

# 11

# NETWORK SECURITY

## PROJECTS

---

- |                     |                                   |
|---------------------|-----------------------------------|
| <b>Project 11.1</b> | Understanding Key Concepts        |
| <b>Project 11.2</b> | Using Auditing and Event Logs     |
| <b>Project 11.3</b> | Managing Account Lockout Policies |
| <b>Project 11.4</b> | Managing Password Policies        |
| <b>Project 11.5</b> | Designing for Security            |

Project 11.1 Understanding Key Concepts	
Overview	<p>Network security is a critical issue on any network. Networks are constantly under attack, from the Internet and other external sources as well as internally from network users. New types of attacks are continually being created. New viruses and other types of malicious software turn up daily. Understanding the terms and technologies related to security is an important part of security management.</p> <p>During this project, you will match various security-related terms to the definitions and descriptions of how they are used.</p>
Outcomes	<p>After completing this project, you will know how to:</p> <ul style="list-style-type: none"> <li>▲ identify key terms and concepts related to network security</li> </ul>
What you'll need	<p>To complete this project, you will need:</p> <ul style="list-style-type: none"> <li>▲ the following worksheet</li> </ul>
Completion time	20 minutes
Precautions	None

The worksheet includes a list of security-related networking terms on the left and descriptions on the right. Match each term with the description that it most closely matches. You will *not* use all descriptions. Each description can be used only once.

<u>O</u>	DES	A. Attack that attempts to disrupt a network or its servers by flooding them with packets
<u>I</u>	RC4	B. Firewall filtering method that passes packets that match sessions initiated on the internal network
<u>A</u>	DoS	C. Term referring to any type of malicious software
<u>P</u>	Spyware	D. Situation where one failure is the direct cause of other failures
<u>K</u>	Trojan	E. 802.1x term referring to a client needing authentication
<u>G</u>	Worm	F. List of communication sessions between stations inside and outside the firewall that is maintained on the firewall
<u>C</u>	Malware	G. Self-propagating form of malicious software

<u>M</u>	Threat	H. Protected area of a network between the internal network and the Internet
<u>E</u>	Supplicant	I. Encryption standard used with WEP
<u>D</u>	Cascading failure	J. Process of sending packets with a fake source address
<u>N</u>	Certificate	K. Program that is expected to do one thing but actually does something else
<u>H</u>	DMZ	L. Term used to refer to the WAP during 802.1x authentication
<u>F</u>	Dynamic state list	M. Any potentially adverse occurrence that can harm the network or its data, interrupt network services, or cause a monetary loss
<u>J</u>	IP Spoofing	N. Secure identifier issued to a company, computer, or person that proves they are who they say they are
		O. Symmetric key encryption standard originally developed by IBM
		P. Software that monitors and records computer activity

Project 11.2	Using Auditing and Event Logs
Overview	<p>You can configure auditing to automatically track selected network activities, even failed attempts to perform audited activities. Auditing can be set up individually on computers or, when configuring auditing for network computers on an Active Directory domain, through Group Policy. In Windows 2008, everything is divided into Roles and Features. <b>Roles</b> are major “changes” to a server. <b>Features</b> are, more or less, “Add/Remove Windows components”. The Group Policy Management Console, which we use in this exercise, is installed as a “Feature”.</p> <p>Audit events, as well as other types of events, are tracked in the Windows Event Logs. You should review the contents of the Event Logs on a periodic basis and whenever you have computer or network problems. During this project, you’ll set up auditing. You’ll also review Event Log contents and save the contents of an Event Log to create a permanent record.</p>

Outcomes	After completing this project, you will know how to: <ul style="list-style-type: none"><li>▲ configure auditing</li><li>▲ manage Event Logs</li><li>▲ review Event Log contents</li></ul>
What you'll need	To complete this project, you will need: <ul style="list-style-type: none"><li>▲ the following worksheet</li><li>▲ a computer running Windows 7 Professional or Windows 7 Enterprise</li><li>▲ a domain controller running Windows Server 2008</li></ul>
Completion time	30 minutes
Precautions	<p>The instructions in this project assume you are working on a two-node network with one computer running Windows 7 Professional or Windows 7 Enterprise and one computer running Windows Server 2008. If these computers are part of a larger classroom network, your instructor will provide you with alternate instructions.</p> <p>If working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.</p>

## ■ Part A: Configure Auditing Policy

You configure auditing for your domain during Part A. You should be logged on to the computer running Windows Server 2008 as Administrator at the start of this project. When you installed Windows 2008 and promoted it to a Domain Controller, Group Policy Management Console wasn't in your Administrative Tools.

1. Open the **Start** menu, and select **Administrative Tools** and then **Server Manager**. If not already expanded, expand your domain.
2. Scroll down to **Features/Add Features** and select **Group Policy Management**.

- Click *Next* and *Install*, as shown in Figure 11-1.

