a caixa de diálogo.



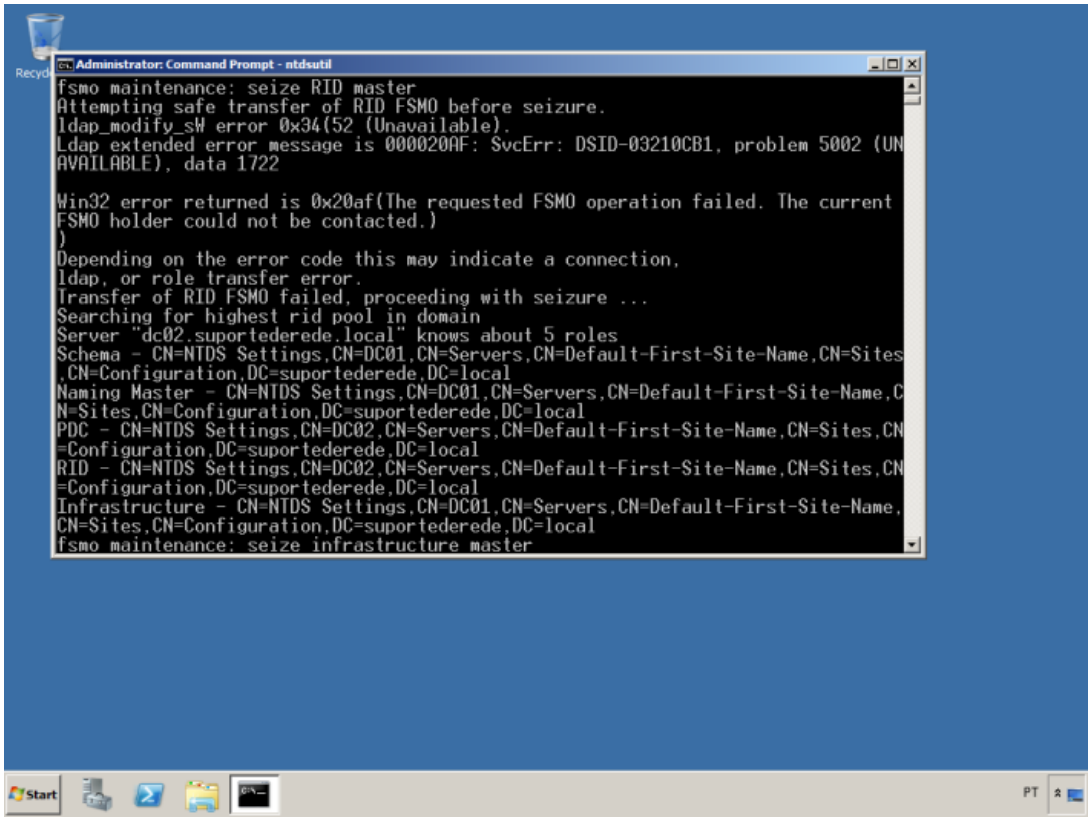
12- Após o término digite: **seize RID master**



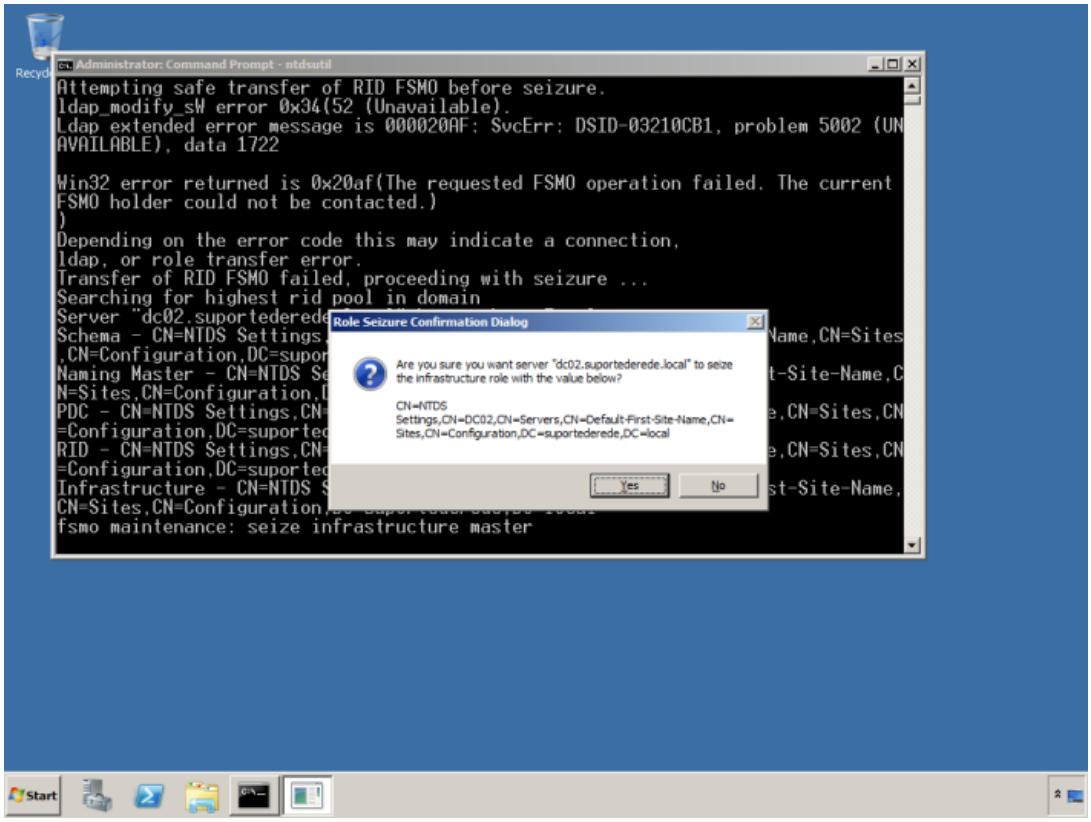
13- Mais uma vez confirme com **Yes** a caixa de diálogo.



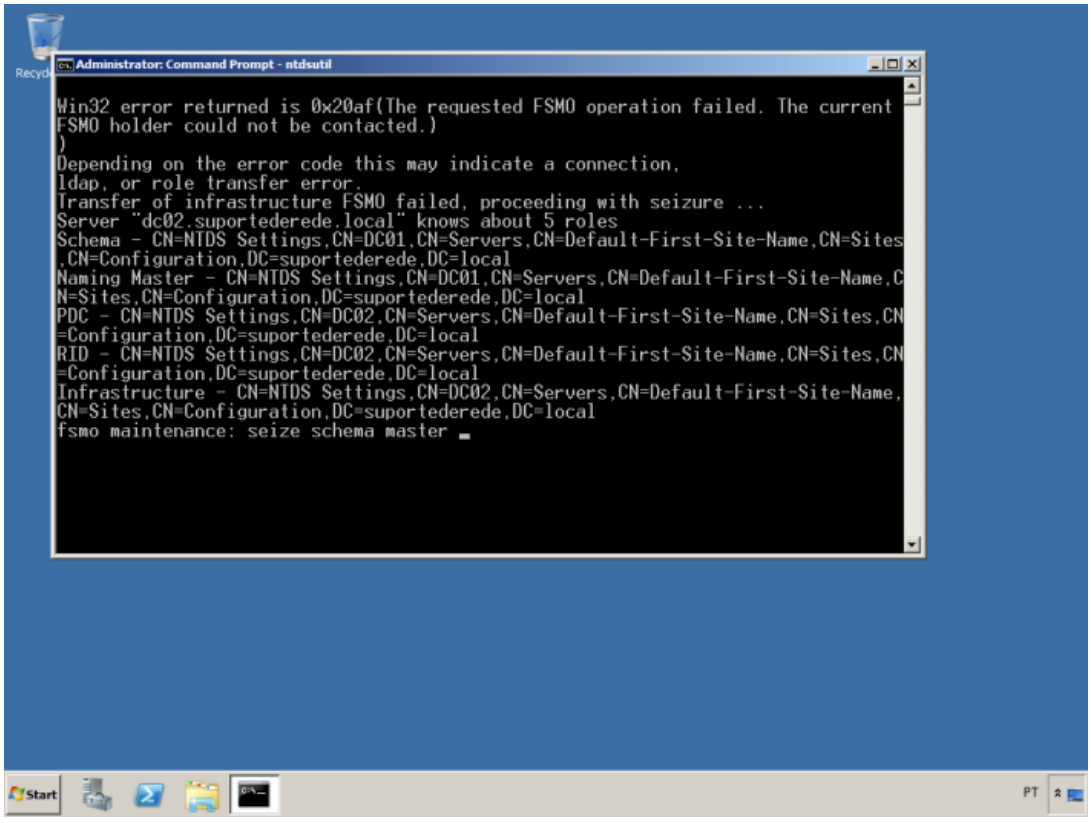
14- Terminando digite: **seize infraestructure master**



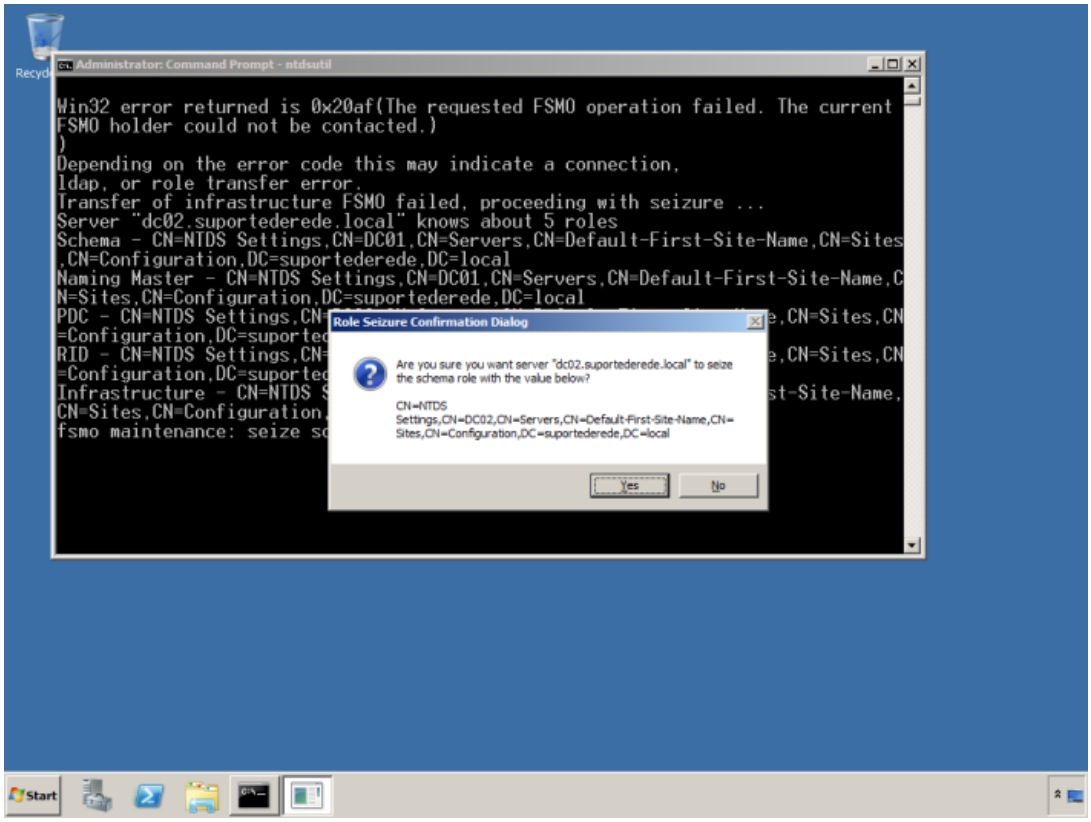
15- Confirme com **Yes** a caixa de diálogo.



