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

Laboratório 15

Configurando aplicação de políticas de restrições

ESTE LABORATÓRIO CONTÉM OS SEGUINTES EXERCÍCIOS E ATIVIDADES:

- Exercício 15.1 – Configurando políticas de restrição de software.
- Exercício 15.2 – Usando AppLocker
- **Criação de regras adicionais.**

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	*Location*
Lab 18 student worksheet	Lab18_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 documentará em uma planilha nomeada para o laboratório, como Lab15_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:

- Criar políticas de restrição de softwares.
- Configurar AppLocker.

Exercício 18.1	Criação de políticas de restrição de software
Visão geral	Neste exercício, você cria uma regra que evita que os usuários executem um programa específico.
Mentalidade	Como você pode impedir que os usuários da rede percam tempo com jogos e outros programas não produtivos?
Tempo de conclusão	20 minutos

1. Faça logon no computador SVR-MBR-B, usando a conta de administrador do domínio e a senha Password. Abra o Gerenciador do Servidor e clique em Ferramentas> Gerenciamento de Política de Grupo. O console de gerenciamento de política de grupo é exibido.
2. Navegue até a pasta Objetos de Política de Grupo.
3. 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.
4. Na caixa de texto Nome, digite Restrições de software e clique em OK. Um novo GPO de Restrições de Software aparece na pasta Objetos de Política de Grupo.
5. Clique com o botão direito do mouse no GPO Restrições de Software e, no menu de contexto, clique em Editar. O console do Editor de Gerenciamento de Diretiva de Grupo é exibido.
6. 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 de Restrição de Software.
7. Clique com o botão direito do mouse na pasta Políticas de restrição de software e, no menu de contexto, clique em Novas políticas de restrição de software. As políticas e subpastas padrão são exibidas.
8. Clique com o botão direito na pasta Regras Adicionais e, no menu de conteúdo, selecione Nova Regra de Hash. A caixa de diálogo Nova regra de hash é exibida (consulte a Figura abaixo).

9. Clique em Browse. Uma caixa de combinação abrir é exibida.
10. Procure e selecione o arquivo C: \ Windows \ regedit. Clique em Abrir. As informações a ser hash aparecem na caixa Informações do arquivo.
11. Clique OK. A regra de hash aparece na pasta Regras Adicionais.

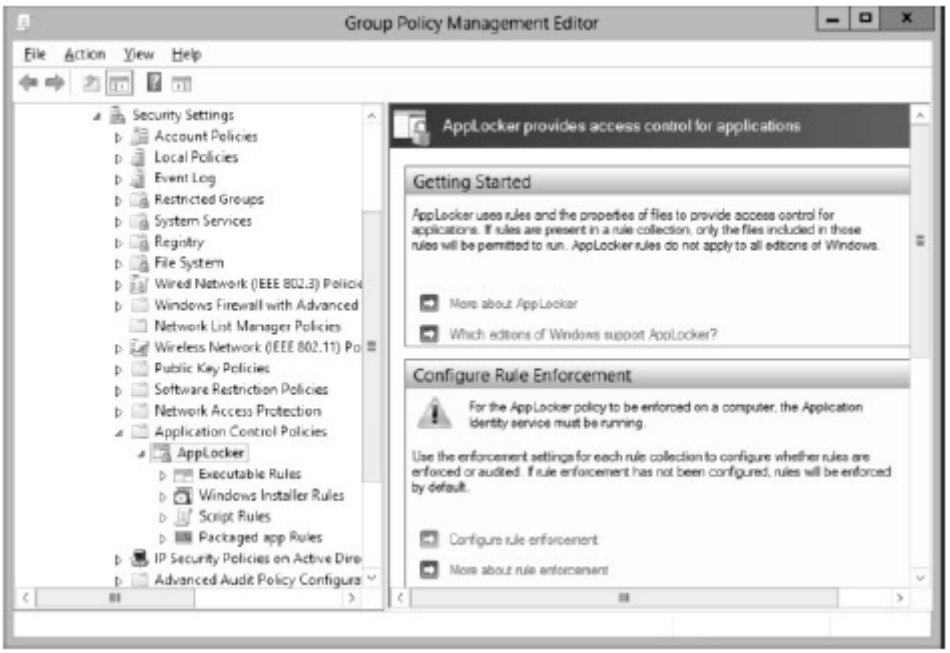
Pergunta 1	Que problema ocorreria se você alterasse a restrição de software padrão para Não permitido e configurasse uma regra de hash definindo o arquivo regedit.exe como Irrestrito?

12. Feche o console do 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 Restrições de Software e clique em OK.
15. No SVR-MBR-C, reinicie o computador.
16. Quando o computador reiniciar, pressione CTRL + ALT + DEL e faça logon usando o Adatum \ Administrador conta com a senha Password.
17. Clique no botão File Explorer na barra de tarefas. A janela do File Explorer é exibida.
18. Navegue até a pasta C: \ Windows no sistema local e clique duas vezes no arquivo regedit. Uma caixa de mensagem é exibida, informando que o acesso ao arquivo está bloqueado.
19. Pressione Alt + Prt Scr para fazer uma captura de tela mostrando a caixa de mensagem. Pressione Ctrl + V para colar a imagem na página fornecida no arquivo de planilha do Lab 15.
20. Em SVR-MBR-B, no console de Gerenciamento de Política de Grupo, clique na guia Objetos de Política de Grupo Vinculados.
21. Clique com o botão direito do mouse no link Software Restriction GPO em adatum.com e clique para desmarcar a marca de seleção Link Enabled. Uma caixa de mensagem é exibida, solicitando que você confirme sua ação.
22. Clique OK.

