

Configuração de AD e GPO

Servidores de Domínio.

Segundo Minasi (2003)¹, um domínio é um grupo de servidores e estações de trabalho que concordam em centralizar os nomes de conta de usuários e máquinas em um banco de dados compartilhado. Isso é muito útil, pois permite que um usuário tenha apenas um nome de conta e senha e utilize-os em dezenas, centenas ou milhares de máquinas dentro do domínio de uma organização. Quando uma empresa contrata um novo funcionário, o administrador poderá criar facilmente uma única conta para esse novo empregado de forma que ele possa acessar imediatamente qualquer sistema da rede. Com a centralização de contas de usuários, computadores e servidores é possível através de ferramentas específicas, estabelecer políticas de grupo para acesso aos recursos da rede.

Para que um domínio exista é necessária a promoção de um computador servidor instalado com o Windows Server 2012 a controlador de domínio. Isso é feito instalando o AD no servidor.

Observação

O AD DS requer que um servidor DNS esteja instalado na rede e com capacidade de atualizações dinâmicas habilitado. Em particular a imagem entregue pelo professor, mesmo depois de instalado o DNS Server na última aula, tem tido problemas para autorizar as atualizações automáticas. Para resolver este problema precisamos criar uma Nova Zona e um registro de Nova Delegação neste domínio. Para tanto vamos seguir os passos indicados.

Entre no Gerenciador de DNS disponível em Ferramentas

Você deve ver a zona minasgerais.net criada.

Agora vamos criar uma nova delegação dentro do domínio minasgerais.net. Da mesma forma que vc criou um registro do tipo A agora ao clicar com o botão direito dentro da zona escolha a opção Nova Delegação. Atribua o nome de Minas a este domínio delegado, conforme figura 2. Ao avançar selecione a opção que permite a atualização dinâmica.

¹ Minasi, Mark. Dominando o Windows 2003: a Bíblia. São Paulo. Pearson.

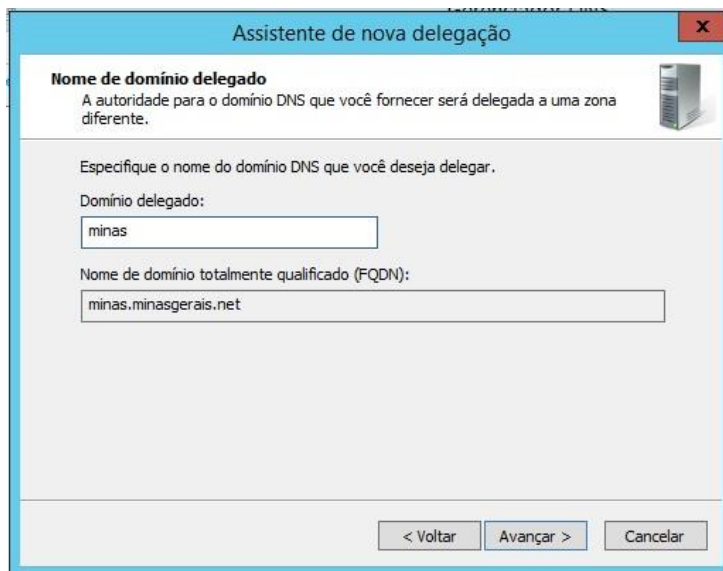


Figura 1. Criando uma Nova Delegação.

Por fim, clique no botão adicionar da figura 3 e digite o nome do servidor (server2012.minasgerais.net) como apresentado na figura 4. Termine o processo de criação da nova delegação concluindo as caixas de diálogos que serão apresentadas.

Reinicialize o servidor para ter certeza que as alterações irão surtir efeito.

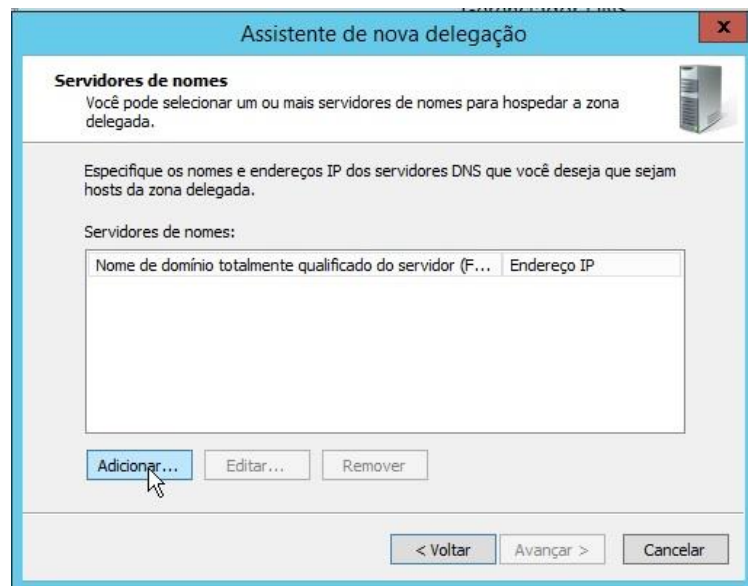


Figura 2. Indicando o Servidor que possui a Nova Delegação.

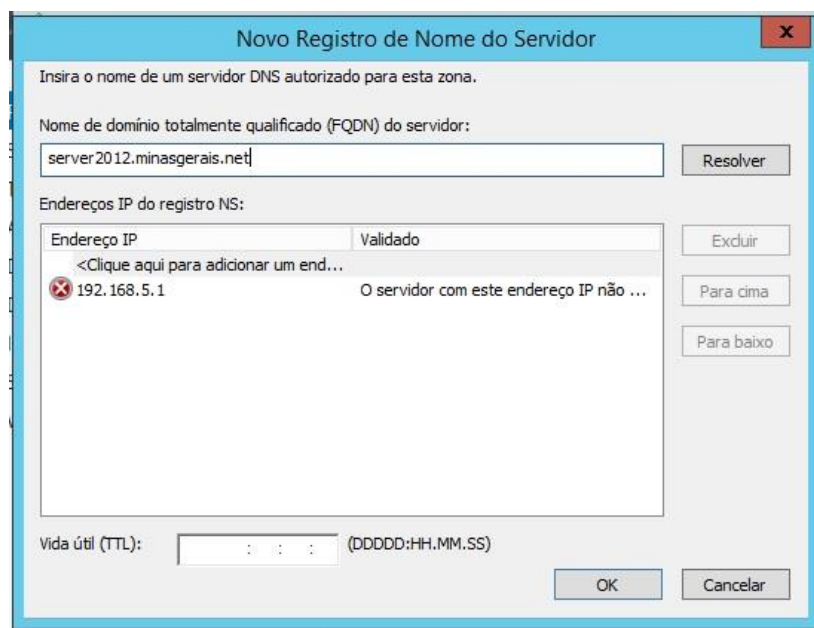


Figura 3. Identificando o Domínio Qualificado

Além de criar a delegação, certifique-se que a zona minasgerais.net está apta a receber atualizações dinâmicas seguras ou inseguras.

minasgerais.net Properties

?

X

Name Servers	WINS	Zone Transfers
General		
Start of Authority (SOA)		
Status: Running	Pause	
Type: Primary	Change...	
Replication: Not an Active Directory-integrated zone	Change...	
Zone file name:		
minasgerais.net.dns		
Dynamic updates:	Nonsecure and secure	
<div><div>⚠</div><div>Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.</div></div>		
To set aging/scavenging properties, click Aging.	Aging...	

OK

Cancel

Apply

Help

Para instalar o AD DS:

No Windows Server 2012, é possível adicionar a função de servidor do controlador de domínio do Active Directory de forma interativa, iniciando os Assistentes de Instalação de Serviços.

- Vá até o gerenciador do servidor e painel. (Figura 5 e 6)
- Clique em **Adicionar Funções e recursos**. (Figura 7)

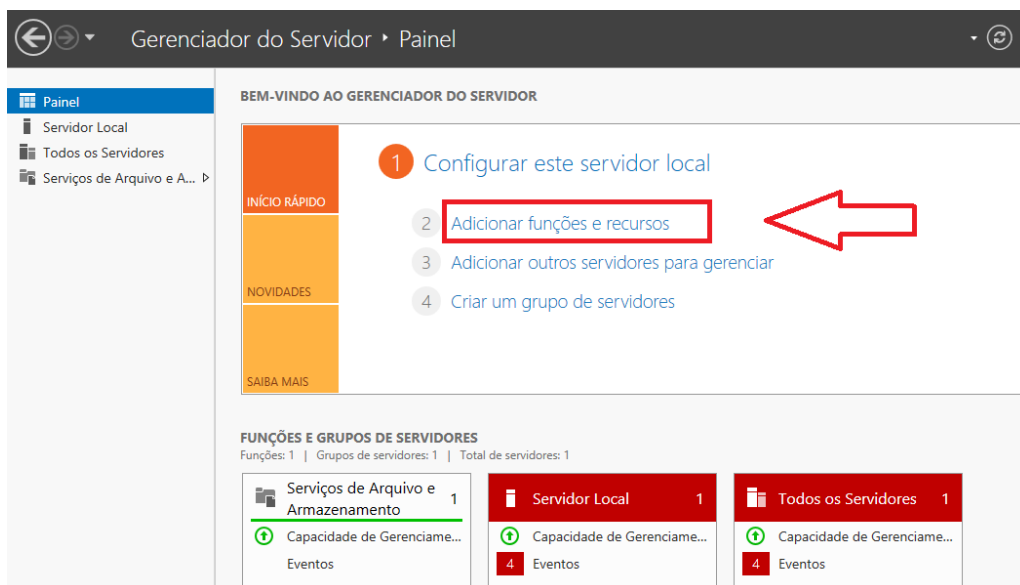


Figura 4. Acesso ao gerenciador de Servidores

Escolha a opção instalação baseada em função ou recurso.

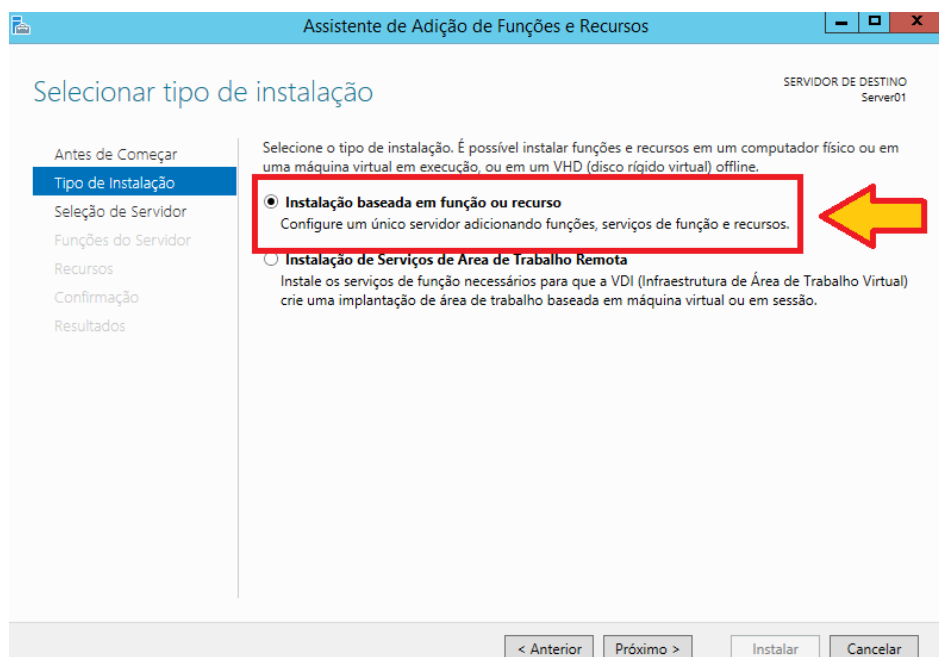


Figura 5. Acesso ao Gerenciador de Servidores

Escolha o Servidor e clique em próximo.

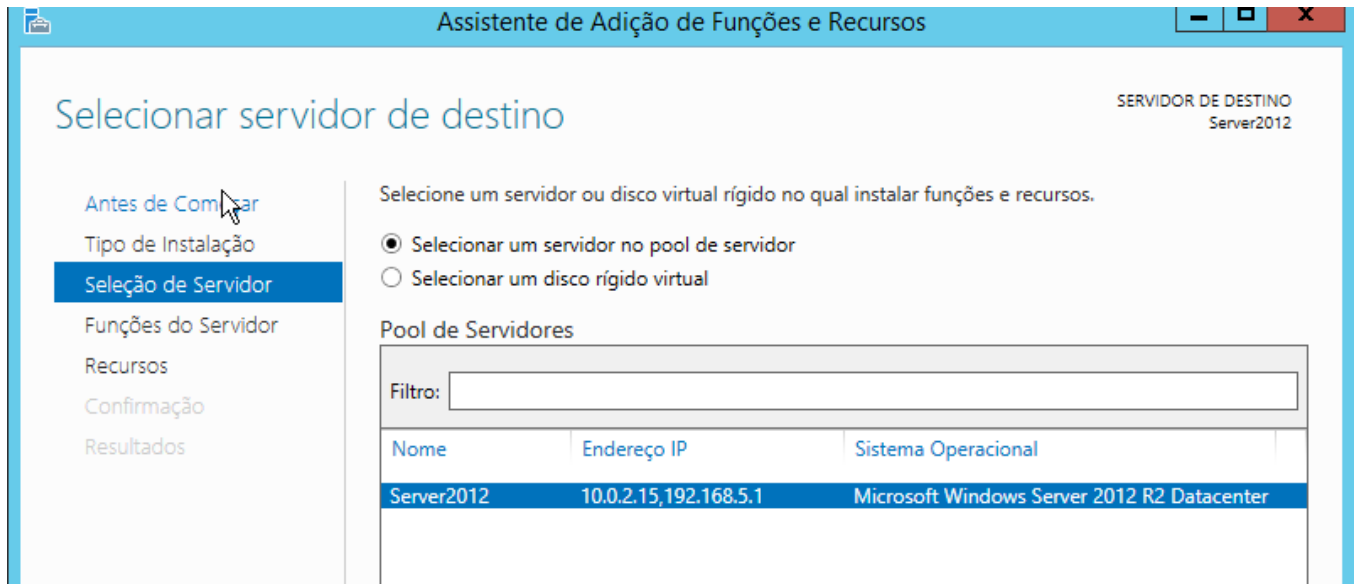


Figura 6. Escolha do Servidor

Escolha os Serviços de Domínio do Active Directory. (AD DS)

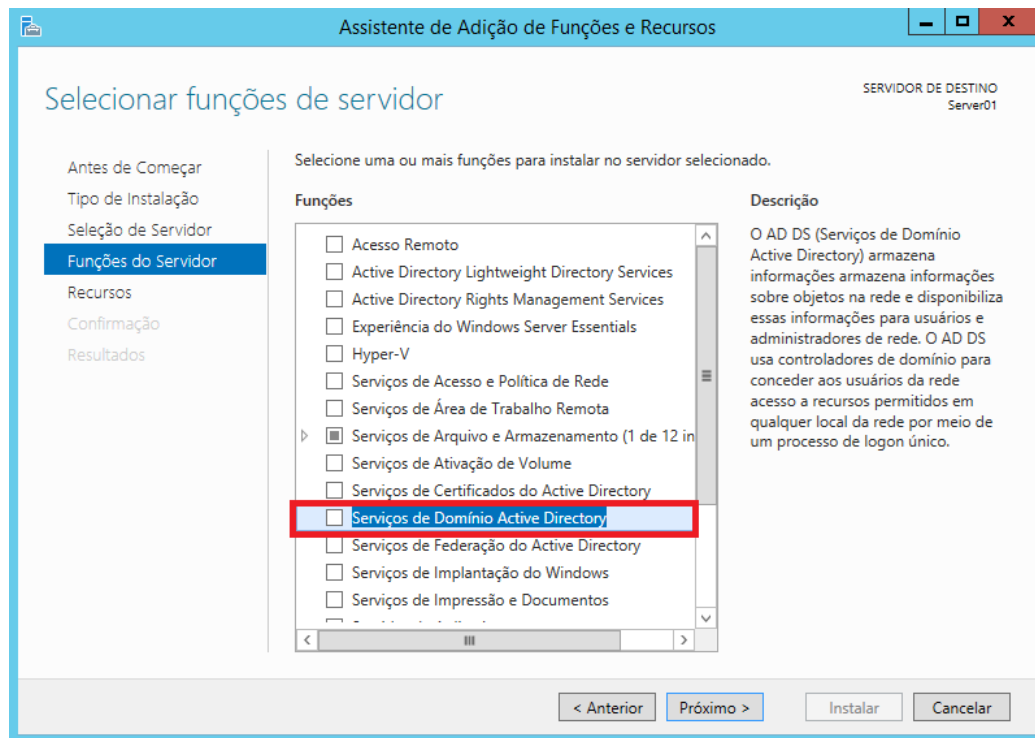


Figura 7. Escolha do Serviço de Domínio AD

O assistente solicitará a instalação de recursos adicionais e necessários para o funcionamento do AD. Clique em adicionar recursos.