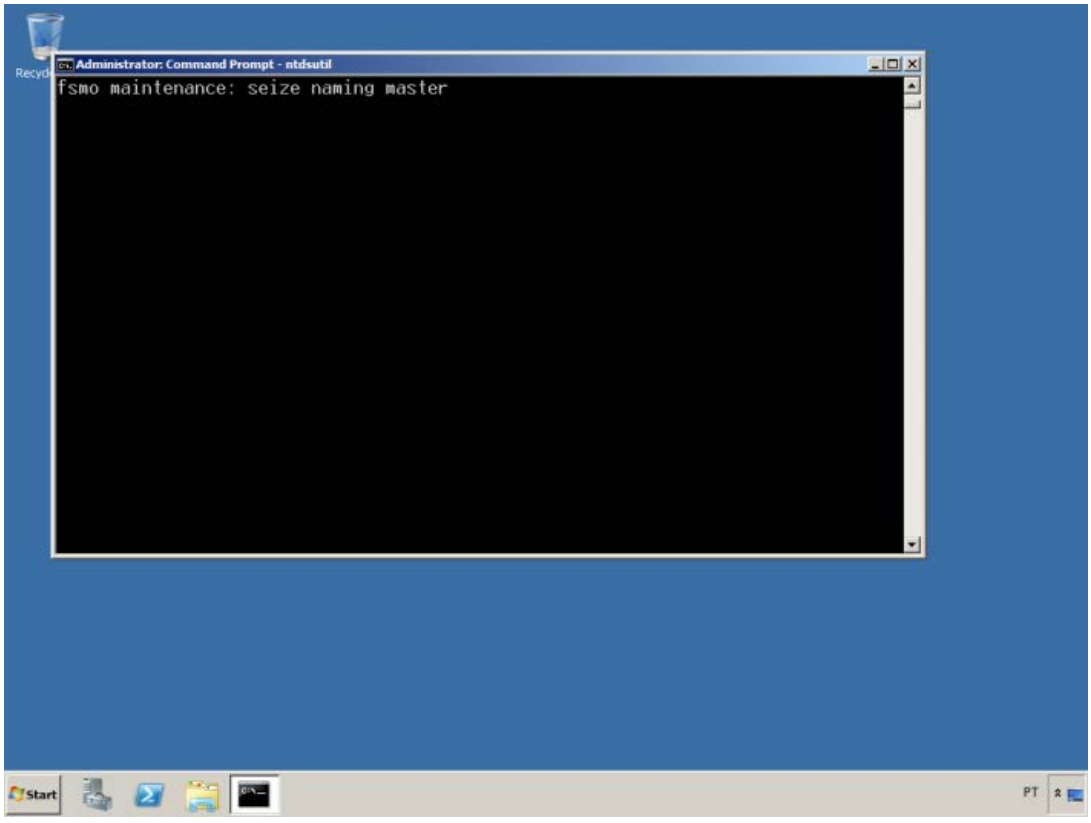
16- Agora digite: **seize schema master**



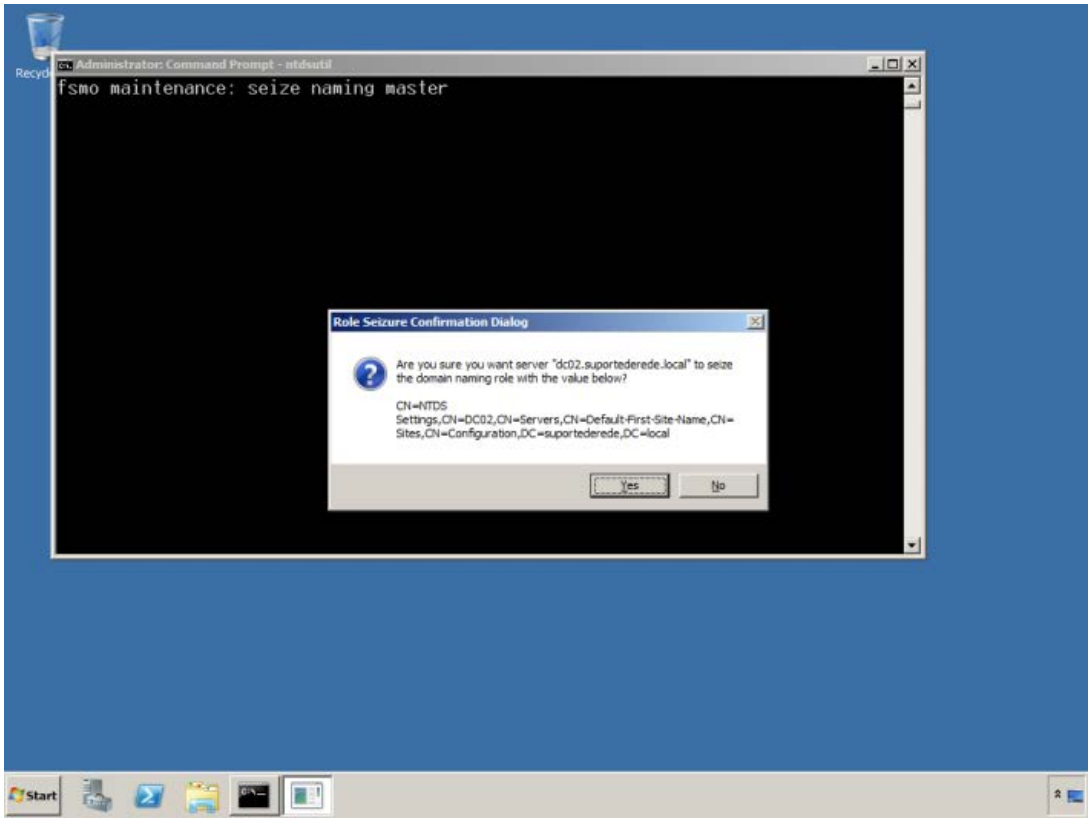
17- Confirme com **Yes** a caixa de diálogo.



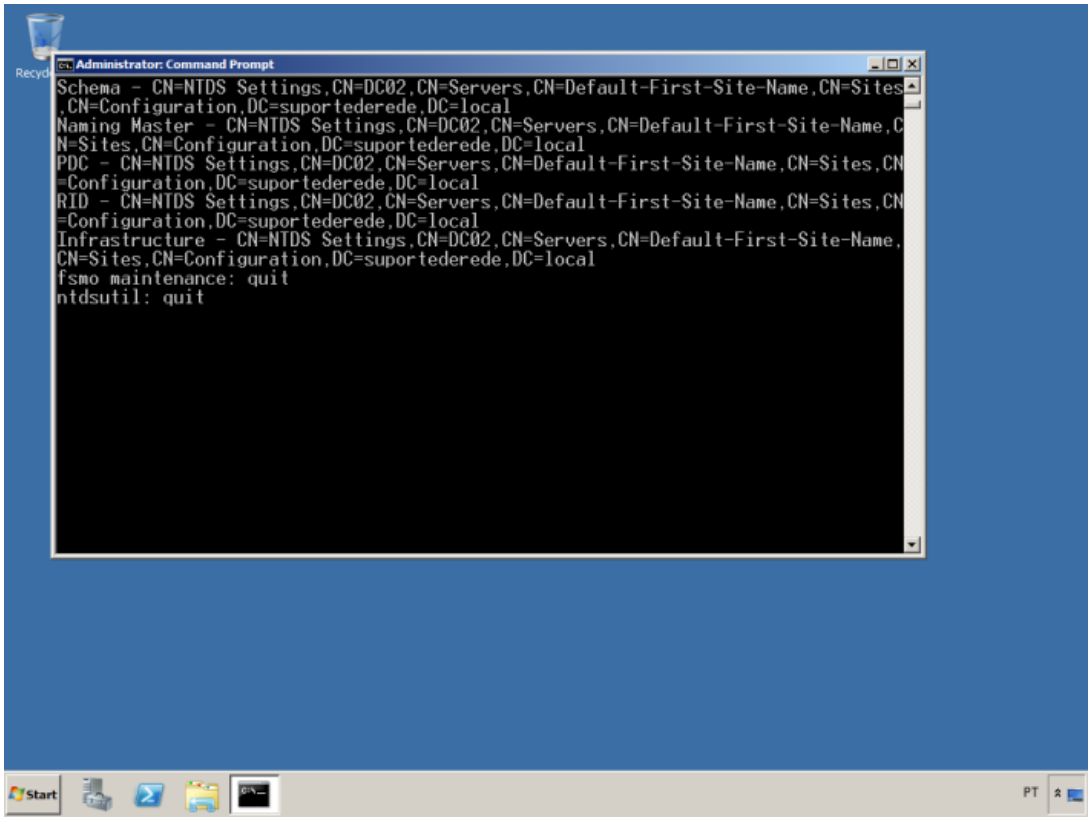
18- Para finalizar digite: **seize naming master**



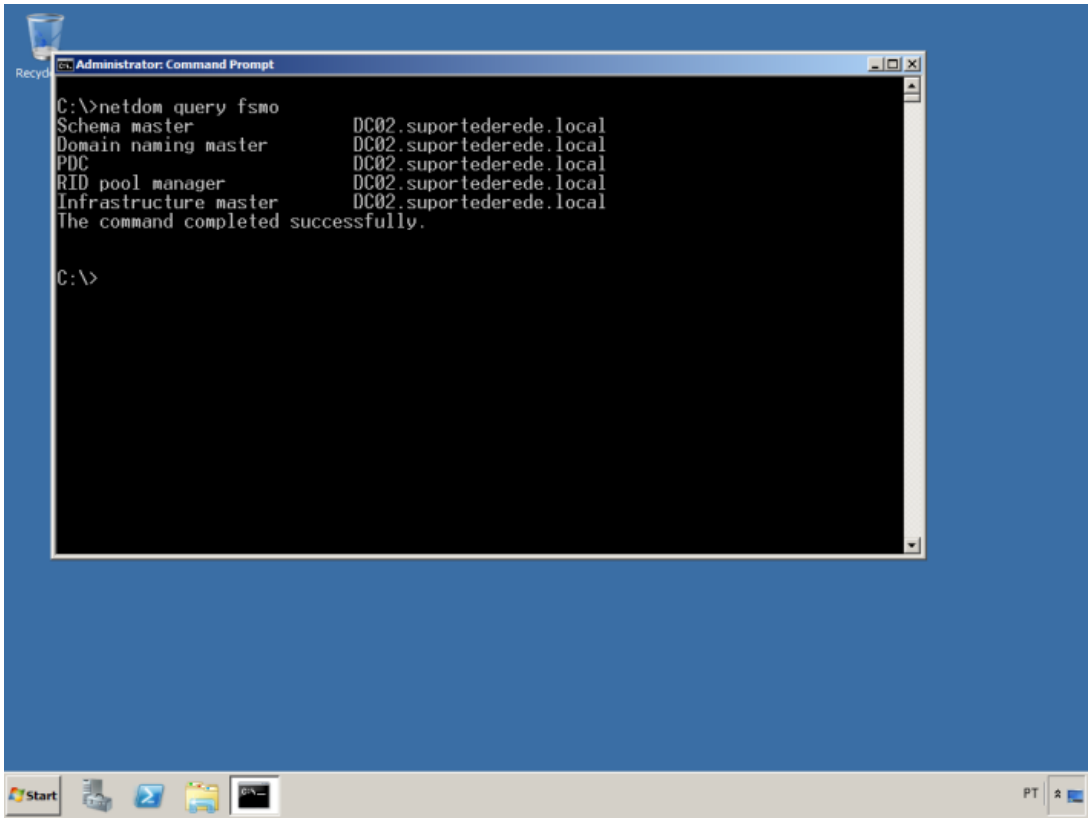
19- Confirme com **Yes** a caixa de diálogo.