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

Exercício 18.2	Usando AppLocker
Visão geral	Neste exercício, você cria regras que regem o acesso ao programa usando o AppLocker.
Mentalidade	Como o processo de criação de regras de AppLocker difere daquele de criação de políticas de restrição de software?
Tempo de conclusão	20 minutos

1. No computador SVR-MBR-B, no Gerenciador do Servidor, clique em Ferramentas> Gerenciamento de Política de Grupo. O console de gerenciamento de política de grupo é exibido.
2. Navegue até a pasta Objetos de Política de Grupo.
3. 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.
4. Na caixa de texto Nome, digite Regras AppLocker e clique em OK. Um novo GPO AppLocker Rules aparece na pasta Group Policy Objects.
5. Clique com o botão direito do mouse no GPO AppLocker Rules e, no menu de contexto, clique em Editar. O console do Editor de Gerenciamento de Diretiva de Grupo é exibido.
6. 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 de Controle de Aplicativos> AppLocker.
7. Expanda a pasta AppLocker (consulte a Figura abaixo).



8. Selecione a pasta Regras executáveis.
9. Clique com o botão direito na pasta Regras executáveis e, no menu de contexto, clique em Gerar regras automaticamente. O Assistente para Gerar Automaticamente Regras Executáveis aparece, exibindo o Pasta e permissões da página.
10. Clique em Avançar. O Preferências de regra página aparece.
11. Clique em Avançar. O Regras de revisão página aparece.
12. Clique em Criar. Uma caixa de mensagem é exibida, perguntando se você deseja criar regras padrão.
13. Clique em Sim. As regras aparecem na pasta Regras executáveis.
14. Repita as etapas 9 a 13 duas vezes para criar as regras padrão nas pastas Regras do Windows Installer e Regras de script.
15. Clique com o botão direito na pasta Regras executáveis e, no menu de contexto, clique em Criar nova regra. O Assistente para Criar Regras Executáveis aparece, exibindo o Antes de você começar página.
16. Clique em Avançar. O Permissões página aparece.
17. Selecione a opção Negar e clique em Avançar. A página Condições é exibida.
18. Selecione a opção Hash do arquivo e clique em Avançar. O Hash do arquivo página aparece.
19. Clique em Procurar arquivos. Uma caixa de combinação abrir é exibida.
20. Navegue até o regedit arquivo e clique em Abrir.
21. Clique em Avançar. O Nome e Descrição página aparece.
22. Clique em Criar. A nova regra aparece na pasta Regras executáveis.
23. Pressione Alt + Prt Scr para fazer uma captura de tela mostrando as regras no console de Gerenciamento de Política de Grupo. Pressione Ctrl + V para colar a imagem na página fornecida no arquivo de planilha do Lab 18.
24. Feche o console do Editor de Gerenciamento de Política de Grupo.
25. 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.
26. Selecione o GPO AppLocker Rules e clique em OK.
27. No SVR-MBR-C, reinicie o computador.
28. Quando o computador reiniciar, pressione CTRL + ALT + DEL e faça logon usando o Adatum \ Administrador conta com a senha Password.
29. Clique no botão File Explorer na barra de tarefas. A janela do File Explorer é exibida.
30. Navegue até a pasta C: \ Windows no sistema local e clique duas vezes no arquivo regedit. O programa Editor do Registro é carregado.
31. Feche o Editor do Registro.
32. No Gerenciador do Servidor, clique em Ferramentas> Serviços. O console de serviços é exibido.
33. Clique com o botão direito do mouse no serviço de Identidade do Aplicativo e, no menu de contexto, clique em Iniciar. O serviço é iniciado.
34. No File Explorer, navegue até a pasta C: \ Windows no sistema local e clique duas vezes no arquivo regedit.
35. Uma caixa de mensagem é exibida, informando que o acesso ao arquivo está bloqueado.

Pergunta 2	Por que é necessário iniciar o serviço de identidade do aplicativo antes que as regras do AppLocker entrem em vigor?

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

Laboratório Desafio	Criação de regras adicionais
Visão geral	Para completar este desafio, você deve criar um novo GPO contendo regras AppLocker adicionais.
Tempo de conclusão	20 minutos

No computador SVR-MBR-B, crie um novo GPO chamado AppLocker 2 e criar uma regra que permita aos membros do grupo Administradores executar todos os arquivos assinados digitalmente publicados pela Microsoft.

Pressione Alt + Prt Scr para fazer uma captura de tela do console do Editor de Gerenciamento de Política de Grupo mostrando a regra que você criou e pressione Ctrl + V para colar a imagem na página fornecida no arquivo de planilha do Lab 18.

FIM