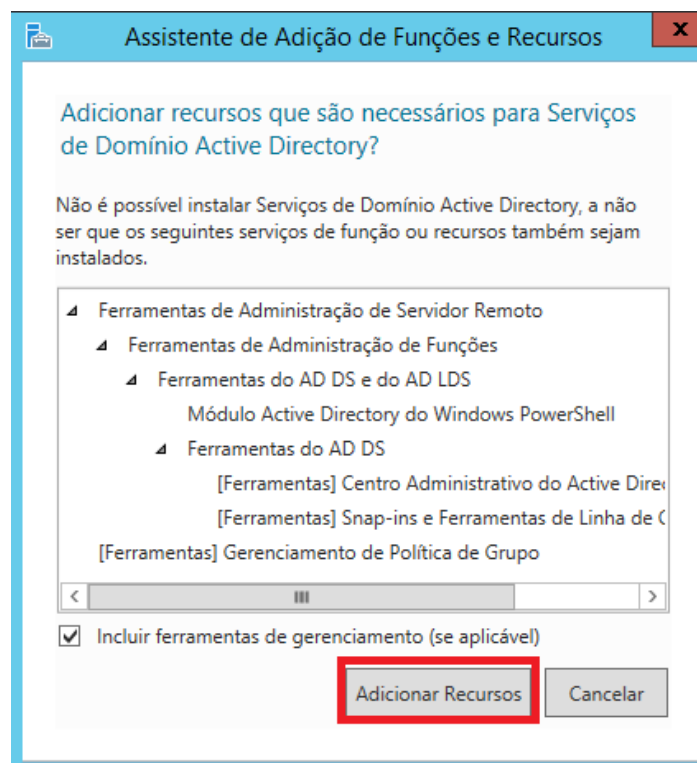


Figura 8. Adição de Recursos

Não é necessário adicionar outros recursos. Clique em próximo.

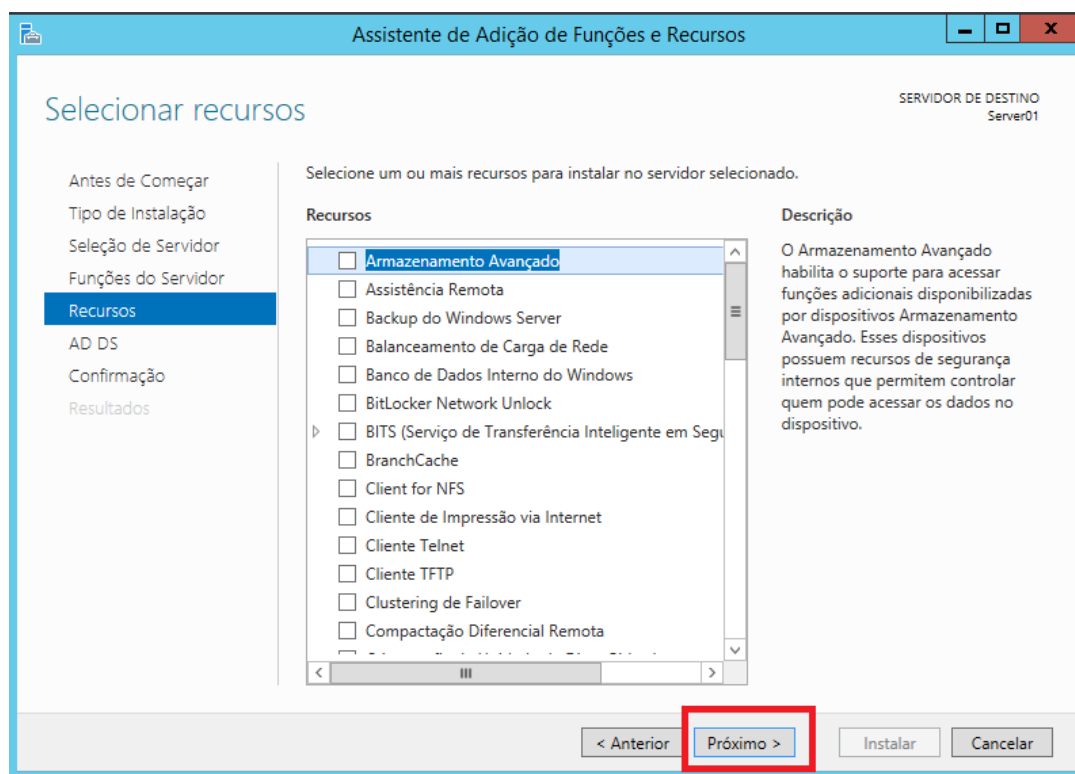


Figura 9. Tela para adição de outros recursos do servidor

O assistente mostrará quais recursos irá instalar. Basta clicar em Instalar.

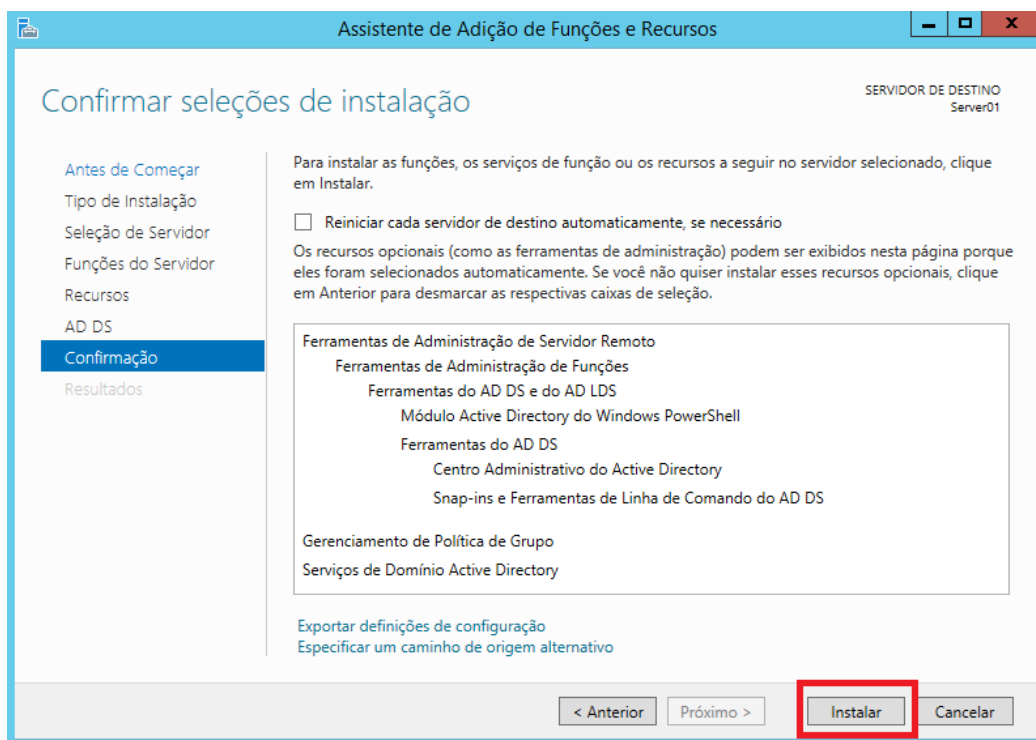


Figura 10. Tela de instalação do AD DS

O assistente do AD iniciará a instalação, este estágio deverá demorar vários minutos.

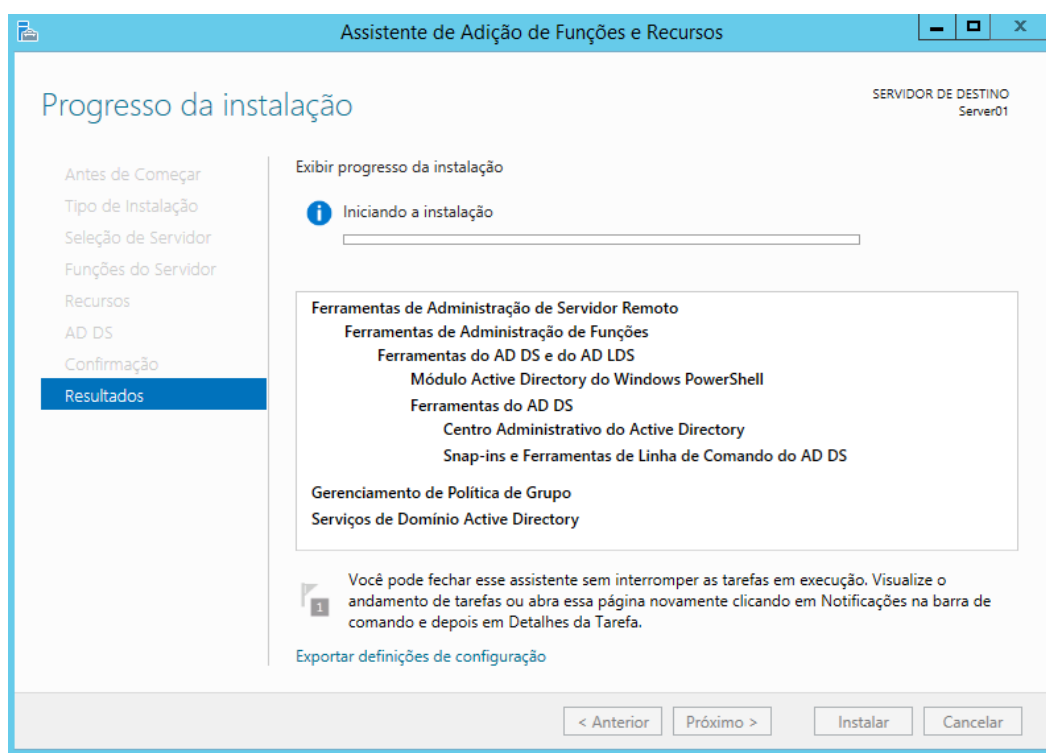


Figura 11. Instalação do AD DS

O assistente para Adicionar Funções **apenas instala os arquivos necessários para instalar e configurar o AD DS em um servidor**, mas não inicia a sua instalação. Quando o Assistente para Adicionar Funções for concluído, clique no símbolo que contém o sinal de exclamação para promover o servidor a controlador de domínio. Veja figura 13.

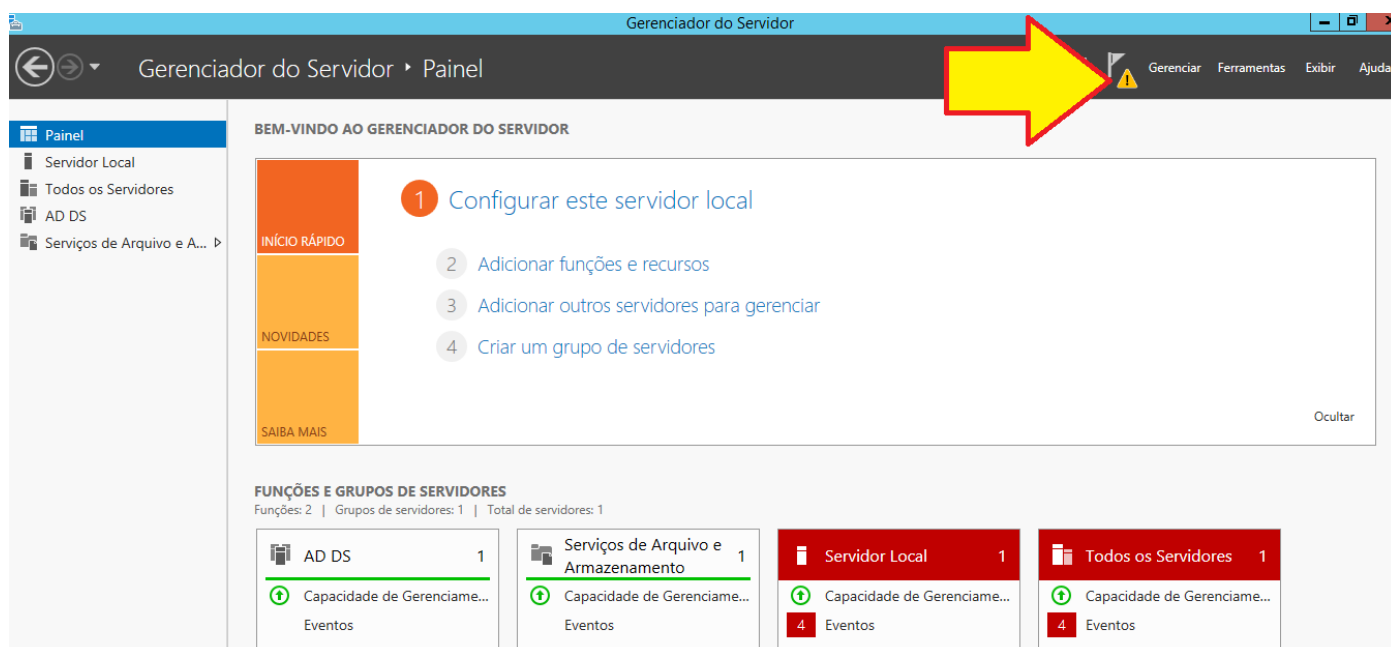


Figura 12. Link para configuração do AD.

Clique no link promover este servidor a um controlador de domínio.