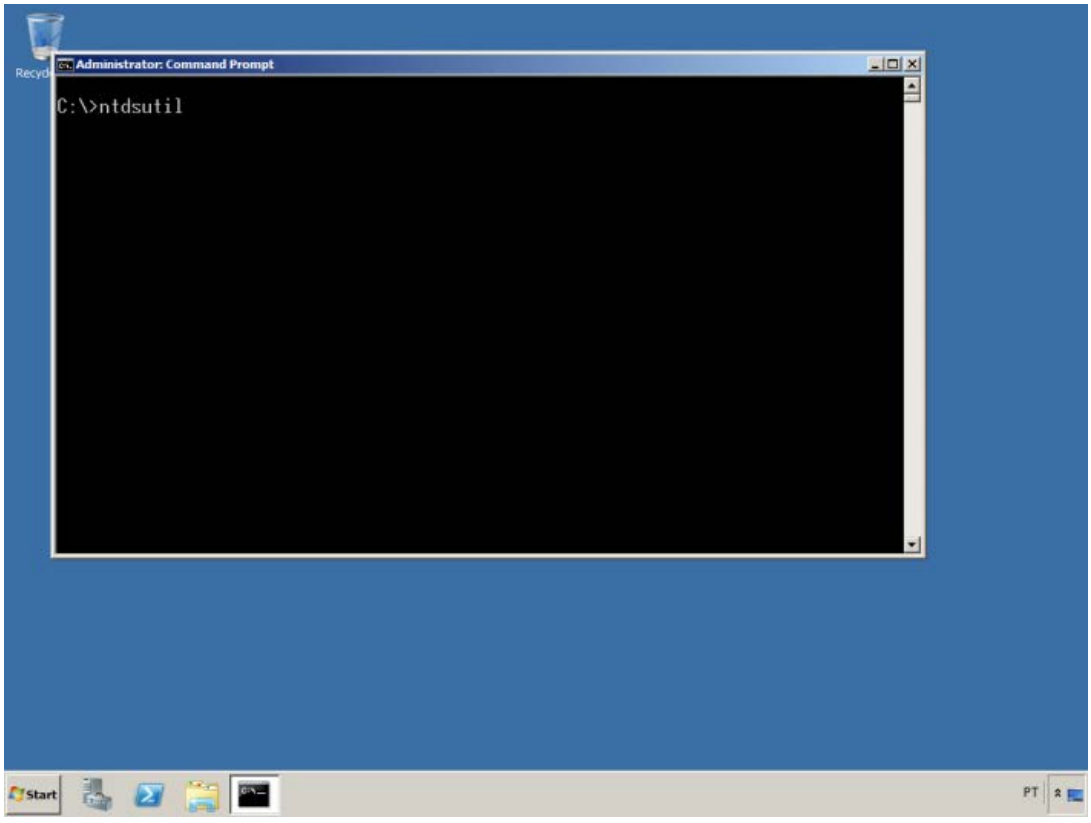
20- Após o término em "fsmo maintenance" digite **quit** e em seguida **quit** novamente.



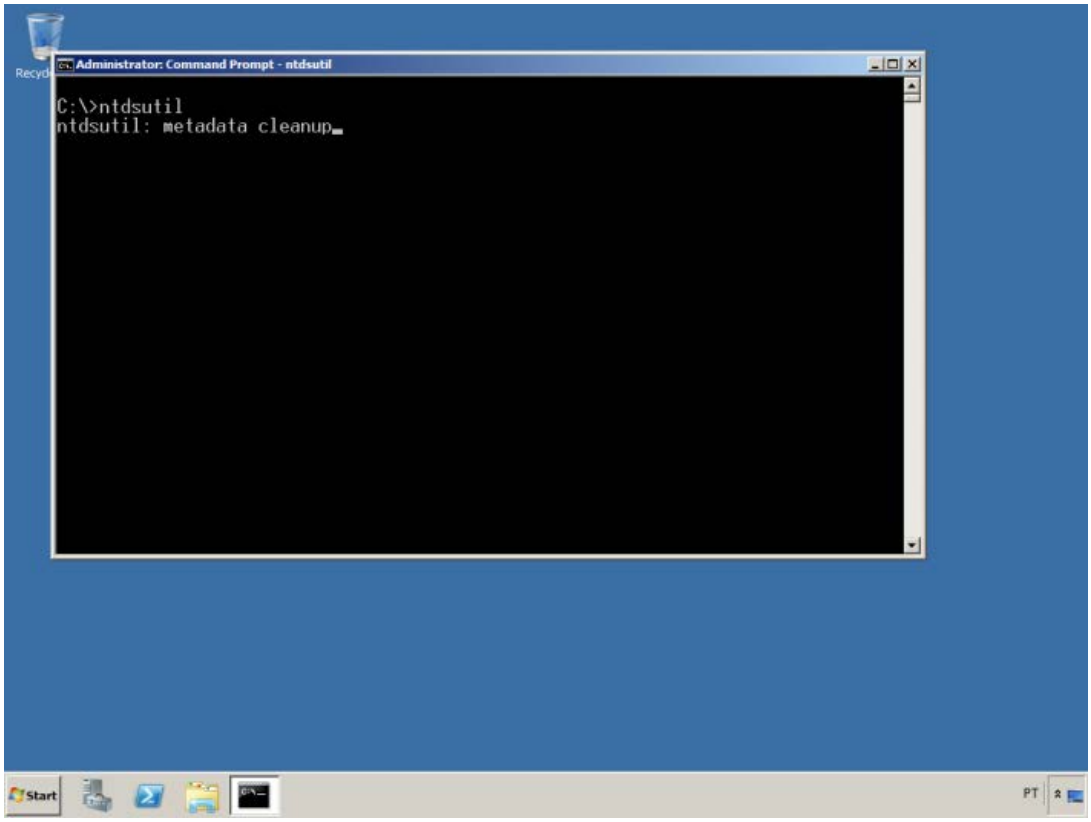
21- Agora de volta ao prompt digite: **netdom query fsmo** verifique se já faz referência ao novo servidor. No nosso cenário no dc02.suportederede.local.



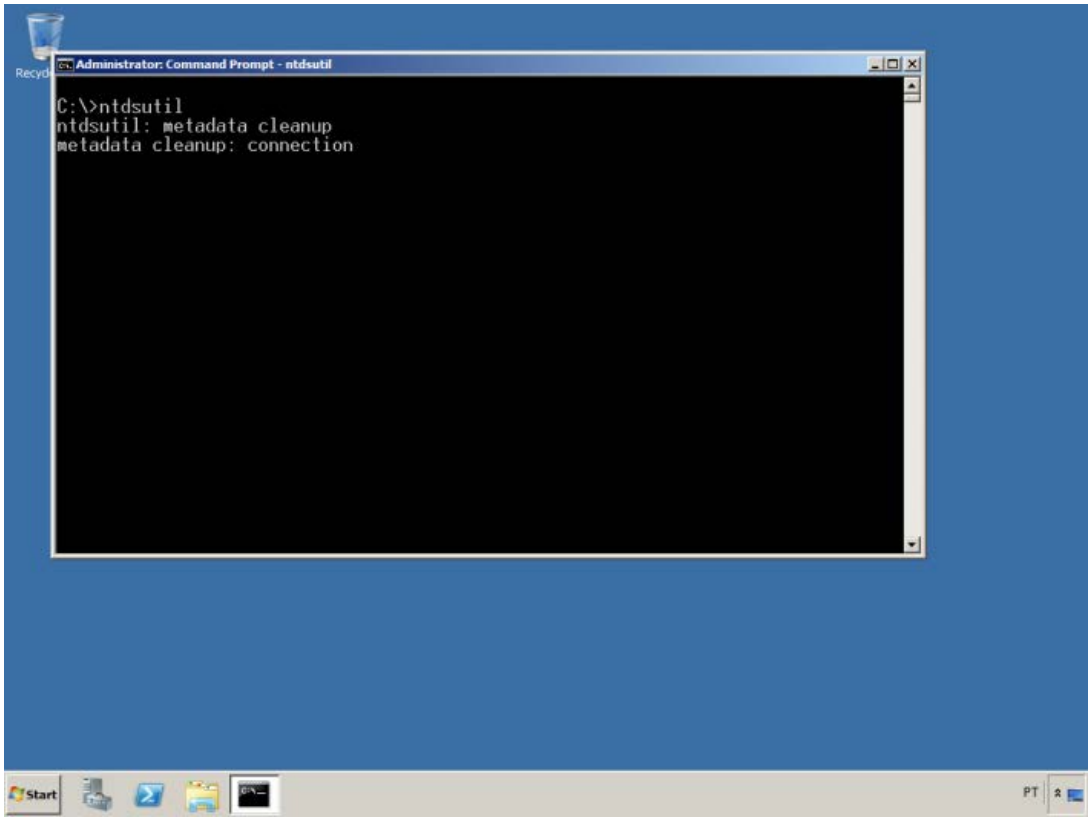
22- Agora será necessário rodar o “metadata cleanup” mais uma vez a ser realizado pela edição da base NTDS. Para isso ainda no prompt digite: **ntdsutil**



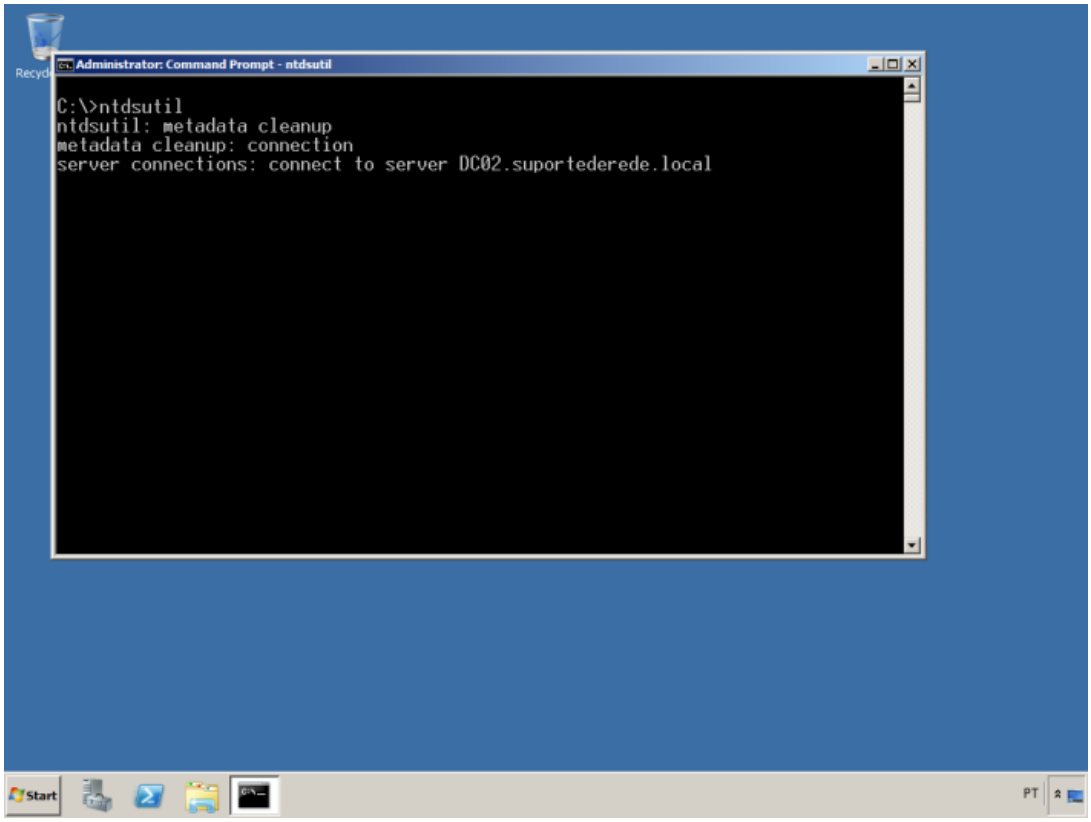
23- Em seguida digite: **metadata cleanup**



