Universidade Federal do Ceará (UFC) - Campus Quixadá
Administração de Sistemas Operacionais Windows
Professor: Antônio Rafael Braga

Laboratório 14

Configurando Políticas de Segurança

ESTE LABORATÓRIO CONTÉM OS SEGUINTES EXERCÍCIOS E ATIVIDADES:

- Exercício 14.1 – Configurando políticas de segurança.
- **Desafio de laboratório: Atribuindo diretos aos usuários.**
- Exercício 14.2 – Configurando políticas de auditoria.
- **Desafio de laboratório: Exibindo dados de auditoria.**

ANTES DE COMEÇAR

O ambiente de laboratório consiste em três servidores conectados a uma rede local, um dos quais está configurado para funcionar como o controlador de um domínio chamado adatum.com. Os computadores necessários para este laboratório estão listados na Tabela abaixo.

Computer	*Operating System*	*Computer Name*
Domain controller 1	Windows Server 2012	SVR-DC-A
Member server 2	Windows Server 2012	SVR-MBR-B
Member server 3	Windows Server 2012	SVR-MBR-C

Além dos computadores, você também precisa do software necessário para esse laboratório listado abaixo.

Software required for Lab 17Software	*Location*
Lab 17 student worksheet	Lab17_worksheet.docx (provided by instructor)

Trabalho com planilhas de laboratório

Cada laboratório neste manual requer que você responda a perguntas, faça capturas de tela e execute outras atividades que você documentou em uma planilha nomeada para o laboratório, como Lab14_worksheet.docx. É recomendável que você use uma unidade flash USB para armazenar suas planilhas, para que você possa enviá-las ao seu instrutor para revisão. Conforme você realiza os exercícios em cada laboratório, abra o arquivo de planilha apropriado, preencha as informações necessárias e salve o arquivo em sua unidade flash.

Depois de concluir este laboratório você será capaz de:

- Configurar Políticas de segurança.
- Configurar e atribuir direitos de usuários.
- Configurar políticas de auditoria.

Exercício 17.1	Configurando Políticas de Segurança
Visão geral	Neste exercício, você examina as configurações de política de segurança padrão para seu domínio e, em seguida, cria um GPO contendo configurações novas e revisadas.
Mentalidade	Como você pode controlar o acesso aos seus computadores de rede usando políticas de segurança?
Tempo de conclusão	15 minutos

1. Faça logon no computador SVR-MBR-B, usando a conta de administrador do domínio e a senha Password. Instale o recurso Gerenciamento de Política de Grupo usando o Assistente para Adicionar Funções e Recursos, assim como você fez no Exercício 16.1.
2. No Gerenciador do Servidor, clique em Ferramentas> Gerenciamento de Política de Grupo. O console de gerenciamento de política de grupo é exibido.
3. Navegue até a pasta Objetos de Política de Grupo.

Pergunta 1	Como você pode saber quais políticas na pasta Opções de segurança alteraram as configurações no GPO de política de domínio padrão?

4. Pressione Alt + Prt Scr para fazer uma captura de tela mostrando as configurações de opções de segurança existentes no GPO de política de domínio padrão. Pressione Ctrl + V para colar a imagem na página fornecida no arquivo de planilha do Lab 14.
5. Clique com o botão direito na pasta Objetos de Política de Grupo e, no menu de contexto, clique em Novo. A caixa de diálogo Novo GPO é exibida.
6. Na caixa de texto Nome, digite Domínio Revisado e clique em OK. Um novo GPO de domínio revisado aparece na pasta Objetos de política de grupo.
7. Clique com o botão direito do mouse no GPO Domínio Revisado e, no menu de contexto, clique em Editar. O console do Editor de Gerenciamento de Diretiva de Grupo é exibido.

8. No console do Editor de Gerenciamento de Política de Grupo, navegue até a pasta Configuração do Computador> Políticas> Configurações do Windows> Configurações de Segurança> Políticas Locais> Opções de Segurança.
9. Na pasta Opções de segurança, clique duas vezes no Dispositivos: Tem permissão para formatar e ejetar a política de mídia removível. Os Dispositivos: Têm permissão para formatar e ejetar política de mídia removível a caixa de diálogo aparece (veja a Figura abaixo).