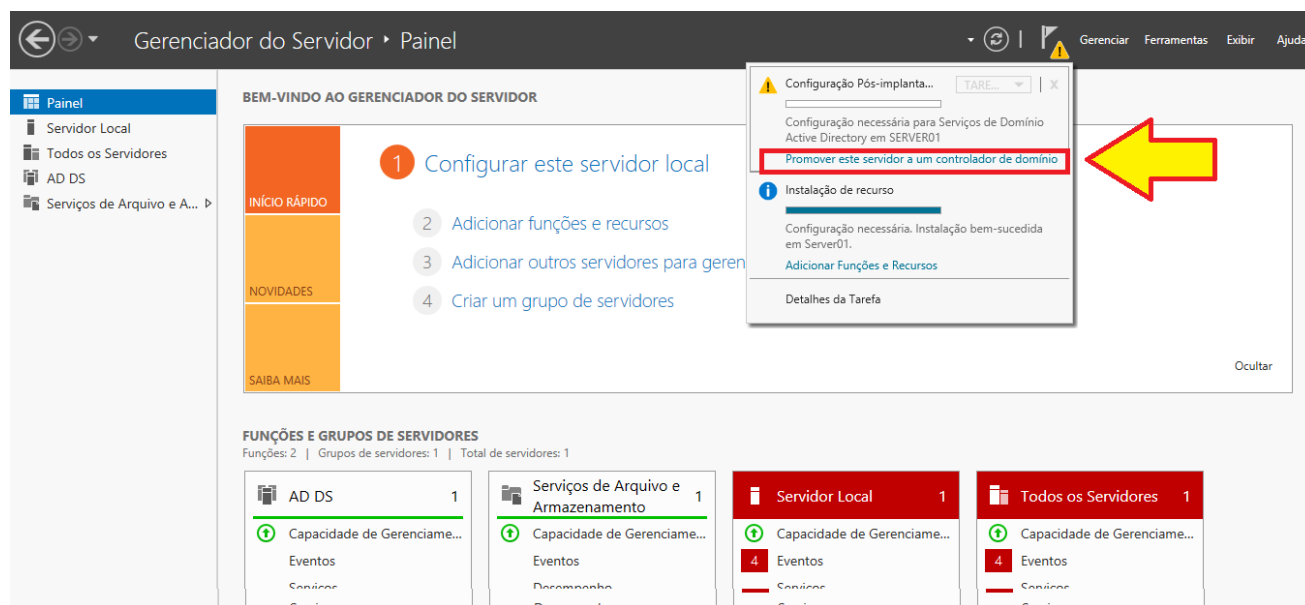


Figura 13. Link para configuração do AD

O AD do Windows considera que as empresas que precisavam de múltiplos domínios tendiam a construir hierarquias de domínios, chamadas de estruturas de árvores. A Microsoft projetou o AD para usar o DNS como sistema de nomeação, e o DNS é hierárquico por natureza. O primeiro domínio do AD é chamado de raiz da árvore. Quando dois ou mais domínios estabelecem uma relação de confiança, uma floresta é criada (Minasi, 2003).

Em adição de uma nova floresta. Entre com o nome **minasgerais.net** para o nome do domínio raiz.

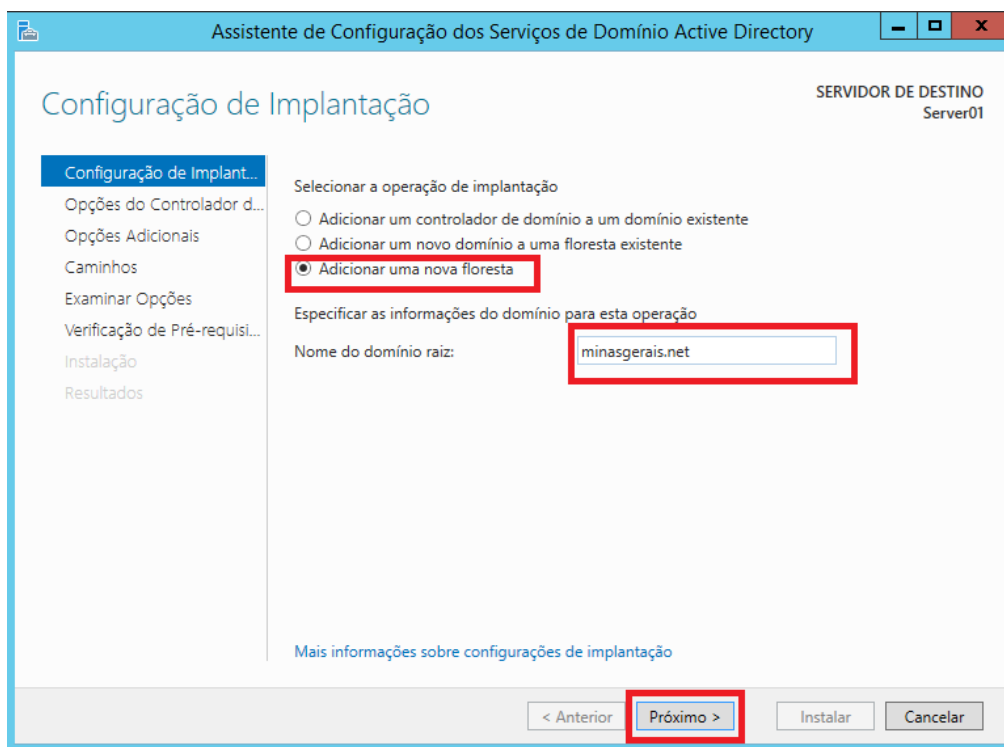


Figura 14. Adição de uma nova floresta

Em um determinado momento da instalação, será solicitada a escolha do nível funcional do domínio. Os níveis funcionais determinam os recursos dos Serviços de Domínio Active Directory (AD DS) que estão habilitados em um domínio ou floresta. Eles também restringem os sistemas operacionais Windows Server que podem ser executados em controladores de domínio na floresta ou no domínio. **Entretanto, os níveis funcionais não afetam os sistemas operacionais que podem ser executados em estações de trabalho e servidores membros associados à floresta ou ao domínio.**

Quando você criar um novo domínio ou uma nova floresta, defina os níveis funcionais do domínio e da floresta com os valores mais altos que você sabe que seu ambiente pode suportar. Desse modo, você poderá aproveitar os recursos do AD DS o máximo possível. Por exemplo, se você tem certeza de que nenhum controlador de domínio que é executado no Windows Server 2008 (ou em qualquer sistema operacional anterior) será adicionado ao domínio ou à floresta, selecione o nível funcional do Windows Server 2012. Por outro lado, se for possível que você retenha ou adicione controladores de domínio que sejam executados no Windows Server 2008 ou versão anterior, selecione o nível funcional do Windows Server 2008 durante a instalação. Você pode elevar o nível funcional após a instalação, quando tiver certeza de que nenhum controlador de domínio será adicionado ou ainda está em uso. Não é possível diminuir um nível funcional.

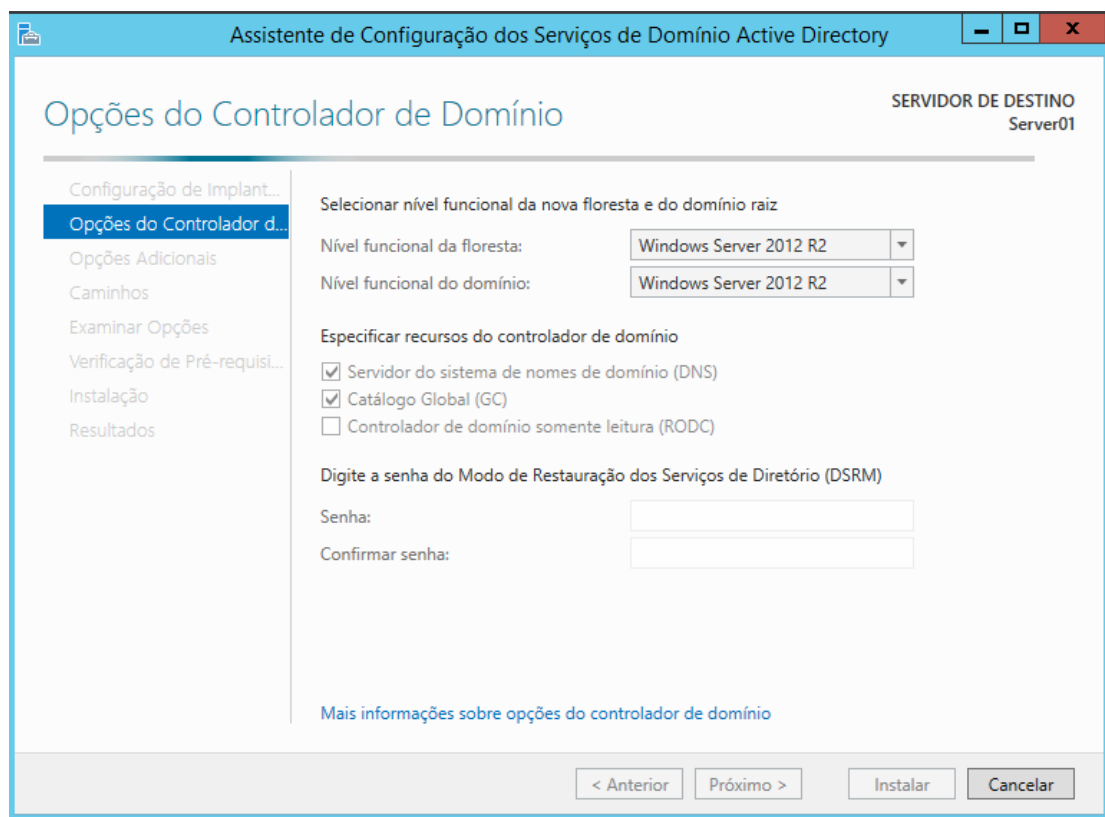
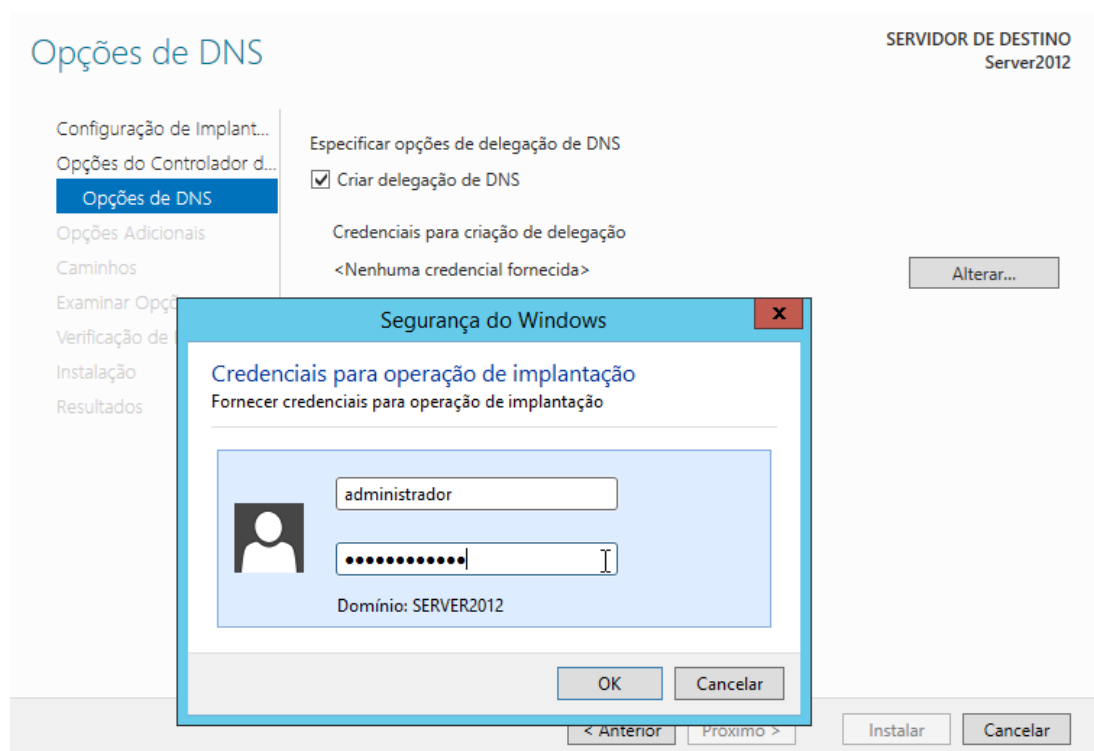


Figura 15. Seleção do nível funcional da rede.

Na caixa de diálogo da seleção do nível funcional da rede (Figura 16), você deve cadastrar a senha, use a **Redes2018** ou Redes2020 se vc fez a alterações como recomendei no vídeo.

Na tela seguinte vc deve clicar no botão Alterar para dar entrada na conta do Administrador e sua senha, se aparecer uma mensagem de warning informando que não foi possível contato com o serviço de DNS significa que vc ainda não habilitou o DNS para receber atualizações dinâmicas.



O assistente mostrará o nome netbios (necessário para redes Microsoft antigas) do domínio.

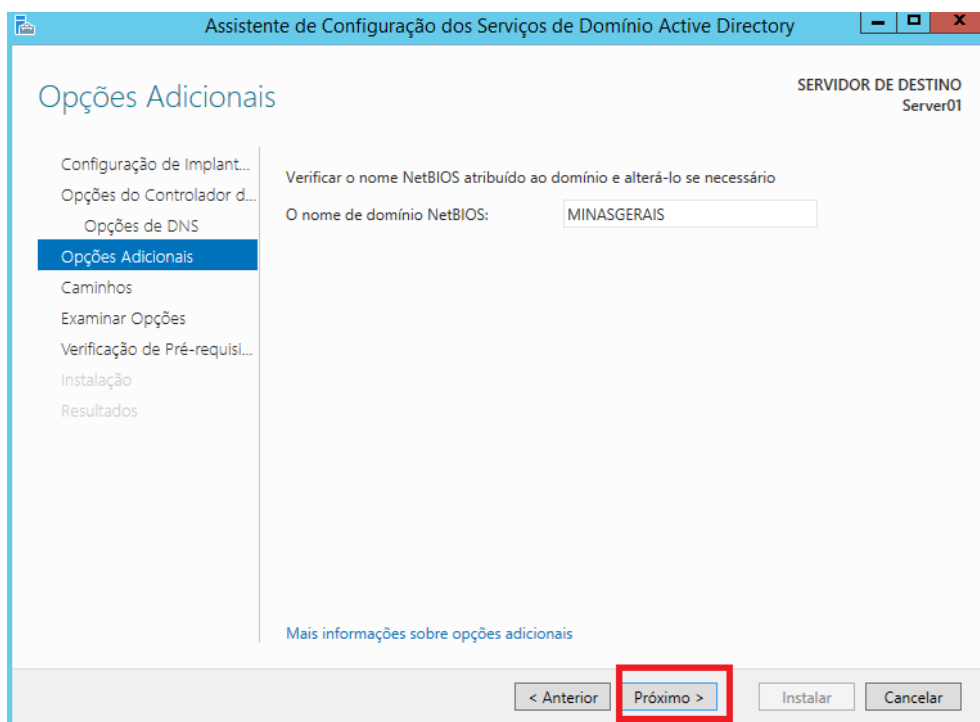


Figura 16. Nome Netbios do domínio

Será informado o local de armazenamento do banco de dados do AD. A recomendação é que eles fiquem em um HD diferente do HD do sistema operacional. Na nossa prática não faremos alteração no caminho padrão.