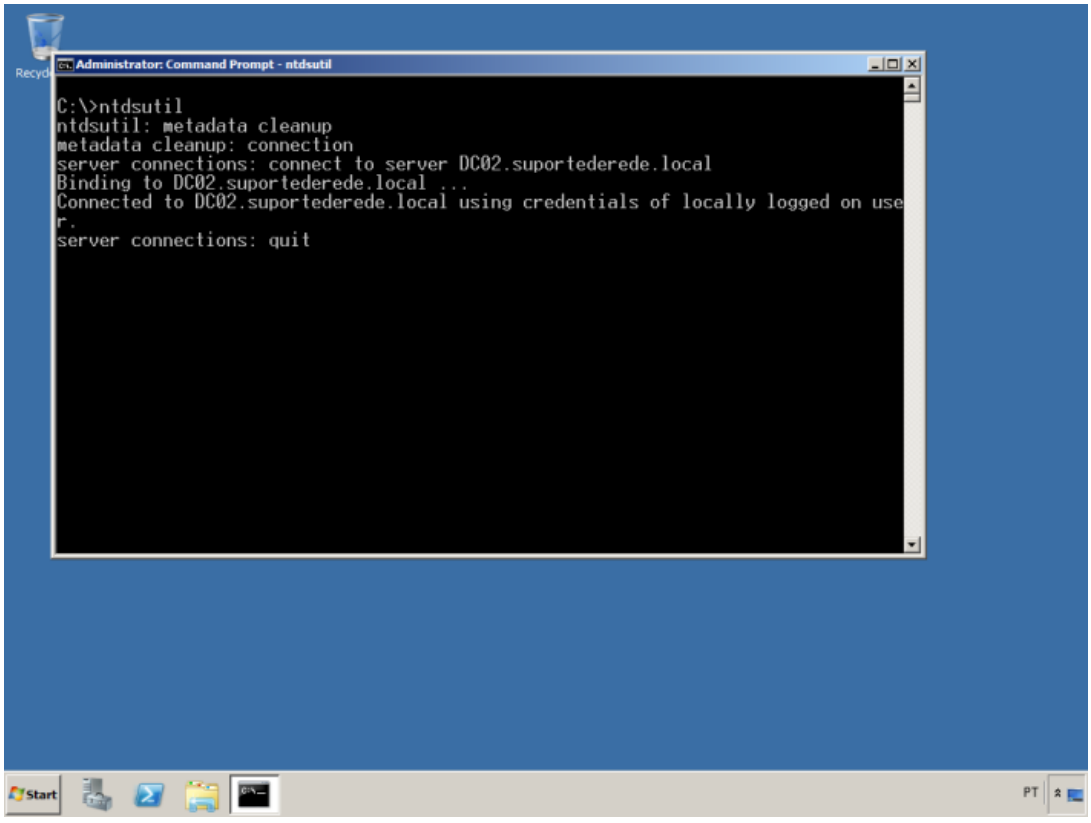
24- Em seguida: **connection**



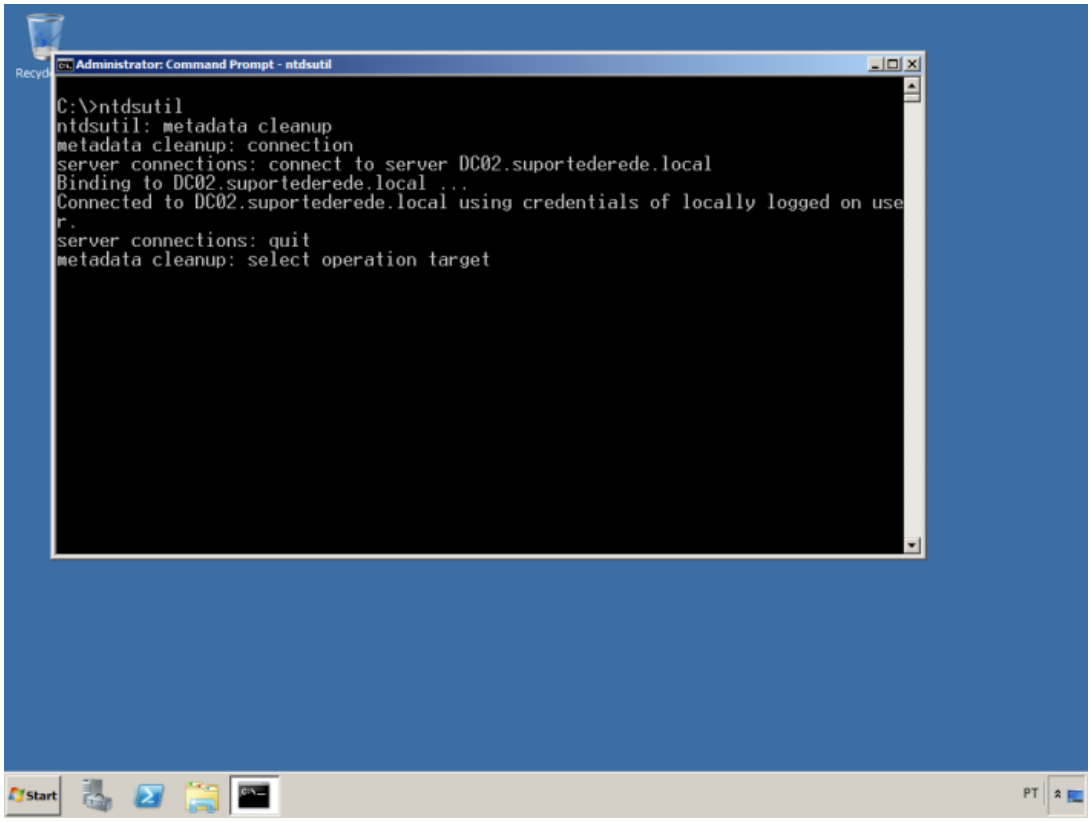
25- Em “server connections” digite: **connect to server *nome_do_dc_ativo*** (No nosso caso dc02.suportederede.local)



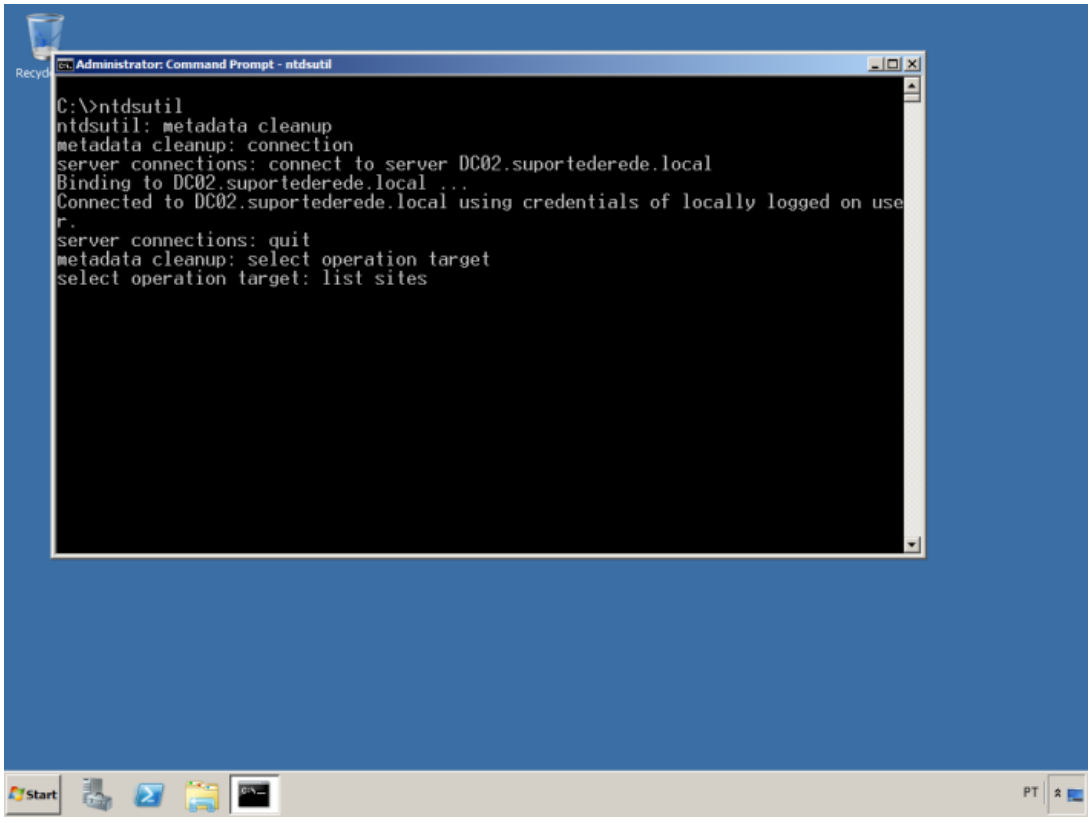
26- Em ”server connections” digite: **quit**