10. Selecione os Defina esta configuração de política caixa de seleção e, na lista suspensa, selecione Administradores e usuários interativos. Em seguida, clique em OK.
11. Defina e ative as seguintes políticas de opções de segurança:
    - Dispositivos: Restrinja o acesso ao CD-ROM à política somente de usuário conectado localmente.
    - Dispositivos: restringir o acesso ao disquete à política somente de usuário conectado localmente.
    - Segurança de rede: Força o logoff quando o horário de logon expirar.
12. Feche o console de editor de gerenciamento de política de grupo.
13. No console de Gerenciamento de Política de Grupo, clique com o botão direito do mouse no domínio adatum.com e, no menu de contexto, clique em Vincular a GPO Existente. A caixa de diálogo selecionar GPO é exibida.
14. Selecione o GPO de domínio revisado e clique em OK.
15. Selecione o domínio adatum.com e clique na guia Objetos de Política de Grupo Vinculados no painel direito.
16. Selecione o GPO de domínio revisado e clique no Mover a seta para cima do link. O GPO de domínio revisado agora aparece primeiro na lista de GPOs vinculados.

Pergunta 2	Por que é necessário que o GPO Opções revisadas apareça primeiro na lista?

Fim do exercício. Deixe todas as janelas abertas para o próximo exercício.

Laboratório Desafio	Atribuição de direitos de usuário
Visão geral	Neste exercício, você adiciona uma seleção de atribuições de direitos do usuário àquelas já existentes.
Tempo de conclusão	15 minutos

Sua organização criou uma nova função de trabalho chamada diretor, e seu trabalho é fornecer aos novos diretores os direitos de usuário do controlador de domínio de que precisam para desempenhar suas funções. O grupo de Diretores já foi criado no domínio adatum.com. Para completar este desafio, você deve conceder ao grupo de Diretores os seguintes direitos de usuário a todos os controladores de domínio na rede, sem interferir em nenhum dos direitos existentes.

- Negar logon localmente.
- Adicionar estações de trabalho ao domínio.
- Forçar desligamento de um sistema remoto
- Permitir que contas de computador e usuário sejam confiáveis para delegação
- Gerenciar auditoria e registro de segurança
- Desligue o sistema

Escreva as etapas básicas que você deve executar para cumprir o desafio e, em seguida, faça uma captura de tela mostrando os direitos do usuário configurados e pressione Ctrl + V para colar a imagem na página fornecida no arquivo de planilha do Lab 14.

Fim do desafio. Deixe todas as janelas abertas para o próximo exercício.

Exercício 17.2	Configurando Políticas de Auditoria
Visão geral	Neste exercício, você configura as políticas de auditoria para monitorar logons de conta e acesso a objetos específicos.
Mentalidade	Como você pode usar os recursos de auditoria do Windows Server 2012 para aumentar a segurança da sua rede sem se sobrecarregar com dados?
Tempo de conclusão	20 minutos

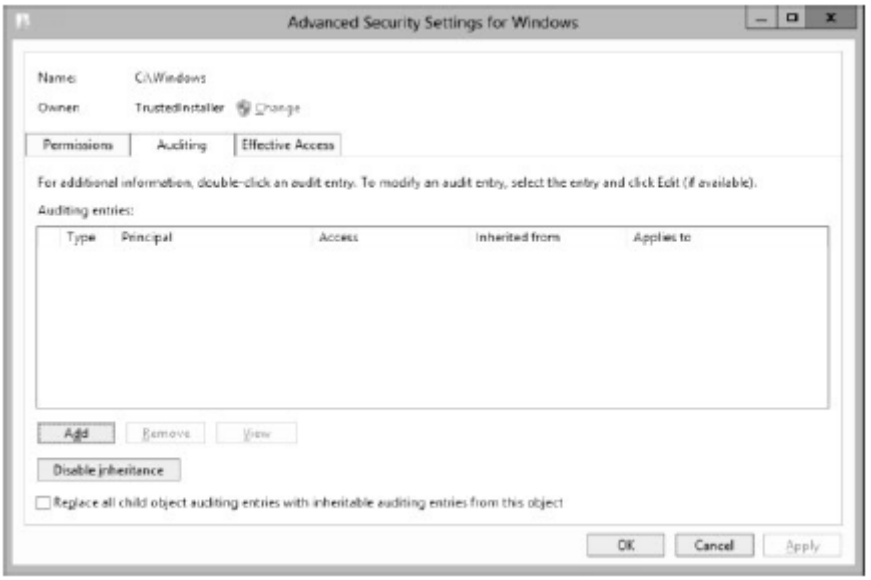
1. Em SVR-MBR-B, no console de Gerenciamento de Política de Grupo, crie um novo GPO chamado Políticas de Auditoria e abra-o no Editor de Gerenciamento de Política de Grupo.
2. Navegue até o nó Configuração do computador> Políticas> Configurações do Windows> Configurações de segurança> Políticas locais> Política de auditoria. As políticas de auditoria aparecem no painel direito.
3. Clique duas vezes no Auditar eventos de logon de conta política. O Auditar propriedades de eventos de logon de conta folha aparece.
4. Selecione os Defina essas configurações de política caixa de seleção.
5. Marque a caixa de seleção Falha, desmarque a caixa de seleção Sucesso e clique em OK.