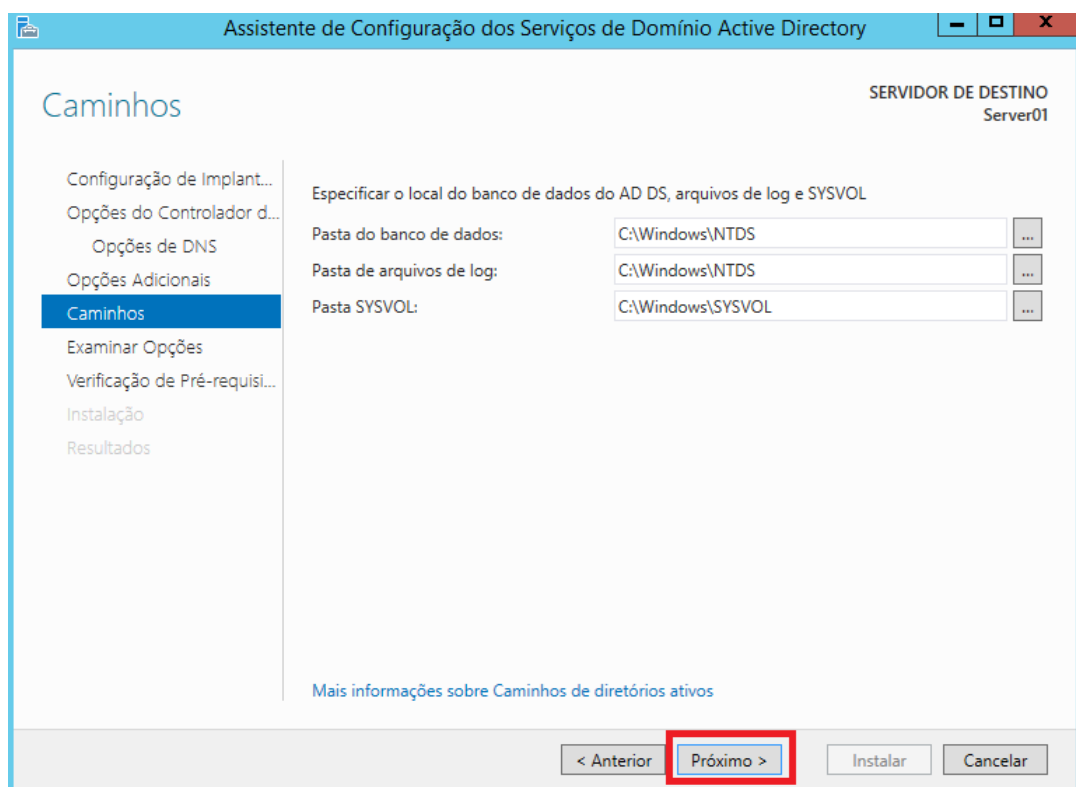


Figura 17. Local de armazenamento dos arquivos de banco de dados do AD.

O assistente mostrará uma tela de verificação de pré-requisitos. Clique em instalar.

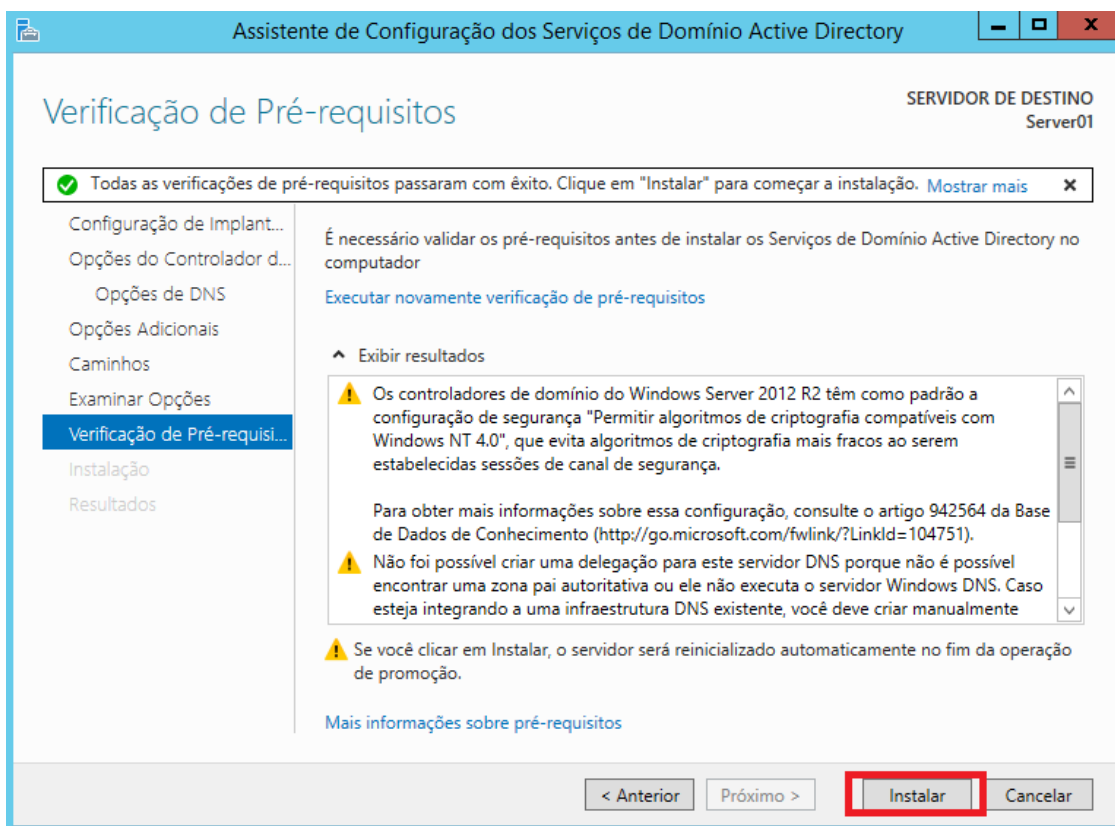


Figura 18. Tela de verificação de pré-requisitos do AD.

Após a instalação e reinicialização do Servidor, vá no menu iniciar e ferramentas administrativas.

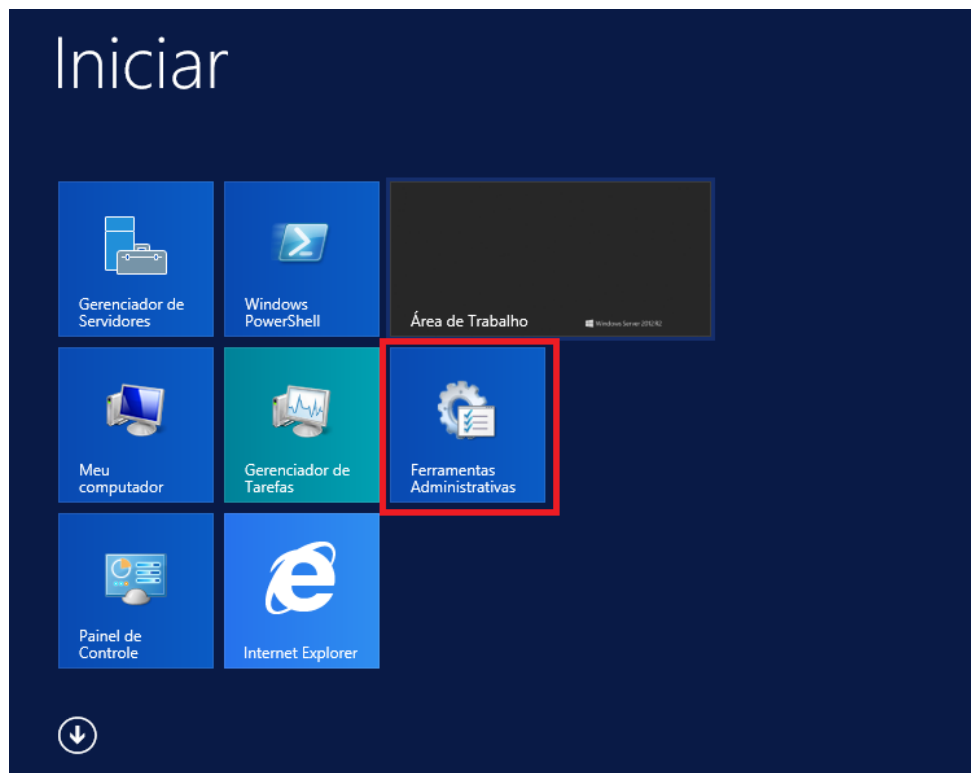


Figura 19. Menu iniciar e Ferramentas Adminsitrativas.

Após a instalação do AD, note que a pasta das **ferramentas administrativas** apresenta novas funcionalidades, como **Usuários e Computadores do AD** e **Gerenciamento de Política de Grupo**. A ferramenta Usuários e Computadores do AD permite ao administrador manipular os

containers do domínio como as unidades organizacionais, incluir, excluir e alterar os usuários dos domínios.

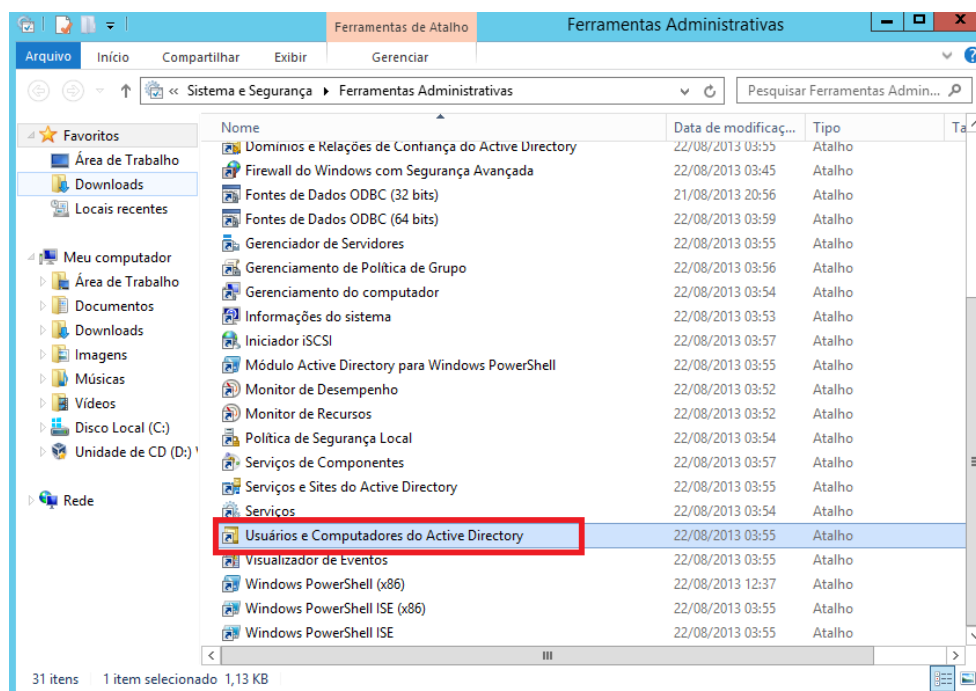


Figura 20. Ferramenta Usuários e computadores do AD.

Em usuários e computadores do AD expanda o domínio minasgerais.net. Clique com o botão direito no nome do domínio e clique em novo e unidade organizacional.

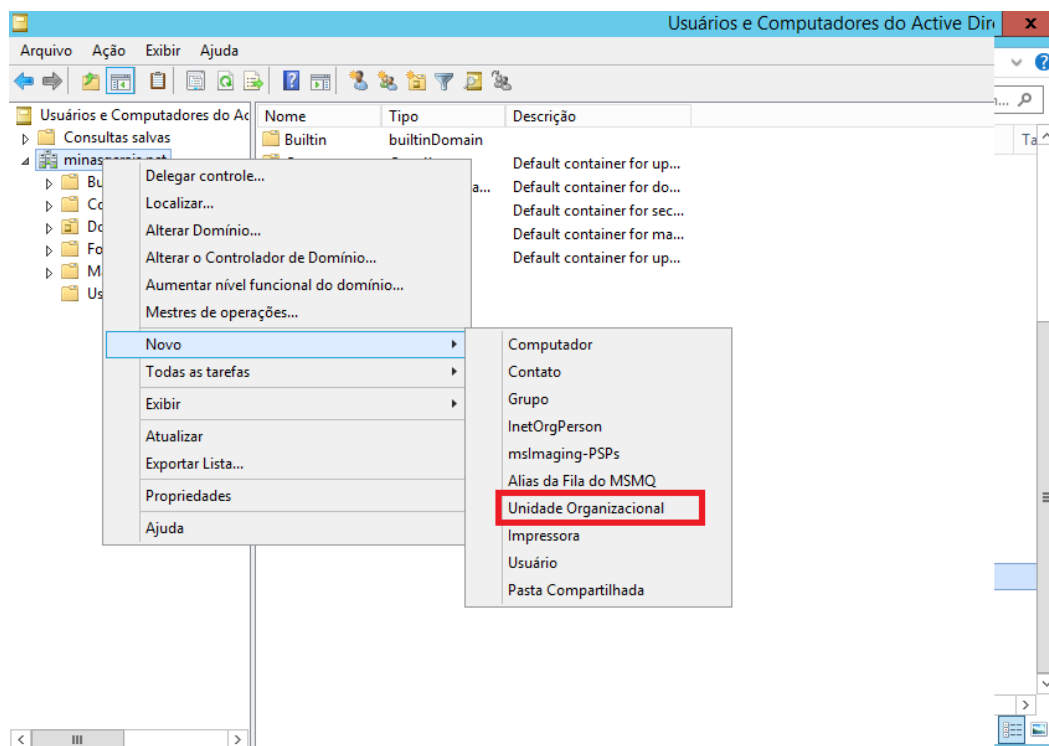


Figura 21. Criação de uma Unidade Organizacional (UO).

A **unidade organizacional**² é um tipo particularmente útil de objeto de diretório contido em domínios. As unidades organizacionais são recipientes do Active Directory nos quais você pode inserir usuários, grupos, computadores e outras unidades organizacionais. Ela é uma divisão lógica do domínio que serve para organizar os objetos do domínio, permite a delegação de controle administrativo e permite o gerenciamento de recursos agrupados

Crie uma estrutura de empresa fictícia com filiais em BH, Betim e Contagem conforme a figura 23.

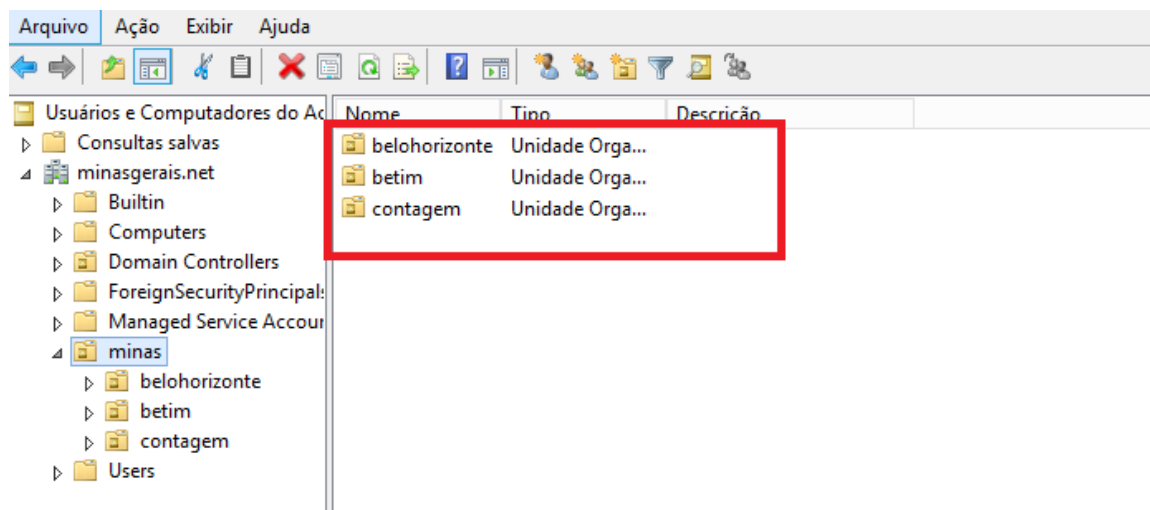


Figura 22. Criação da estrutura organizacional da empresa

Dentro das filiais, crie as UOs computadores e usuários.