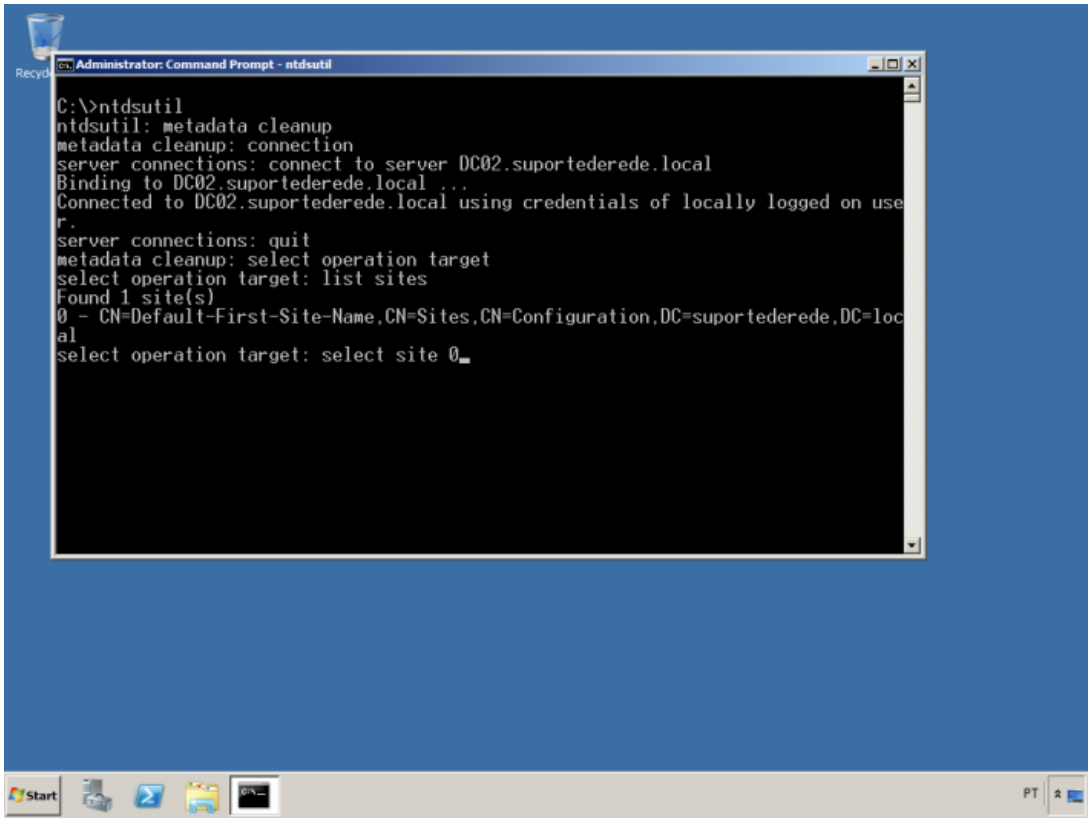
27- Em “metadata cleanup” digite: **select operation target**



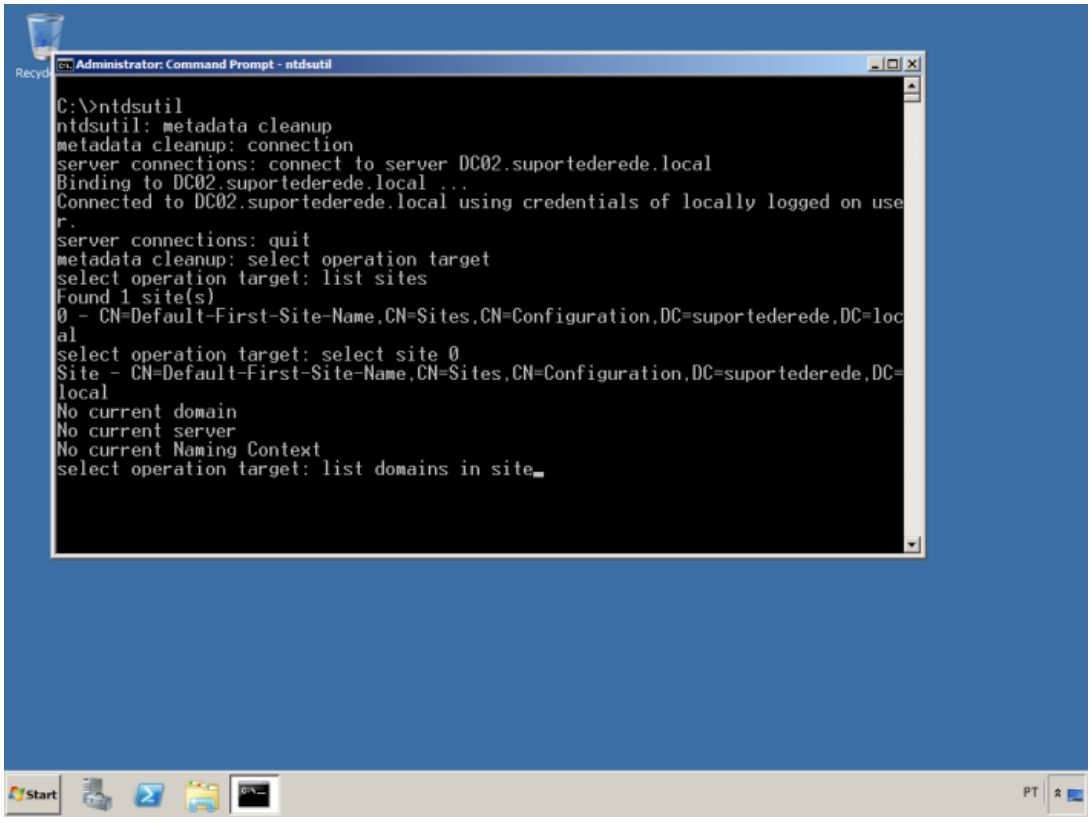
28- Em seguida: **list sites**



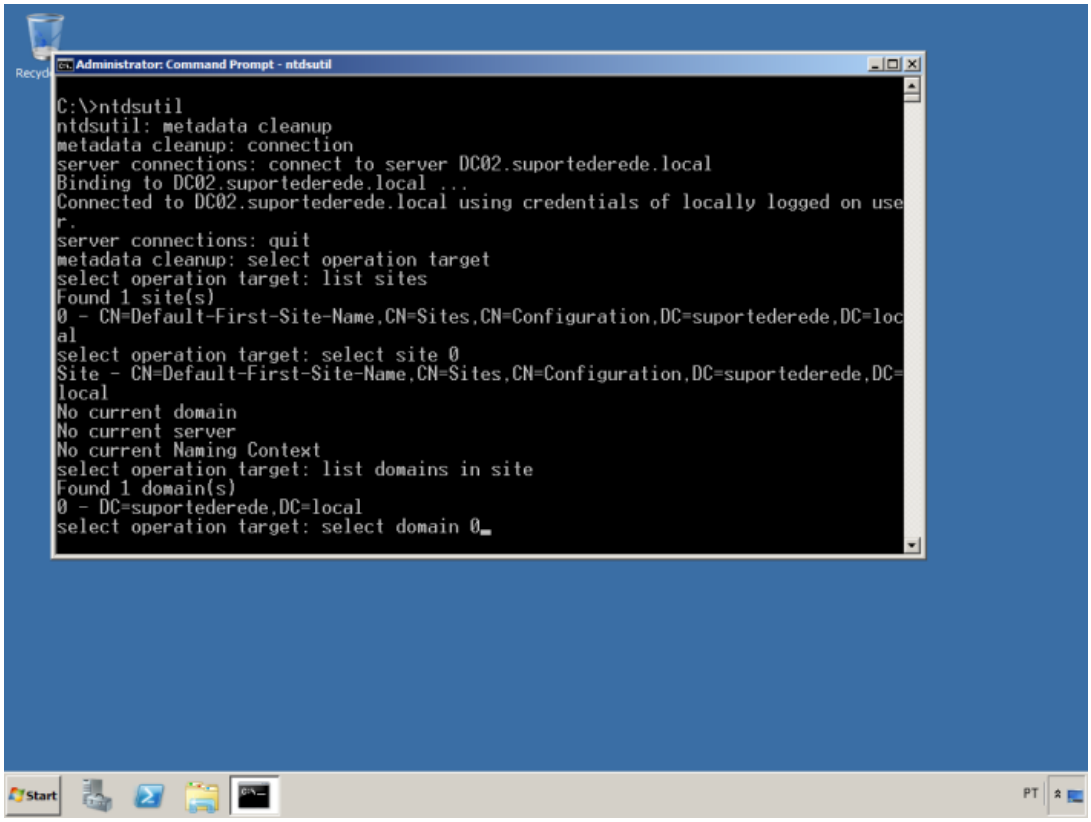
29- Os sites disponíveis serão listados, como temos somente um, verifique que é apresentado um identificador "0" antes do CN, digite: **select site 0**



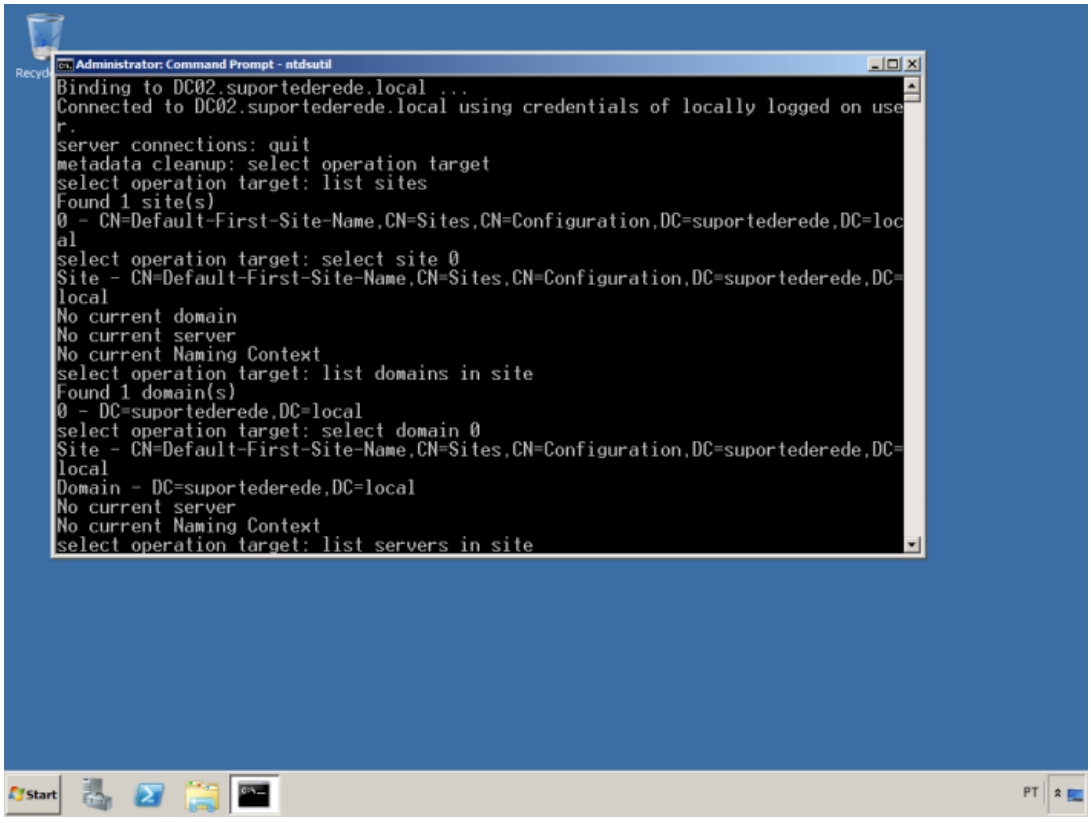
30- Após selecionar o site, é necessário listar os domínios, para isso vamos digitar: **list domains in site**