Pergunta 3	Por que, neste caso, a auditoria de falhas de eventos é mais útil do que a auditoria de sucessos?

6. Clique duas vezes na política de acesso ao objeto de auditoria. A folha Propriedades de acesso ao objeto de auditoria é exibida.
7. Marque a caixa de seleção para definir estas configurações de política.
8. Selecione as caixas de seleção Falha e Sucesso e clique em OK.
9. Pressione Alt + Prt Scr para fazer uma captura de tela mostrando as políticas que você configurou. Pressione Ctrl + V para colar a imagem na página fornecida no arquivo de planilha do Lab 14.
10. Em Configurações de segurança, selecione o nó Log de eventos.
11. No painel direito, clique duas vezes na política Tamanho máximo do log de segurança.
12. Selecione o Definir esta configuração de política caixa de seleção, deixe o valor da caixa de rotação em 16384 kilobytes e clique em OK.

Pergunta 4	Por que é prudente limitar o tamanho do log de eventos ao usar a auditoria.

13. Feche o console do Editor de Gerenciamento de Política de Grupo.
14. Vincule o GPO de Políticas de Auditoria ao domínio adatum.com.
15. Clique no ícone File Explorer na barra de tarefas. A janela do File Explorer é exibida.
16. No painel esquerdo, navegue até a unidade C: no computador local.
17. Clique com o botão direito na pasta C: \ Windows e, no menu de contexto, clique em Propriedades. A folha de Propriedades do Windows é exibida.
18. Clique na guia Segurança.
19. Clique em Advanced. A caixa de diálogo Configurações de segurança avançadas para Windows é exibida.
20. Clique na guia Auditoria (veja a Figura abaixo).



21. Clique em Adicionar. A caixa de diálogo Entrada de auditoria para Windows é exibida.
22. Clique em Selecionar um Principal. A caixa de diálogo selecionar usuário, computador, conta de serviço ou grupo é exibida.
23. No insira o nome do objeto para selecionar caixa de texto, tipo Administrador e clique em OK.
24. Marque a caixa de seleção Controle total e clique em OK.
25. Clique em OK para fechar a caixa de diálogo Configurações de segurança avançadas para Windows.
26. Clique em Continuar para ignorar as mensagens de erro, se necessário. Clique em OK para fechar a folha de Propriedades do Windows.
27. Abra uma janela de Prompt de Comando administrativa e digite gpupdate / force para atualizar as configurações de Política de Grupo do sistema.

Fim do exercício. Deixe todas as janelas abertas para o próximo exercício.

Laboratório **Desafio**	**Visualizando Dados de Auditoria**
Visão geral	Para concluir este exercício, você deve demonstrar que seu computador SVR-MBRB está realmente coletando os dados de auditoria para os quais você configurou suas políticas.
Mentalidade	Como você exibe os dados de auditoria?
Tempo de conclusão	10 minutos

Para completar este desafio, exiba os dados de auditoria que você configurou em seu servidor para coletar no Exercício 14.2. Pressione Alt + Prt Scr para fazer uma captura de tela mostrando uma amostra dos dados coletados. Pressione Ctrl + V para colar a imagem na página fornecida no arquivo de planilha do Lab 14.

FIM