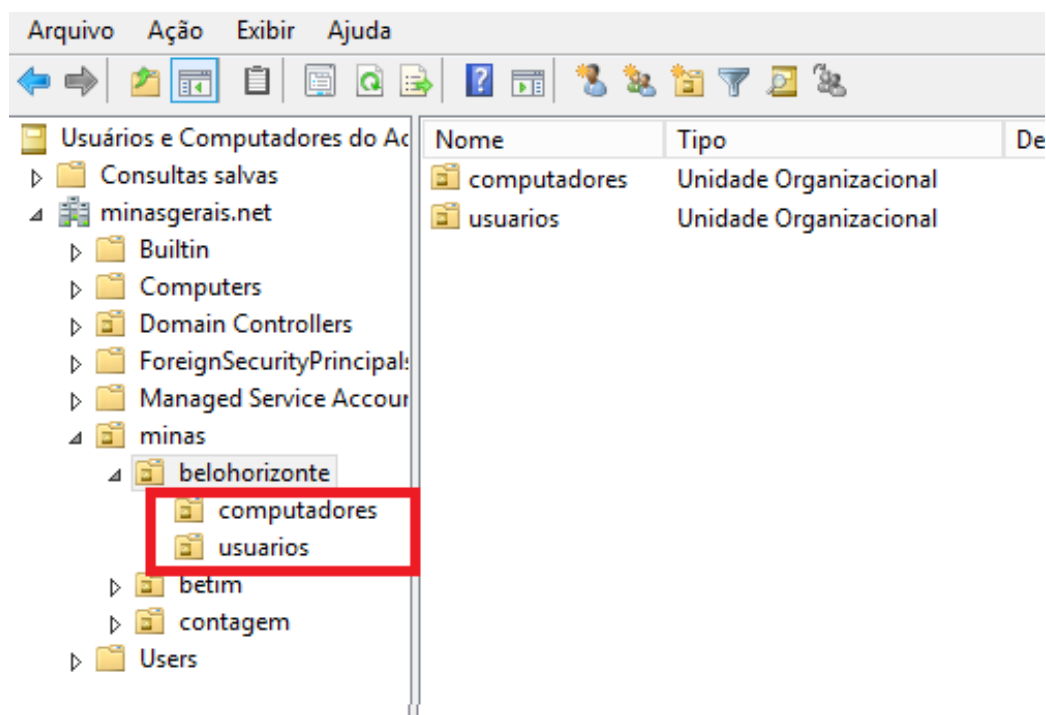


Figura 23. Criação da estrutura organizacional da empresa

Dentro da UO usuários de Belo Horizonte, crie um usuário.

² [http://technet.microsoft.com/pt-br/library/cc758565\(v=ws.10\).aspx](http://technet.microsoft.com/pt-br/library/cc758565(v=ws.10).aspx)

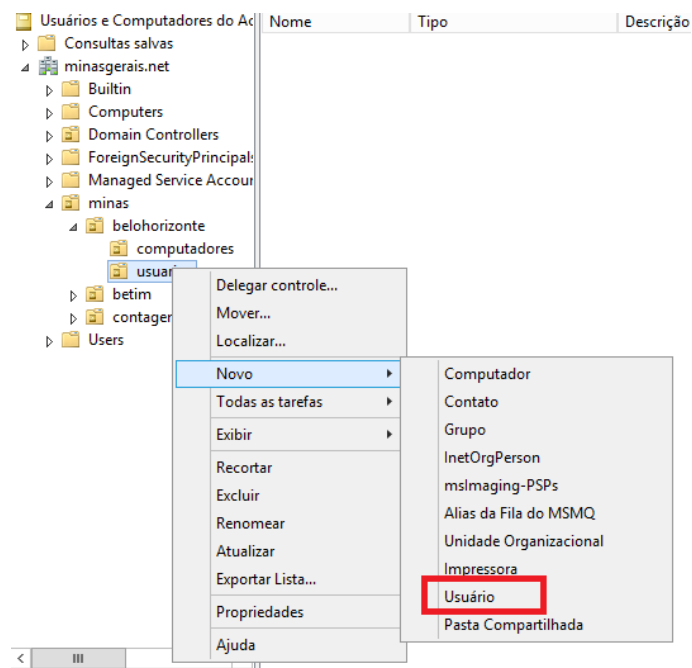
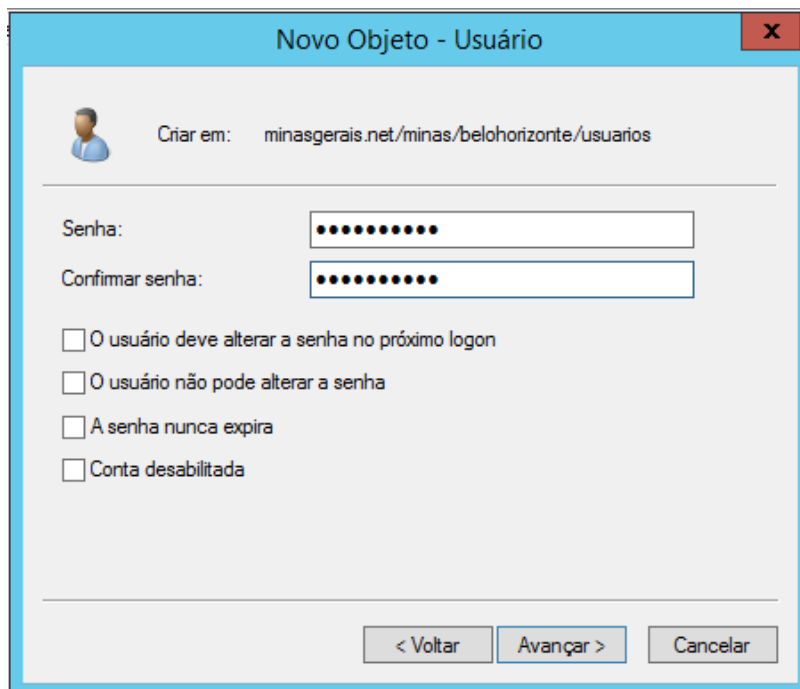


Figura 24. Criação de usuários

Figura 25. Criação de usuário

Entre com a senha **redes@2020** e desmarque as opções como na figura 27 para evitar o pedido de troca de senha no próximo login.



Novo Objeto - Usuário

Criar em: minasgerais.net/minas/belohorizonte/usuarios

Senha: [password field]

Confirmar senha: [password field]

☐ O usuário deve alterar a senha no próximo logon
☐ O usuário não pode alterar a senha
☐ A senha nunca expira
☐ Conta desabilitada

< Voltar Avançar > Cancelar

Figura 26. Criação de Usuário

Após a criação do usuário, clique com o botão direito no usuário e vá em propriedades. Verifique se as abas abaixo conferem com a sua configuração.