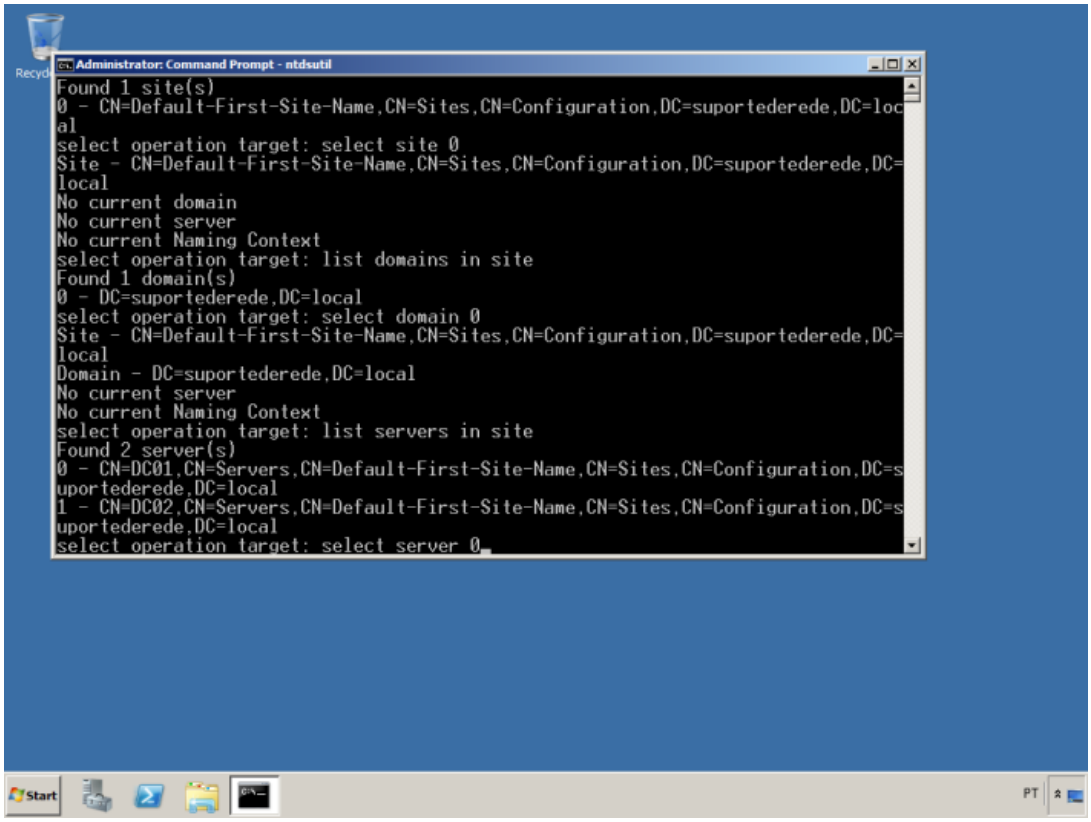
31- Os domínios serão listados, como temos somente um (identificador "0") digite para selecionar: **select domain 0**



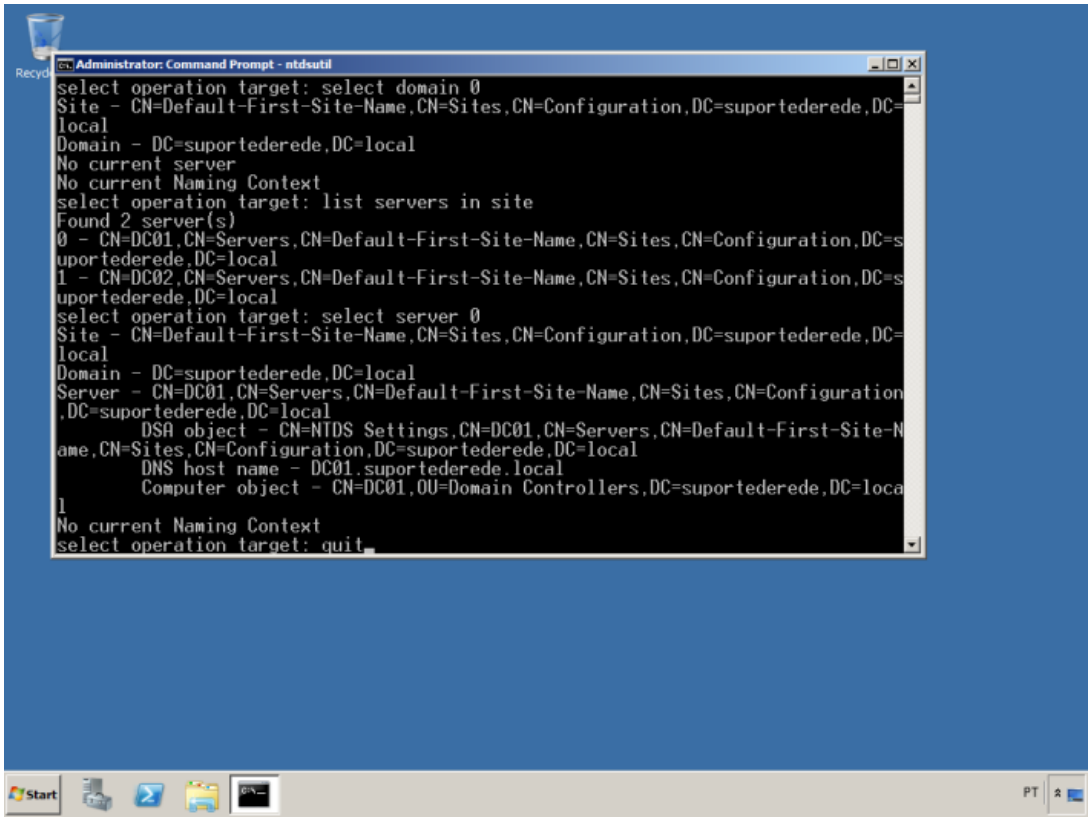
32- Após selecionar o domínio precisaremos listar os servidores, para isso digite: **list servers in site**



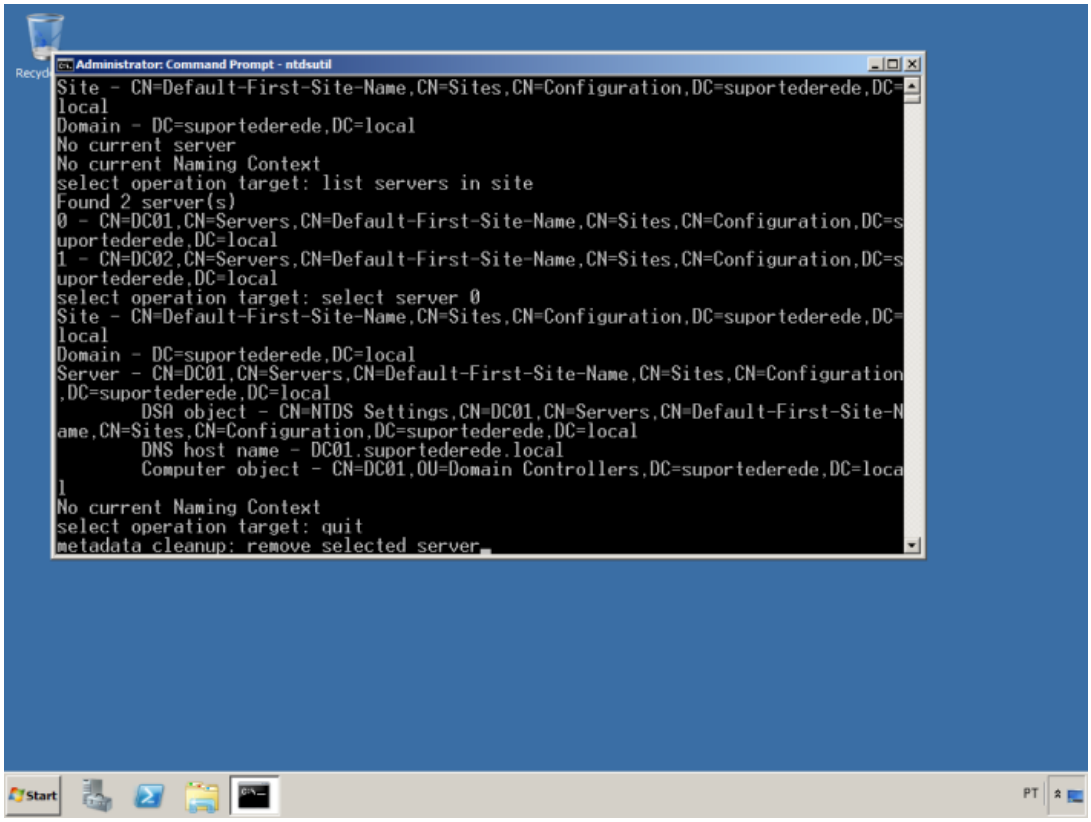
33- Os dois servidores (DC01 e DC02) serão listados, precisamos selecionar o servidor a ser excluído da base, verifique com atenção e digite, fazendo referencia ao identificador do servidor: **select server 0**



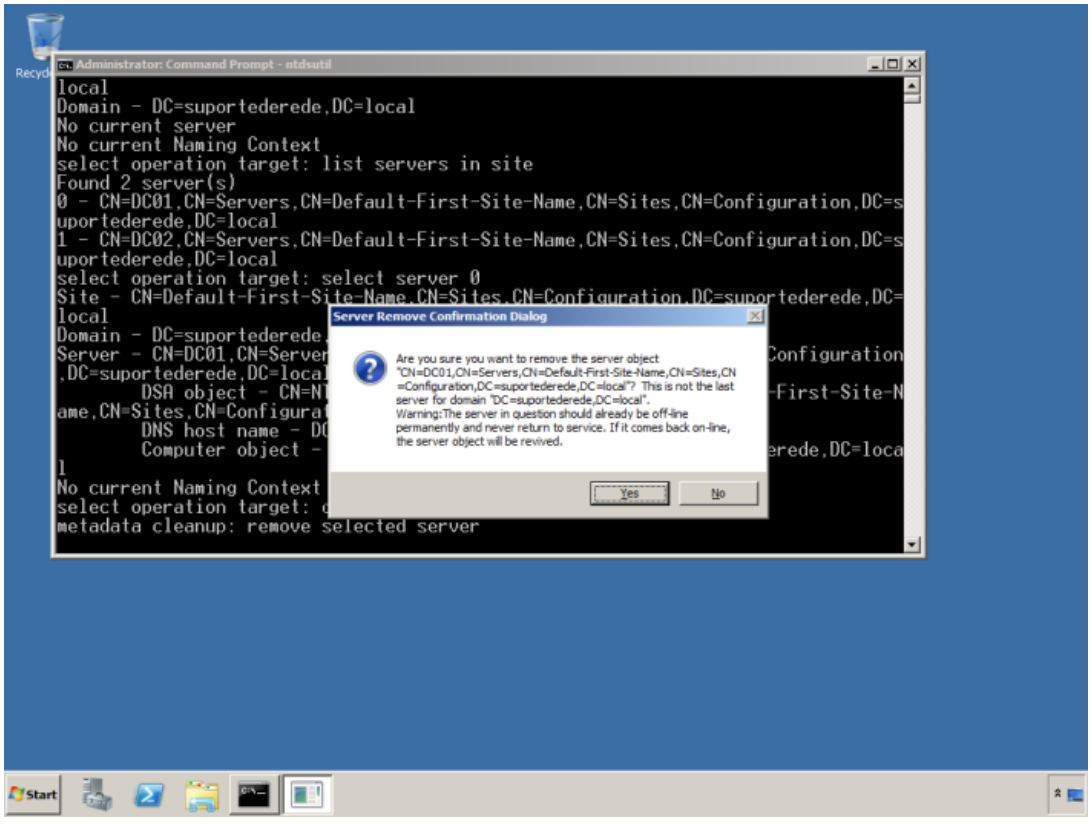
34- Em “select operation target” digite: **quit**