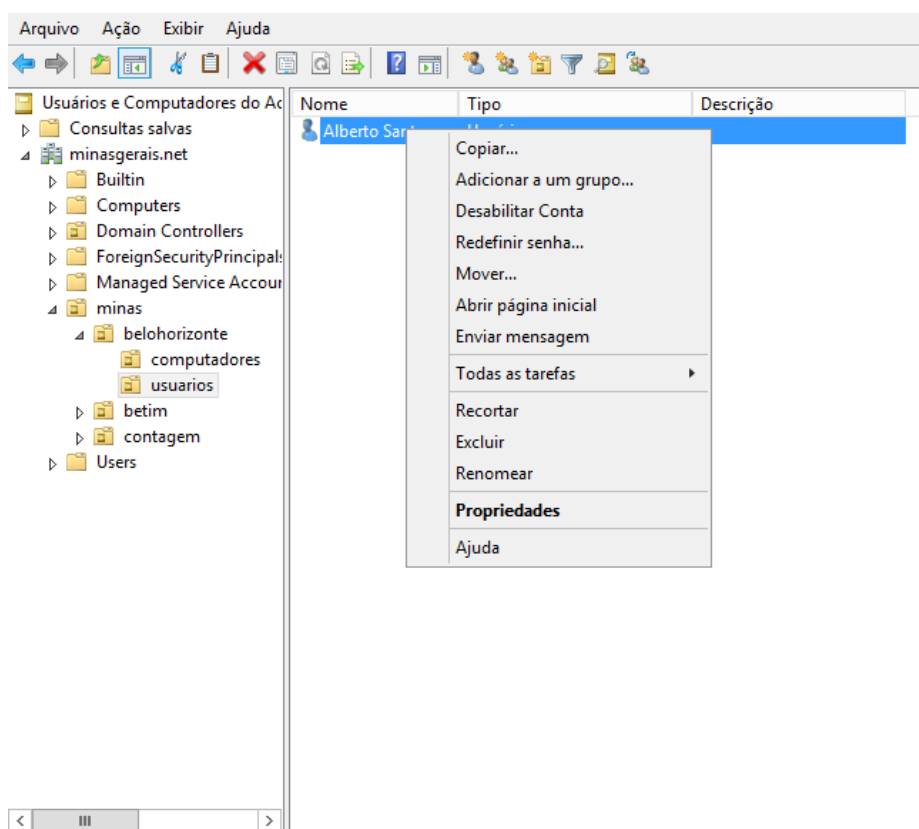


Figura 27. Propriedades do Usuário

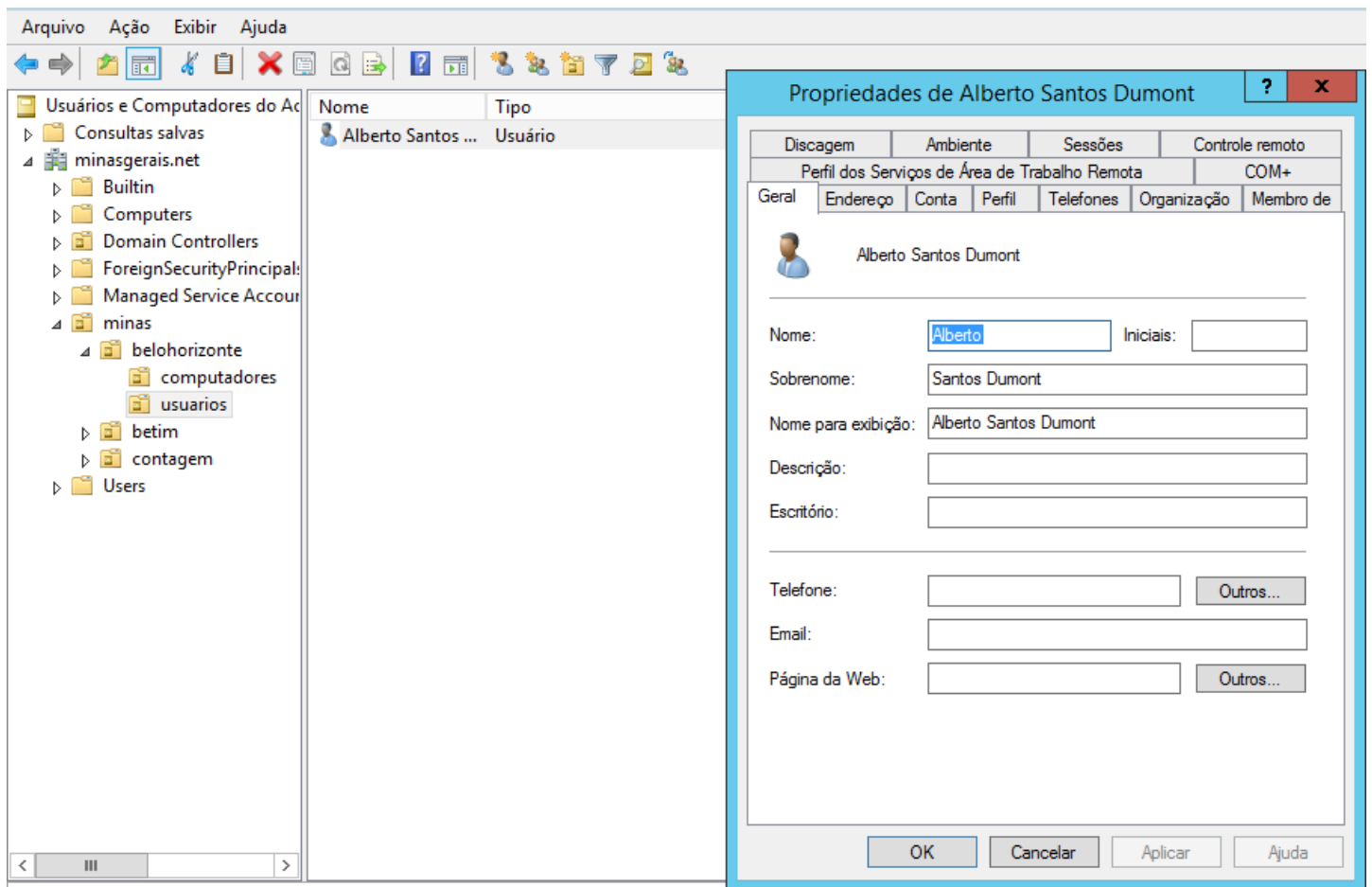


Figura 28. Propriedades Gerais do usuário

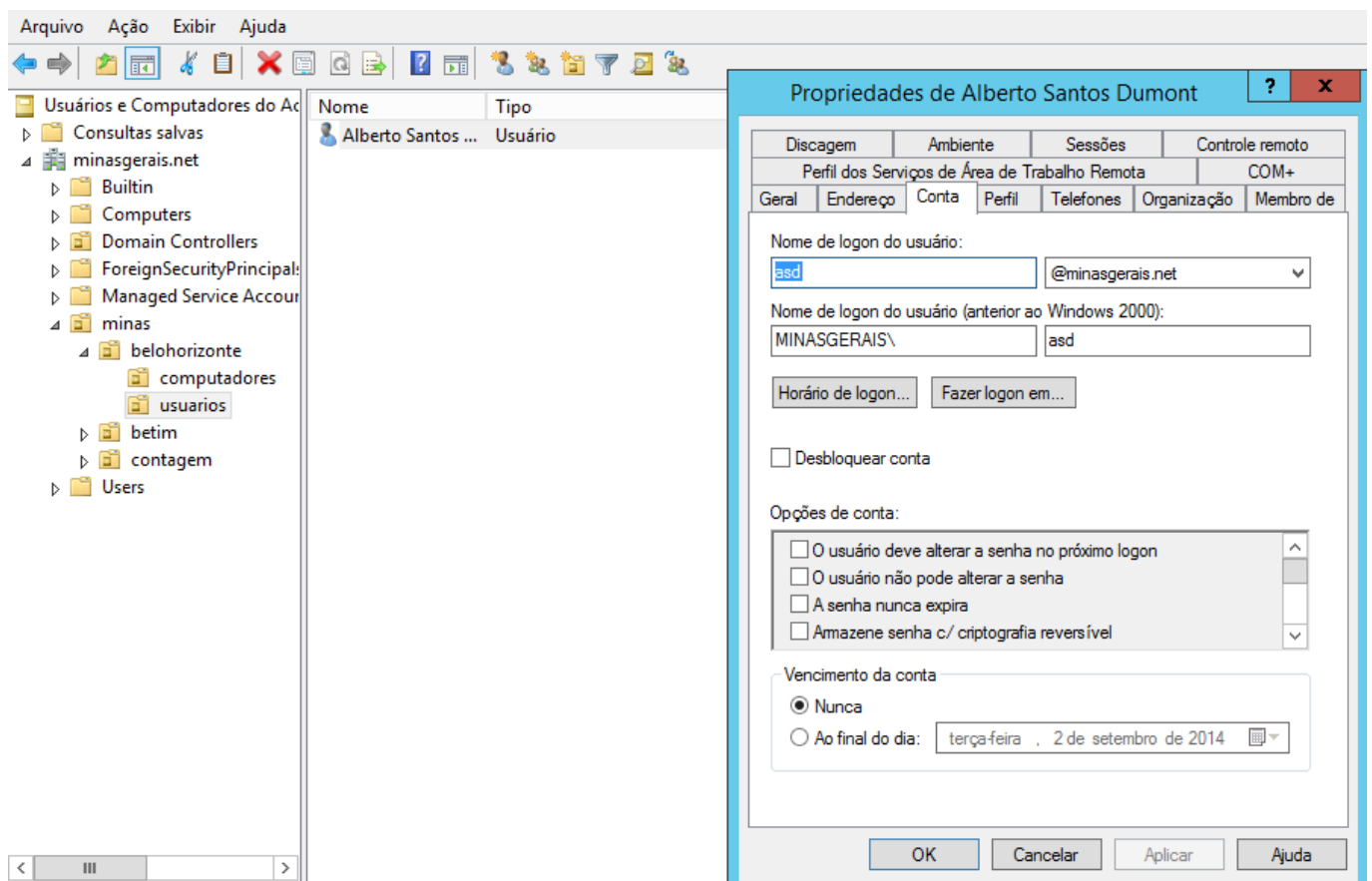


Figura 29. Propriedades da conta de usuário

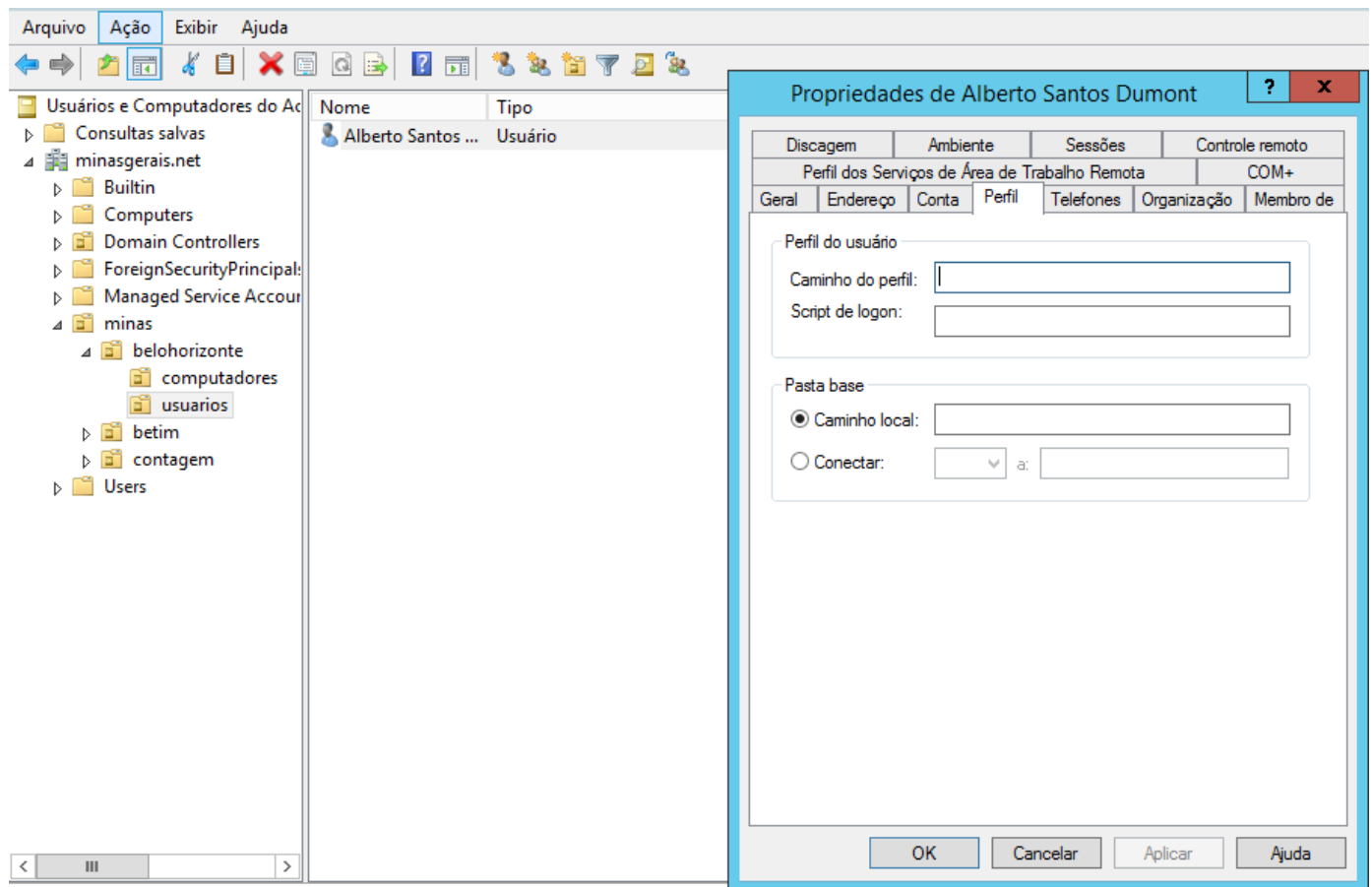


Figura 30. Propriedades do perfil de usuário

Para entrega ao professor, deve ser criado uma conta com o seu nome!!

Inserir a estação no domínio.

Para inserir uma estação no domínio, vá na estação Windows 7 ou 8.1, clique com o botão direito no menu iniciar e depois em sistema.

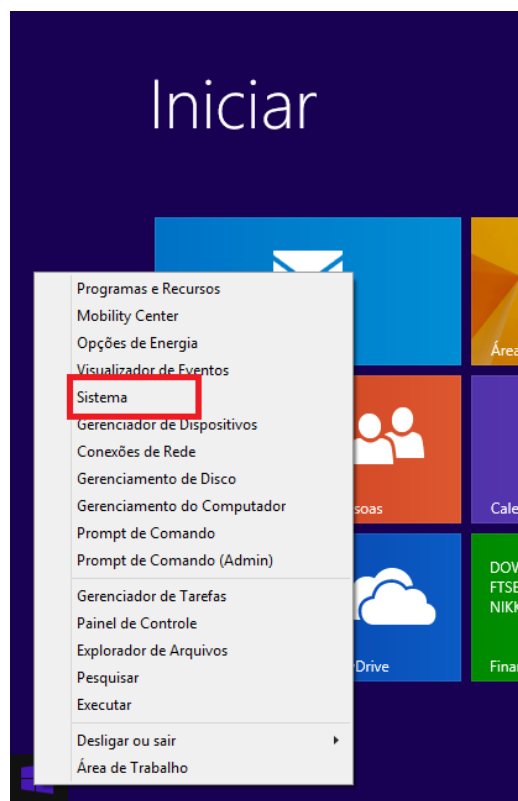


Figura 31. Ferramenta Sistema do Windows 8.1

Vá em alterar configurações para mudar o nome do computador ou o domínio em que a estação vai conectar.

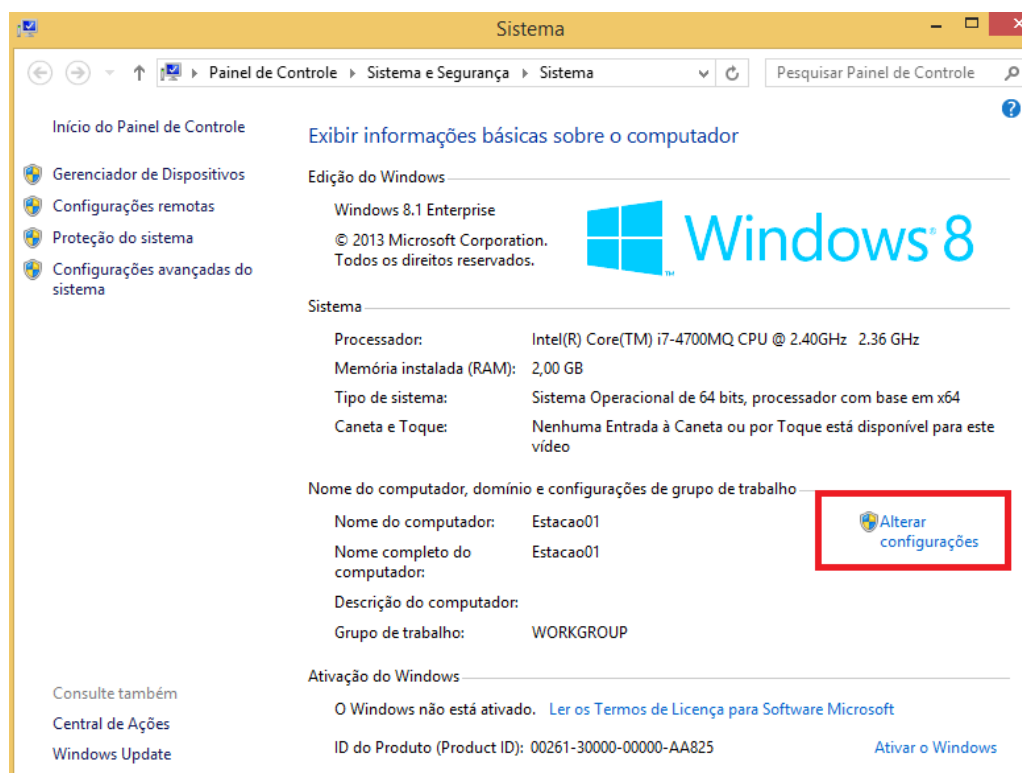


Figura 32. Alteração de configurações do computador

Clique em alterar.

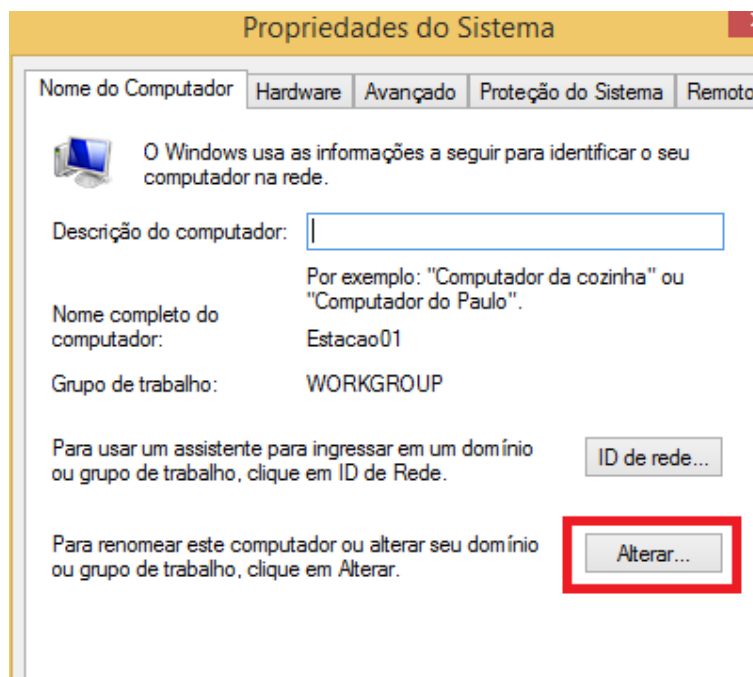


Figura 33. Alteração de configurações do computador

Entre com o nome do domínio.

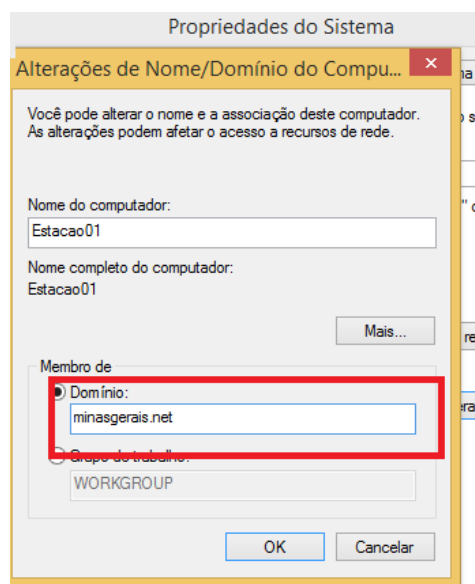


Figura 34. Inclusão da estação no domínio minasgerais.net

Para incluir a estação no domínio é necessário entrar com as credenciais do usuário que tem autorização para isso. No caso da nossa organização fictícia será o **administrador** e a senha é **Redes2020** ou **Redes2018** se vc ainda não alterou.

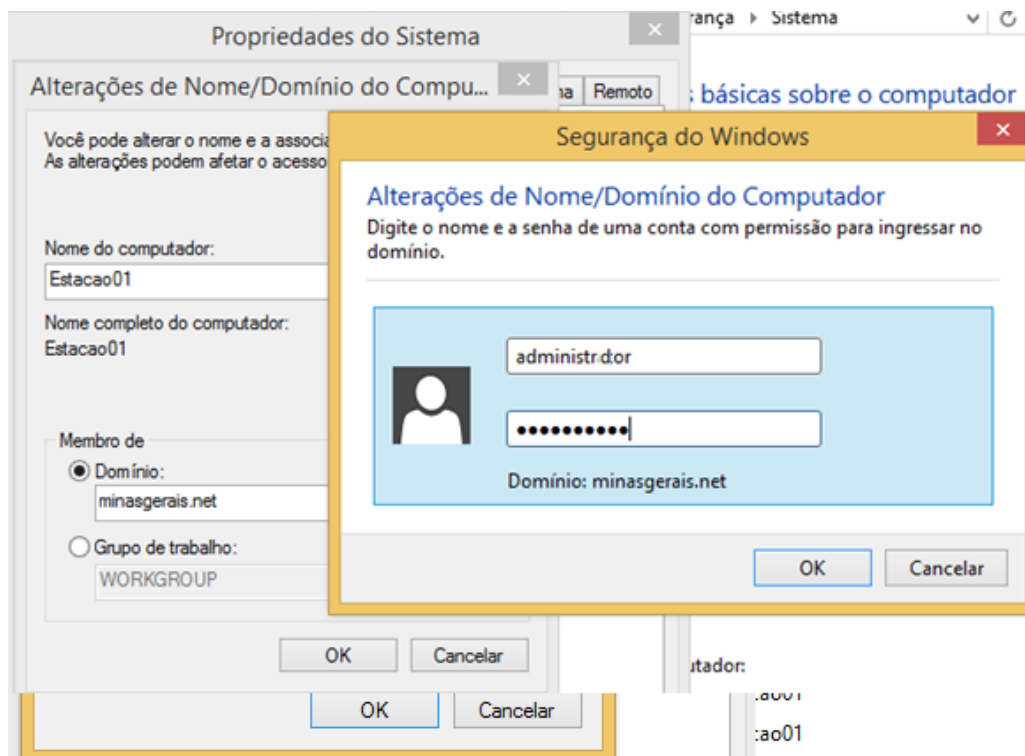


Figura 35. Inclusão da estação no domínio minasgerais.net

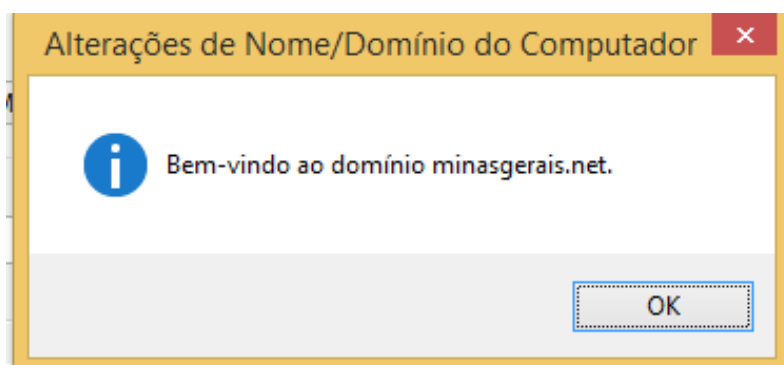


Figura 36. Tela de boas-vindas ao domínio

Se não receber a mensagem de boas vindas, significa que o seu Windows 7 não está se comunicando com o servidor ou vc não está usando o DNS certo na estação de trabalho.