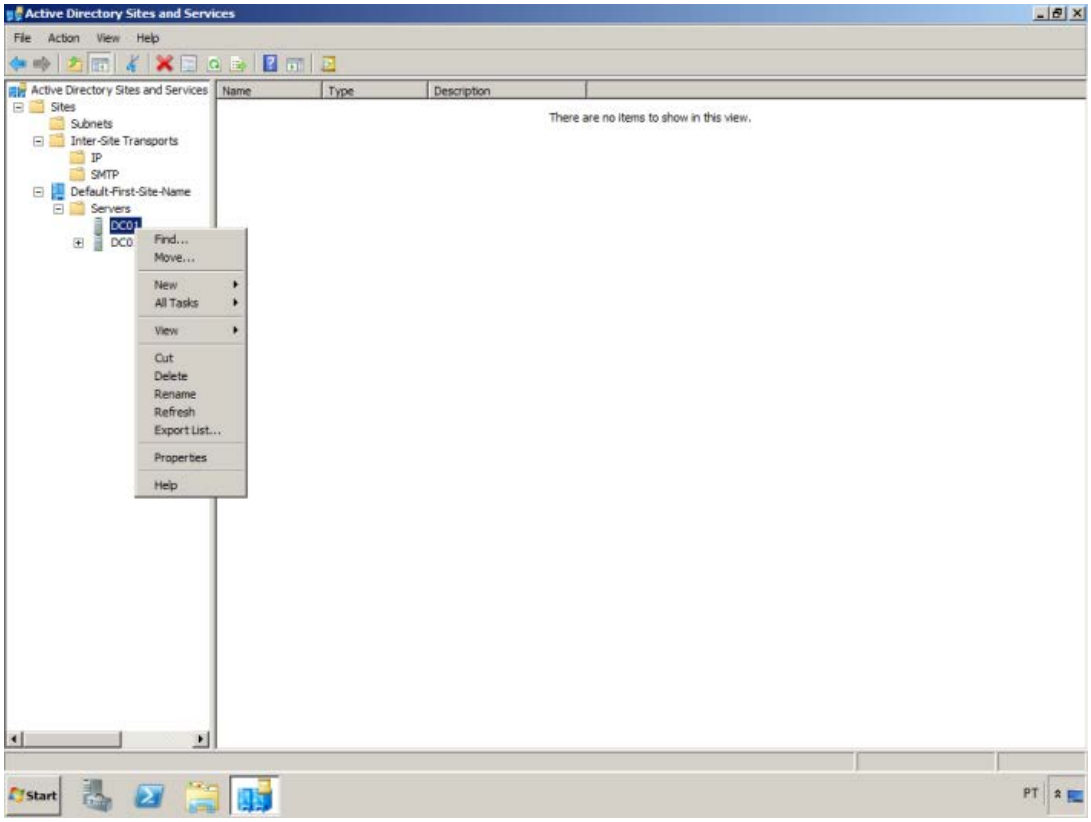
35- Retornando para “metadata cleanup” digite: **remove selected server**



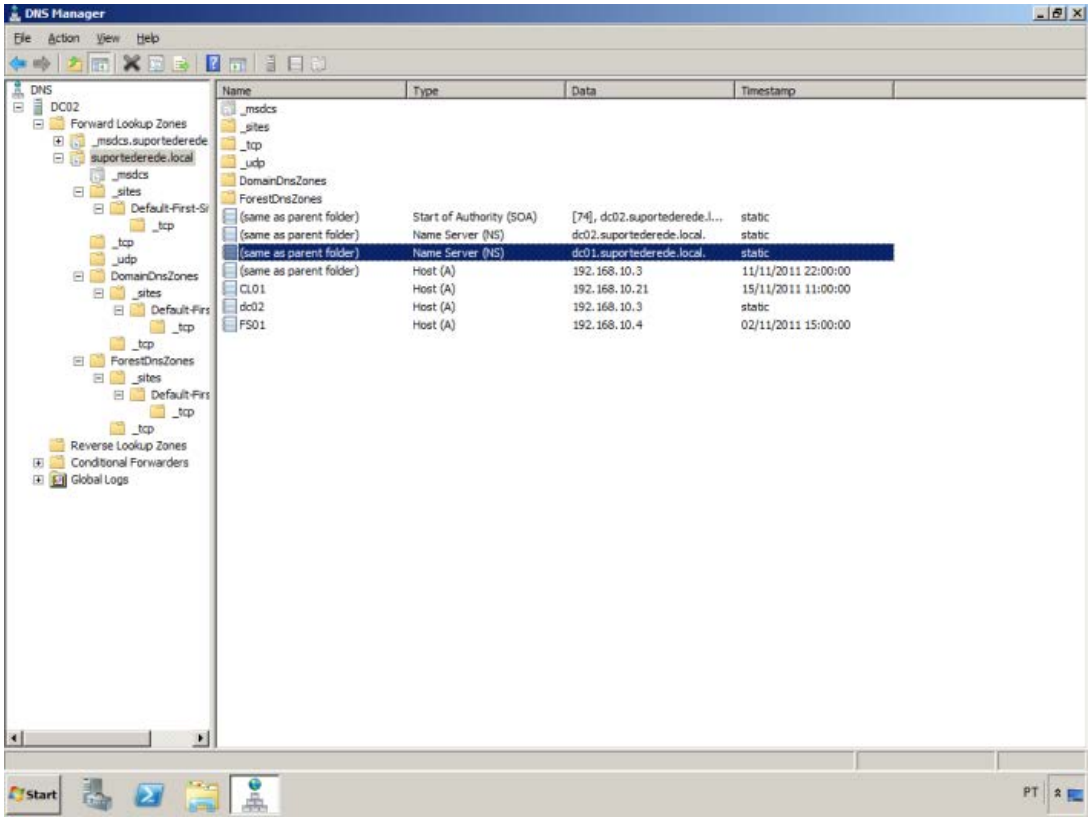
36- Confirme com **Yes** na caixa de diálogo.



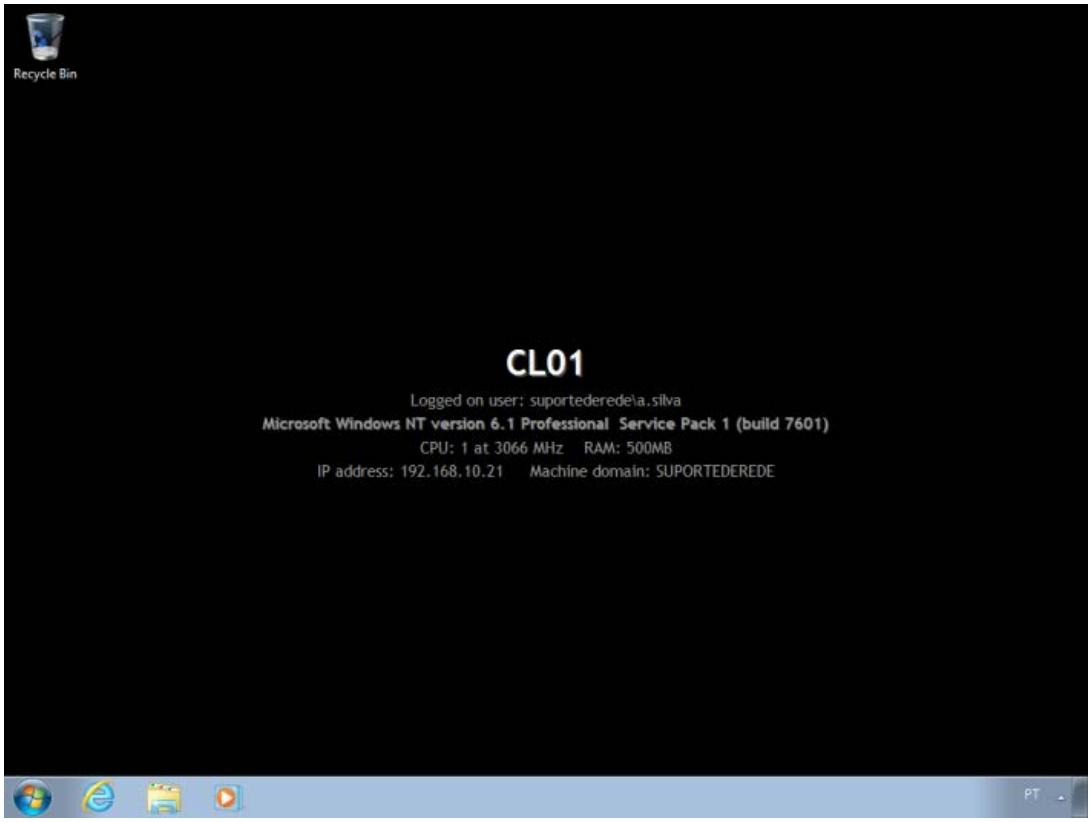
37- A parte mais trabalhosa já foi concluída, agora somente resta algumas verificações e exclusões de referências ao antigo servidor. Acesse o "**Active Directory Sites and Services**" em Start Menu / Administrative Tools. Navegue até Servers e exclua o servidor perdido.



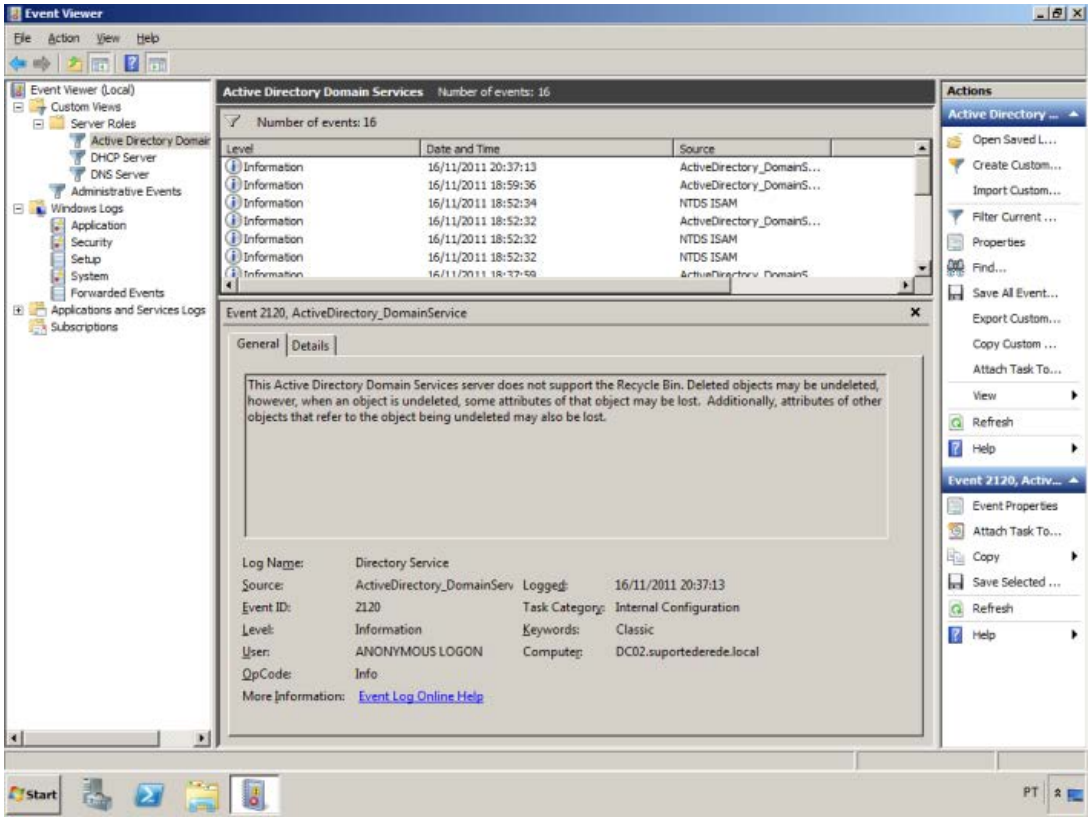
38- O importante é verificar o "**DNS Manager**" se há registros com referência ao servidor, aproveite para certificar se está apontando corretamente os registros SOA / NS / SRV / LDAP para o novo servidor. Todas referências ao servidor antigo deve ser excluída.



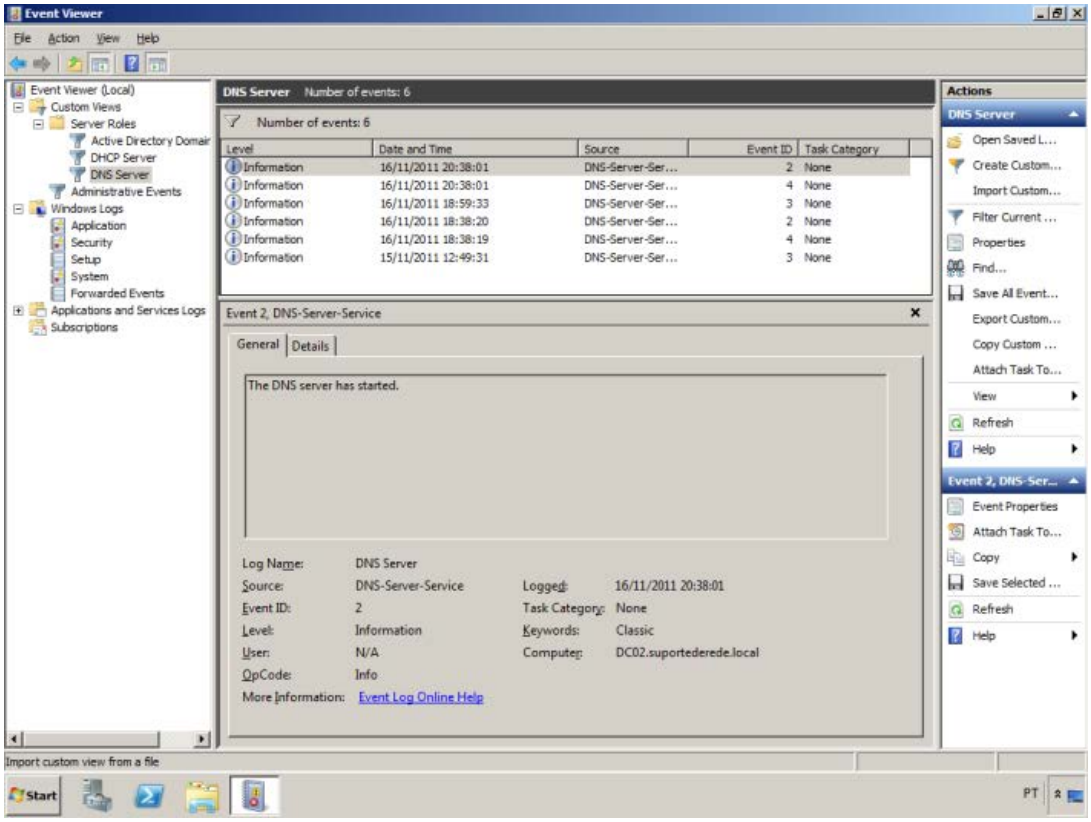
39- Após os procedimentos realizados anteriormente devemos conseguir acessar normalmente o nosso domínio através de nosso client. O que vemos abaixo É o logon de nosso client através de um usuário do Active Directory.



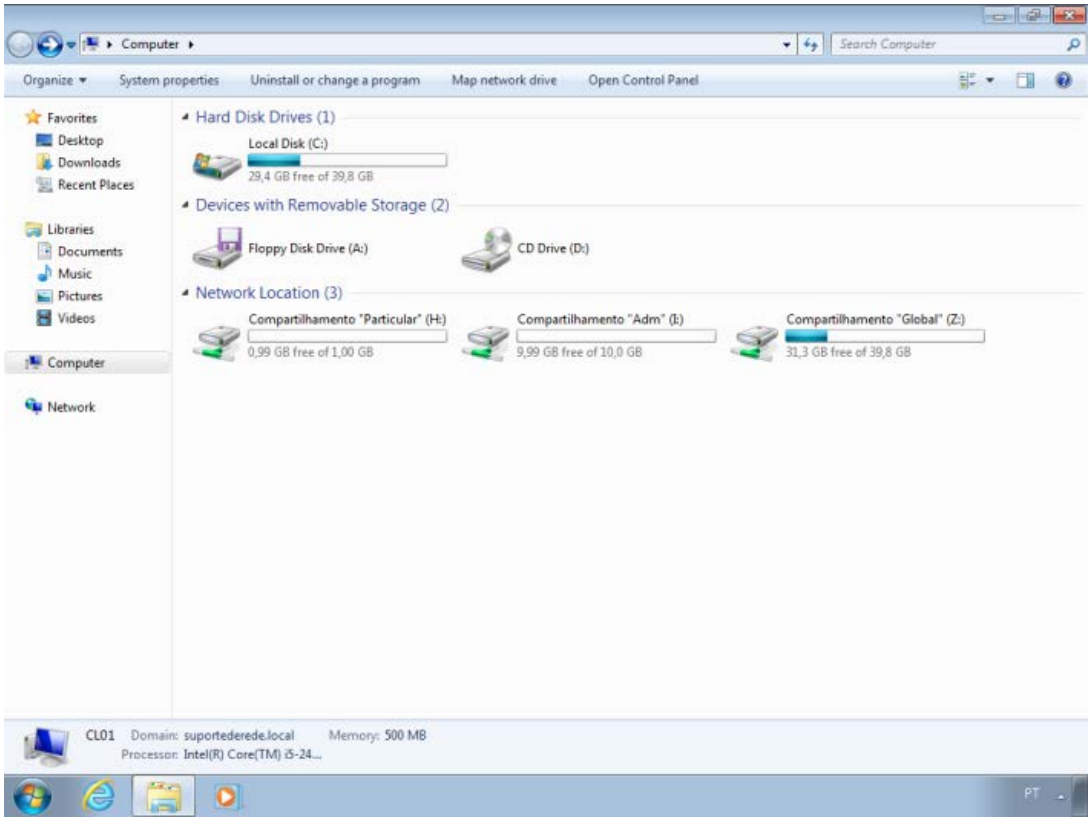
40- Após esses processos é recomendado observar sempre o Event Viewer do DC02 para identificar eventuais falhas e problemas. Abaixo vemos a consulta do “Active Directory Domain Services”.



41- E agora vamos analisar o “DNS Server”. Constatamos que o nosso log (até o presente momento) está sem erros ou alertas o que é muito bom para o êxito de nosso procedimento.



42- No ambiente existia uma Group Policy de mapeamentos, que criava um mapeamento particular / um global e um por departamento, todos fazendo referência aos compartilhamentos / permissões do meu File Server (FS01), verifique abaixo que os mapeamentos foram atribuídos normalmente.



Se tivéssemos um servidor com todas as funções, o tempo de recuperação não seria tão rápido, seria necessário recuperar os backups, verificar permissões, o que com certeza iria estressar a equipe técnica.

Espero que tenham gostado do artigo e torço para que não precisem usar, caso precise espero que seja uma boa referência para consulta.

Abraços a todos

Compartilhe: Email Imprimir Facebook 3 Twitter

Curtir isso: Gosto

Be the first to like this.

« Trocar a senha de administrador de domínio (em caso de perda da mesma)

Como criar um servidor VPN no Windows Server 2008 R2 »

DISCUSSÃO

5 Respostas para “Definir DC secundário como principal em caso de desastres”

Bruno,

Fiz recentemente um procedimento parecido adicionei um WSSTR2 a um Dominio Pai ou Floresta pai como queira WSST e nao deleguei as funçoes Schema, PDC, RID e demais para o novo Servidor o WSSTR2 e estou gerenciando meu ambiente em ambos mas sempre usando mais o novo SRV.
Esse procedimento que você informo pelo que entendi você o fez quando o seu DC1 já não estava no ar por algum problema.
O ambiente que você simulo aí e muito parecido com o meu, ai vem uma pergunta se baseando no ambiente que você apresento.

Eu consigo passa as funçoes Masters para o outro servidor que no caso esta como Filho na floresta sendo que o Dominio principal o servidor nao está no ar ?

E Meus Parabens Muito conteudo bacana no Blog, e este tutorial será de grande importancia para um procedimento que irei efetuar após sua respota.

PUBLICADO POR **ANDRÉ LIMA** | SEXTA-FEIRA, 16 DEZEMBRO 2011, 09:08

REPLY TO THIS COMMENT

Olá **André Lima**, agradeço os elogios ao conteúdo do blog.

Então, referente a sua pergunta, o procedimento demonstrado no artigo é voltado caso o DC principal morra (não existindo nenhuma possibilidade de contato com outros servidores e nem será reintegrado ao domínio).
Esse procedimento serve e atende a sua necessidade.

Recomendo, caso esteja inseguro, faça testes antes em ambientes virtuais.

E mesmo antes de executar em seu ambiente de produção faça um belo backup.

Abraços

PUBLICADO POR **BRUNO FELIPE** | DOMINGO, 18 DEZEMBRO 2011, 22:08

REPLY TO THIS COMMENT

Bom dia Bruno.

Muito bom seu artigo e funcionou direitinho em meu cenário. Só tem um probleminha o meu DC SECUNDARIO é virtualizado no server2008 que é primario, quando transformei o server2012 virtualizado em primario eu não consigo fazer os procedimentos de exclusão do DC antigo eu acredito que este procedimento funciona apenas para quando os servidores são separados e não quando o DC PRINCIPAL TENHA UM SECUNDARIO VIRTUALIZADO NELE MESMO.

O problema é que não estou conseguindo rebaixar o DC que era principal e muito menos exclui-lo do ACTIVE DIRECTORY SITES AND SERVICE, sabe como resolvo este problema?

Sei que o correto é deixar um servidor físico como DC principal e não virtualizar DCS principal, mas precisei fazer isso provisório.

Abs.
Zacheo

PUBLICADO POR **ZACHEO** | SÁBADO, 22 DEZEMBRO 2012, 10:40

REPLY TO THIS COMMENT

Muito bom … parabéns pelo post. Andei lendo bastante coisa em outros blogs e sites, e não achei nada tão completo. Parabéns pelo trabalho.

PUBLICADO POR **EDUARDO POPOVICI** | QUINTA-FEIRA, 06 JUNHO 2013, 10:16

REPLY TO THIS COMMENT

Olá eu sou o Rui Morais sou analista de S.O. aqui em Angola, cara você me safou de uma… Muito obrigado e os meus parabens…

PUBLICADO POR **RUI MORAIS** | SEXTA-FEIRA, 21 JUNHO 2013, 06:05

REPLY TO THIS COMMENT

DEIXE UMA RESPOSTA