Gerenciamento de Políticas de Grupo.

No **servidor**, clique no menu iniciar e vá em ferramentas administrativas e gerenciamento de política de grupo.

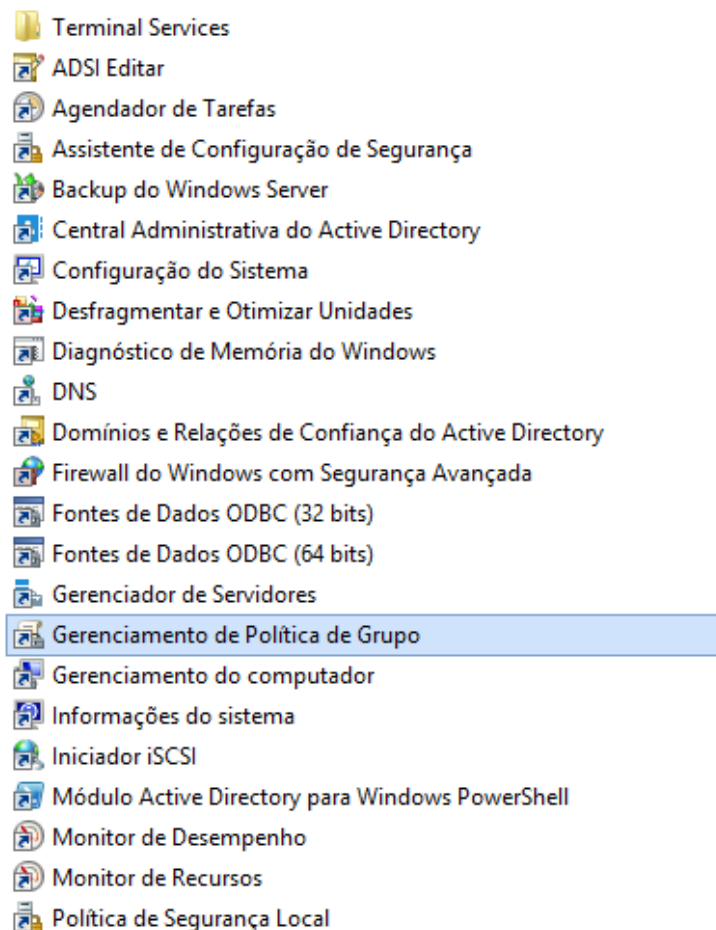


Figura 37. Gerenciamento de Políticas de Grupo

Uma Política de Grupo³ é uma infraestrutura que permite que você especifique configurações gerenciadas para usuários e computadores através de configurações de Política de Grupo. Vamos criar uma política de grupo para a unidade organizacional usuários de Belo Horizonte. Na ferramenta de política de grupo, expanda o domínio minasgerais.net, a ou minas, a ou belohorizonte. Clique com o botão direito em usuários de belohorizonte e escolha a opção Criar um GPO neste domínio. Dê o nome de **pgbh** para essa política.

³ <http://technet.microsoft.com/pt-br/library/hh831791.aspx>

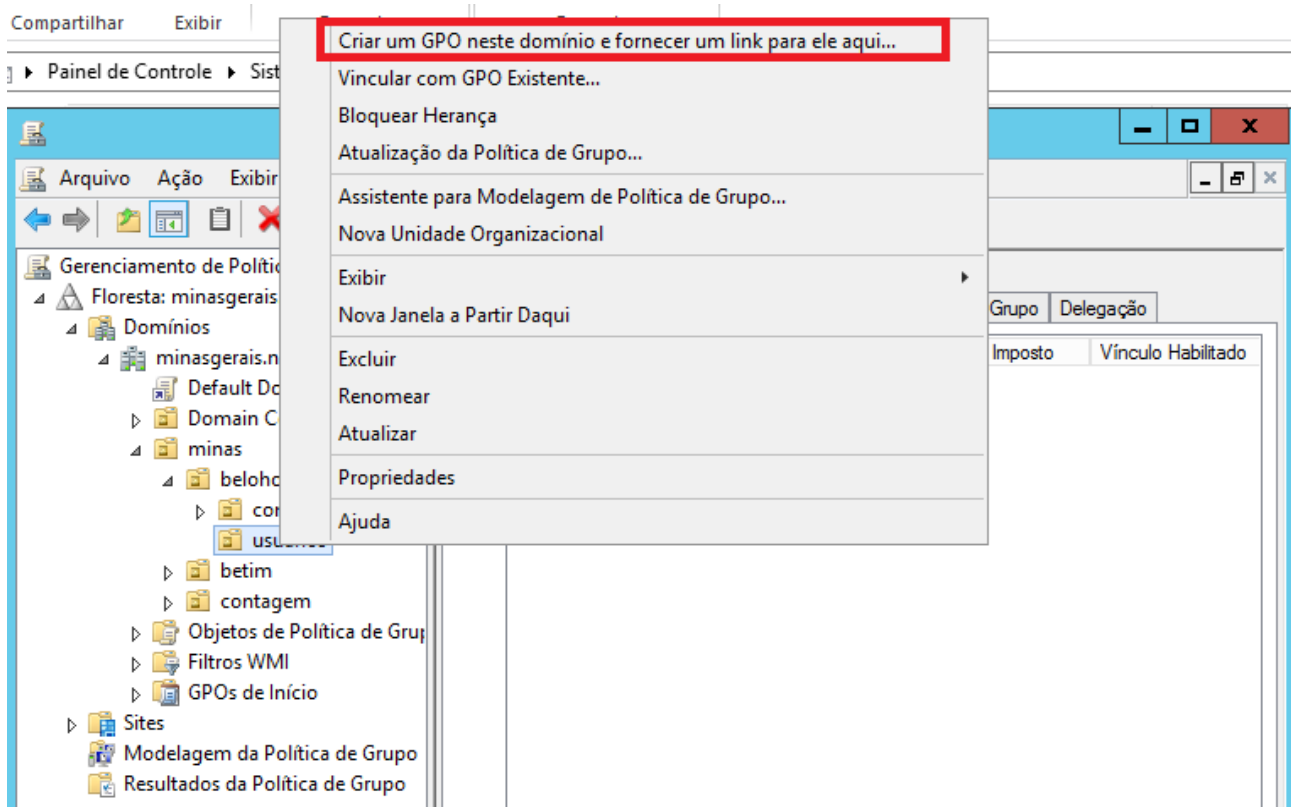


Figura 38. Criação de uma nova política de Grupo

Para editar a política, clique com o botão direito na pgbh e clique em editar.

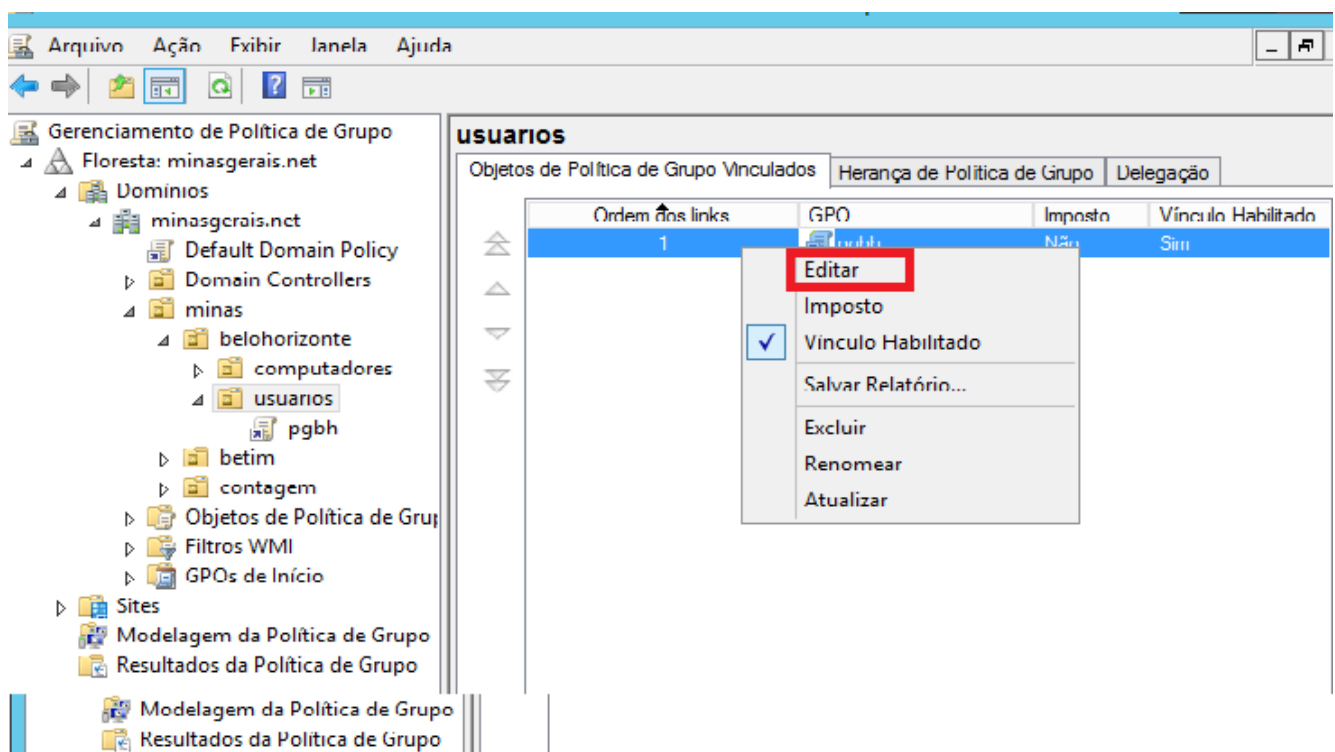


Figura 39. Edição da política de grupo.

Vamos ativar o filtro para que a ferramenta mostre apenas as políticas que possam ser aplicadas ao windows 7 ou 8.1. Certifique-se de ter selecionado a pasta “Modelos Administrativos: definições ...” dentro de Políticas em Configuração do Usuário.

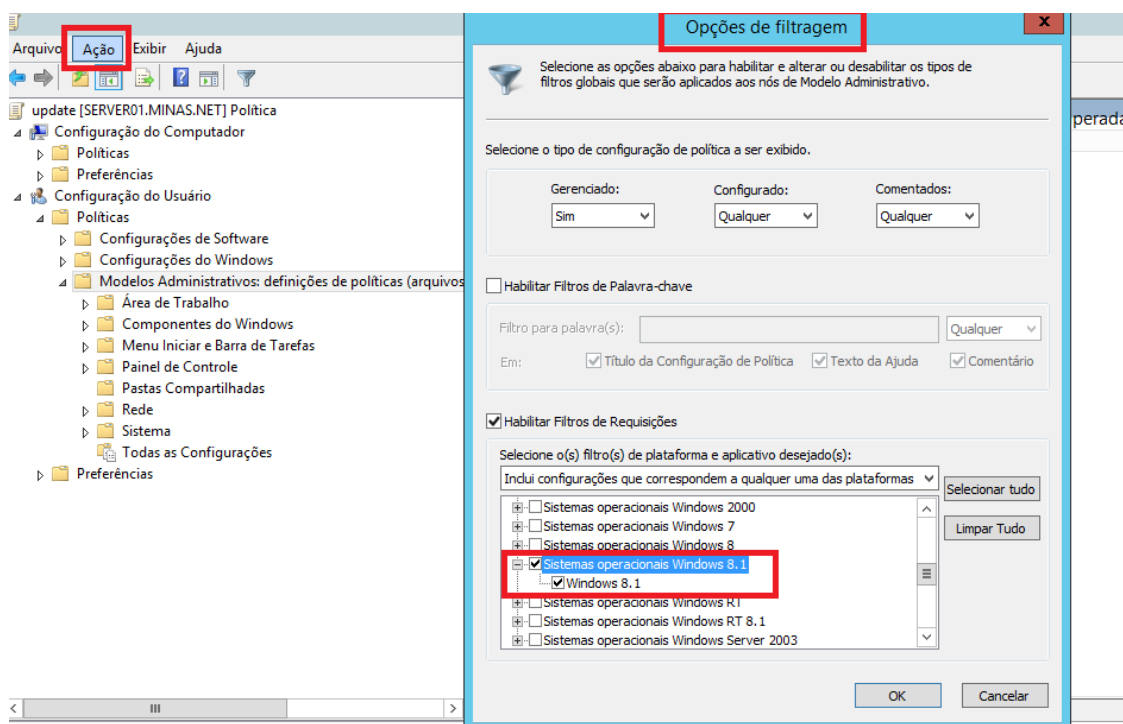


Figura 40. Ativação do Filtro para Windows 7 e 8.1

Habilite as políticas recomendadas a seguir

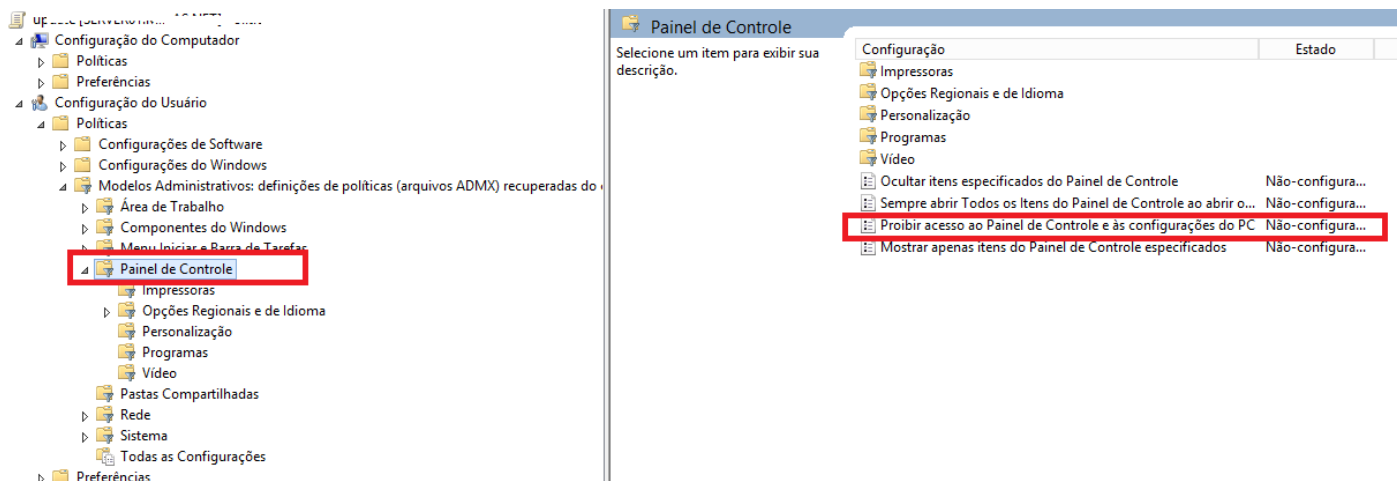


Figura 41. Alteração de política de grupo.

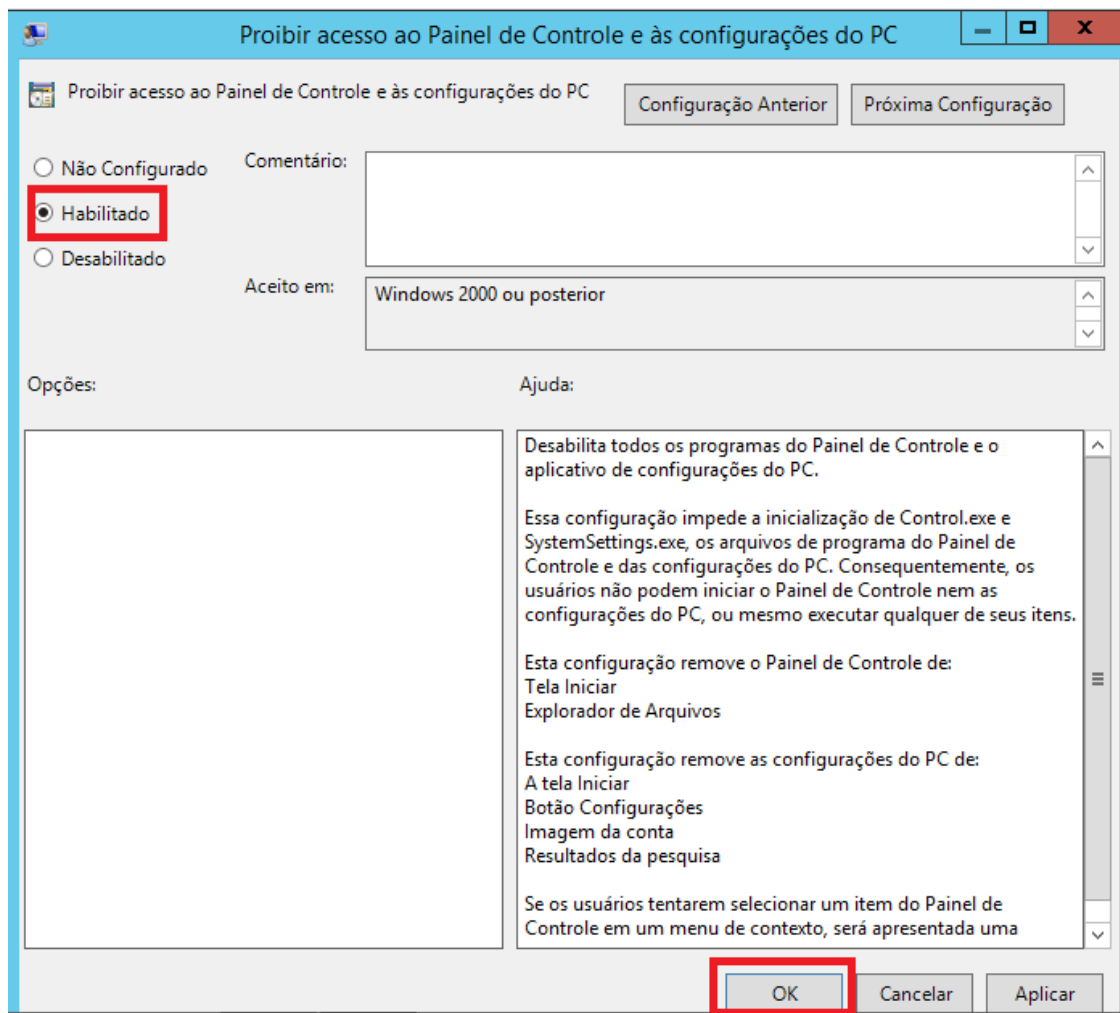


Figura 42. Detalhe da alteração de política de grupo

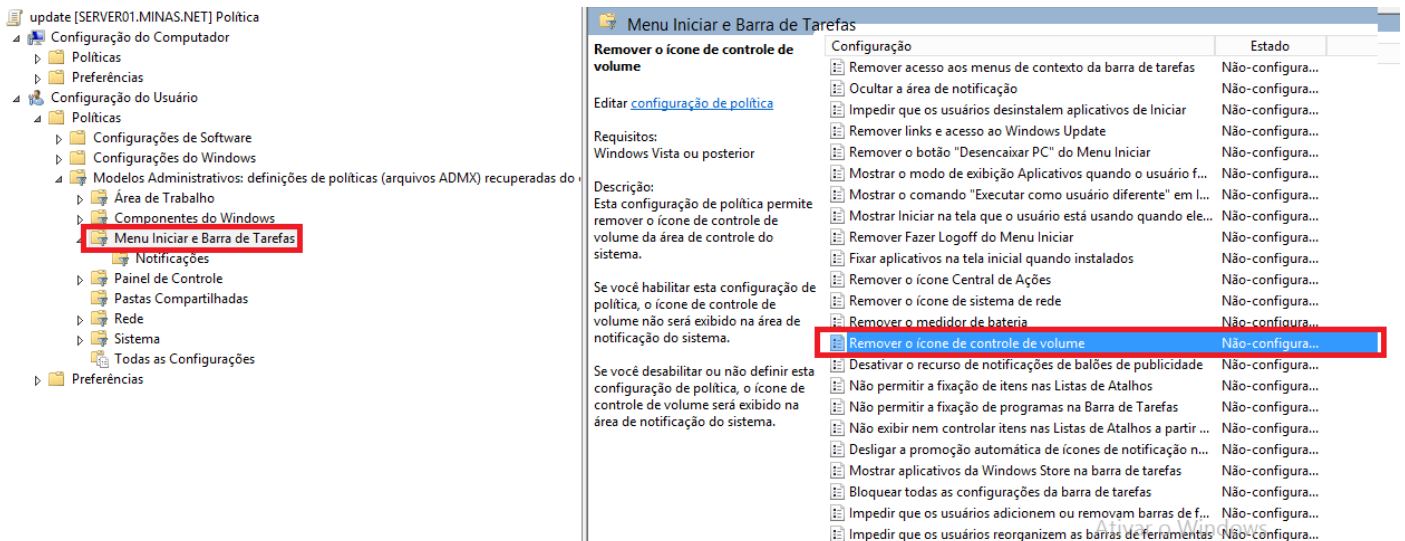


Figura 43. Alteração de política de grupo.

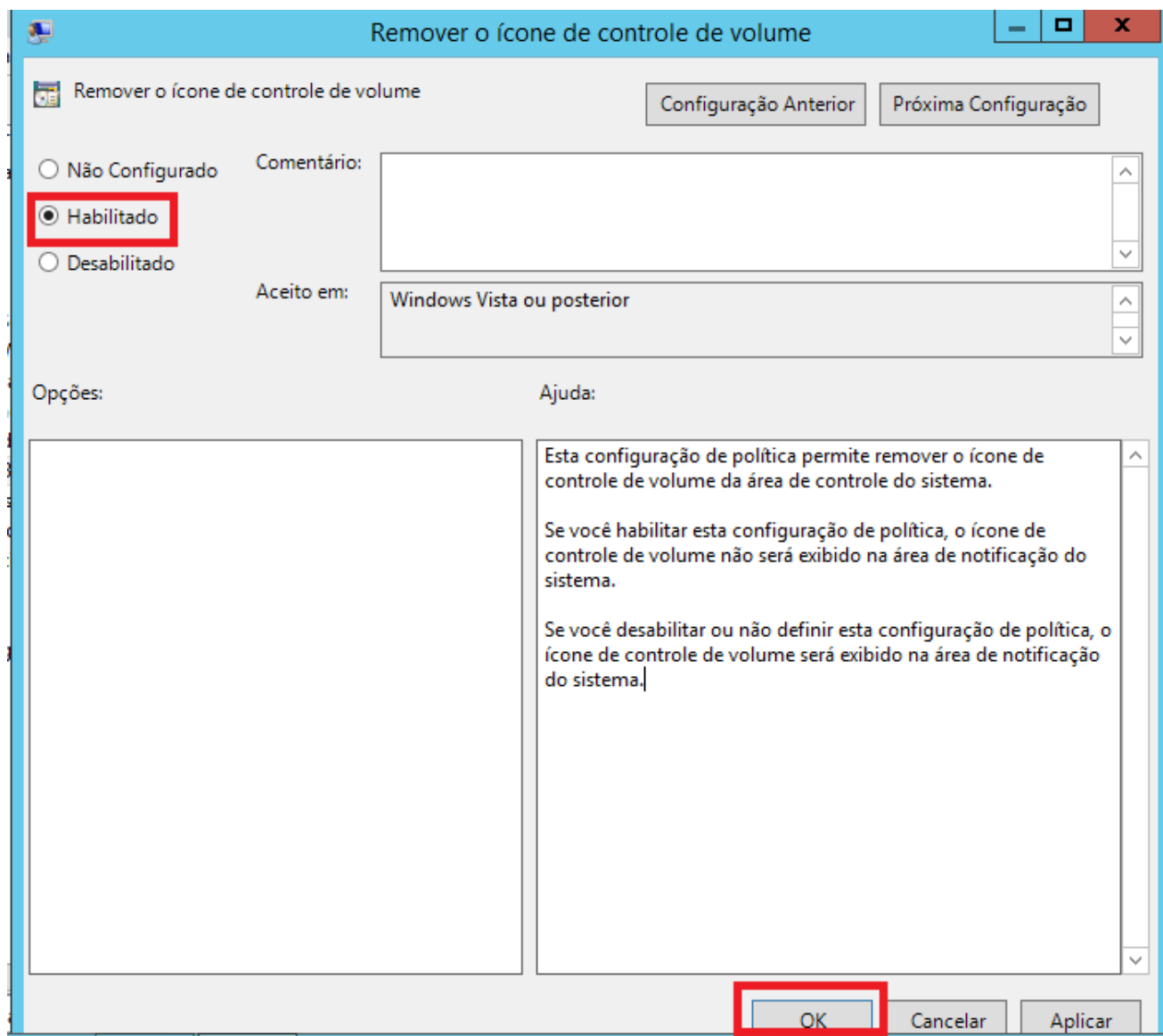


Figura 44. Detalhe da alteração de política de grupo.

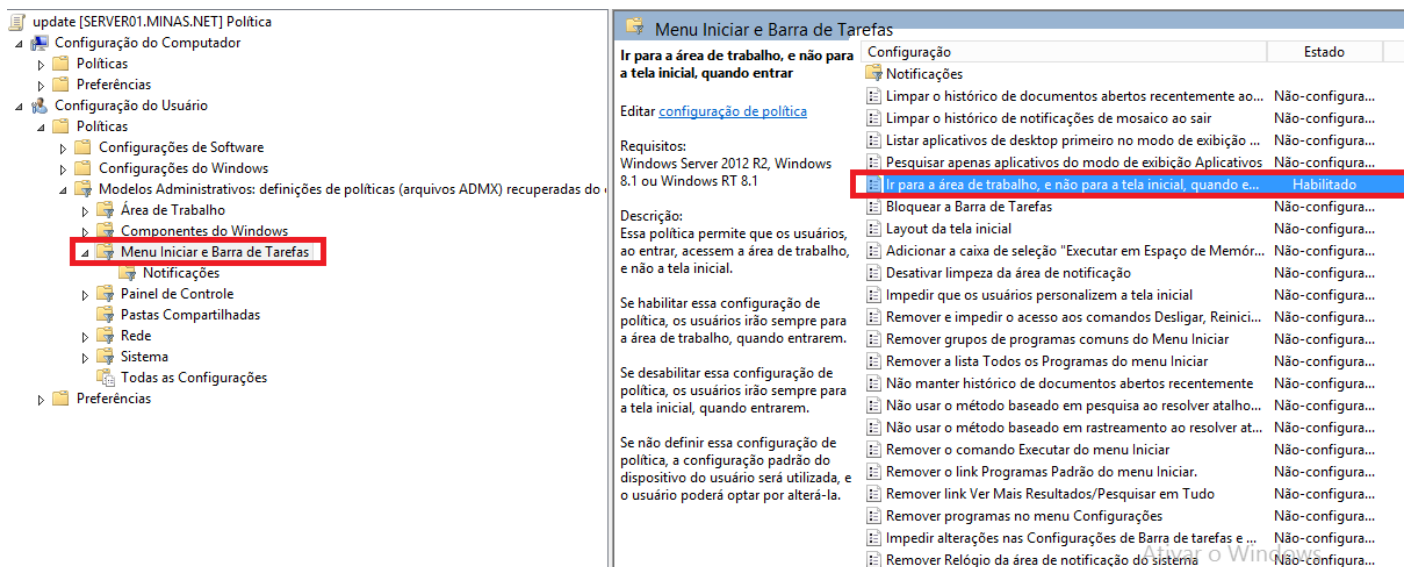


Figura 45. Alteração de política de grupo, disponível apenas no Windows 8.1

Ir para a área de trabalho, e não para a tela inicial, quando eu entrar, ou quando to...

Ir para a área de trabalho, e não para a tela inicial, quando eu entrar, ou quando todos os aplicativos de uma tela forem fechados

Configuração Anterior Próxima Configuração

☐ Não Configurado
 ☒ **Habilitado**
☐ Desabilitado

Comentário:

Aceito em: Windows Server 2012 R2, Windows 8.1 ou Windows RT 8.1

Opções: Ajuda:

Essa configuração de política permite aos usuários ir para a área de trabalho, em vez de para a tela inicial, ao entrar, ou quando todos os aplicativos de uma tela forem fechados. Essa configuração de política se aplica a todas as versões do Windows e às versões do Windows Server com a Experiência Desktop instalada.

Se você habilitar essa configuração de política, os usuários sempre irão para a área de trabalho quando entrarem ou quando todos os aplicativos de uma tela forem fechados.

Se você desabilitar ou não definir essa configuração de política, por padrão, os usuários irão para a tela inicial ao entrar e poderão definir essa configuração.

Figura 46. Detalhe da alteração de política de grupo.

É possível visualizar um relatório das políticas aplicadas. Basta clicar na política criada e depois em opções.

update		
Escopo	Detalhes	Opções
update		
Dados coletados em: 15/08/2014 14:25:37		mostrar tudo
Configuração do Computador (Habilitada)		ocultar
Políticas		ocultar
Modelos Administrativos		Mostrar
Configuração do Usuário (Habilitada)		ocultar
Políticas		ocultar
Modelos Administrativos		ocultar
Definições de política (arquivos ADMX) recuperadas do computador local.		
Menu Iniciar e Barra de Tarefas		ocultar
Política	Configuração	comentário
Ir para a área de trabalho, e não para a tela inicial, quando entrar	Ativada	
Remover o ícone de controle de volume	Ativada	
Painel de Controle		ocultar
Política	Configuração	comentário
Proibir acesso ao Painel de Controle e às configurações do PC	Ativada	Ativar o Windows
Vá para Sistema no Painel de Controle para ativar.		

Figura 47. Relatório da política de grupo

Figura 49 – Relatório da política de grupo.

Para forçar a aplicação da política na estação, faça o logoff na estação e entre com o usuário **asd**, Alberto Santos Dumont, verifique se o Painel de Controle e as outras restrições foram implantadas, se ainda não foram, log como administrador e rode o comando **gpupdate /force** na própria estação de trabalho.

Teste o acesso aos recursos que foram negados ao usuário.