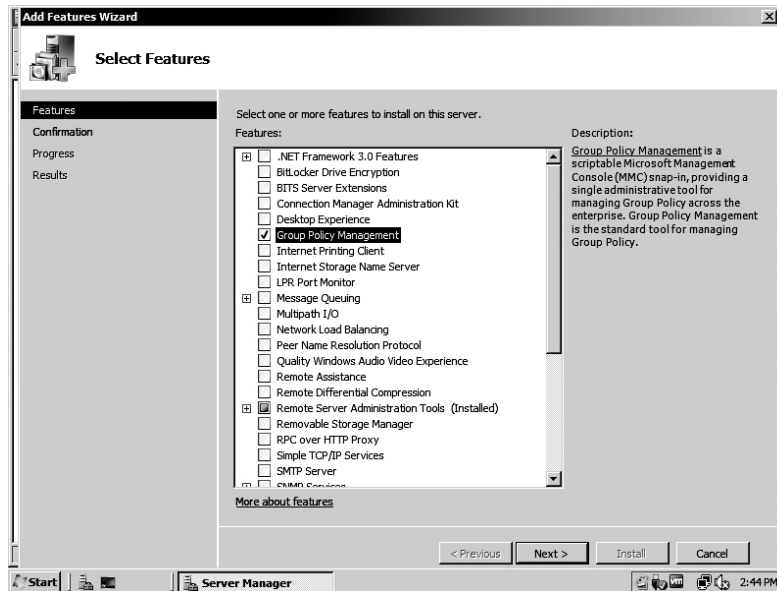


Figure 11-1: Installing Group Policy Management Console

- At the Server Manager window, expand **Group Policy Management**, **Forest, Domains**, **Busicorp.com**, and select **Default Domain Policy** as in Figure 11-2.

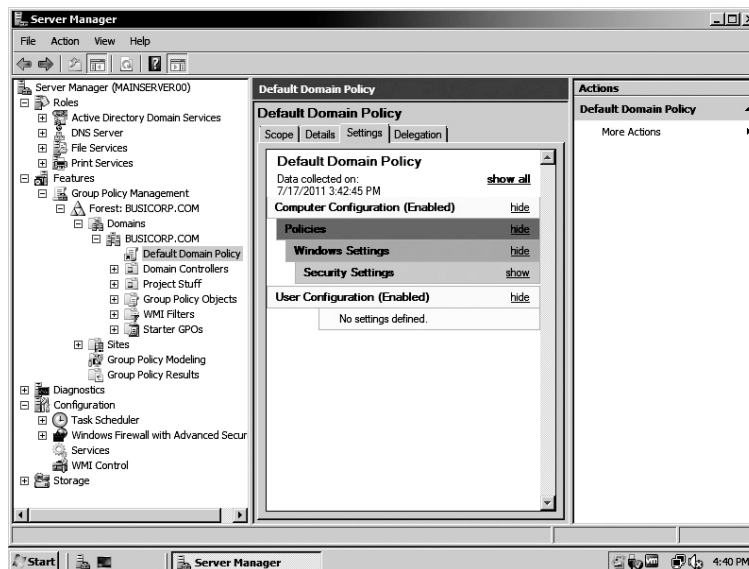


Figure 11-2: Default Domain Controllers Policy

- Right-click on **Default Domain Policy** and choose *Edit*.
- Under **Computer Configuration**, expand **Windows Settings**, **Security Settings**, and **Local Policy**. Select **Audit Policy**, as shown in Figure 11-3. Your policy settings may differ from those shown in the figure.

**Note:** You can also open the **Security Settings** portion of **Default Domain Controllers Policy** by opening the **Start** menu, selecting **Administrative Tools** and then **Local Security Policy**. This gives you access to the **Security Settings** policies only. You can also do this by opening the **Group Policy Management Console** from **Administrative Tools**.

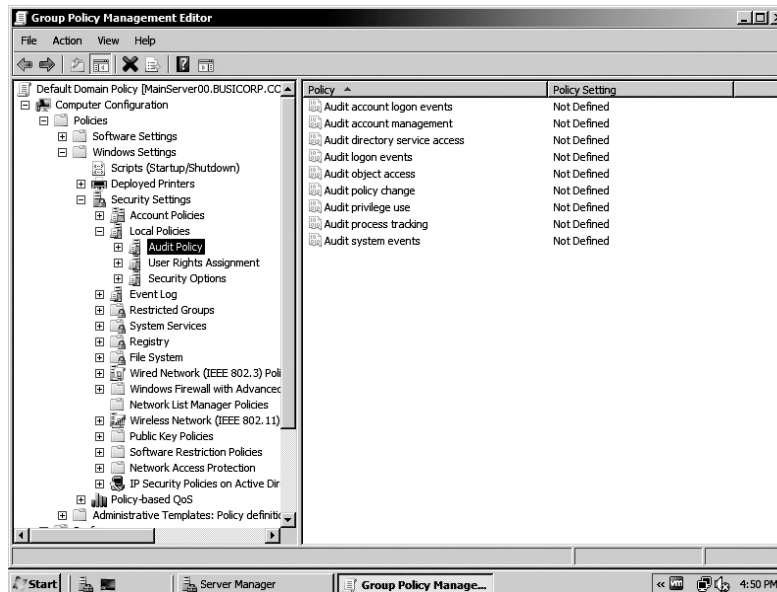


Figure 11-3: Audit Policy

- Right-click on **Audit logon events** and select **Properties** and the **Explain** tab, as indicated in Figure 11-4.

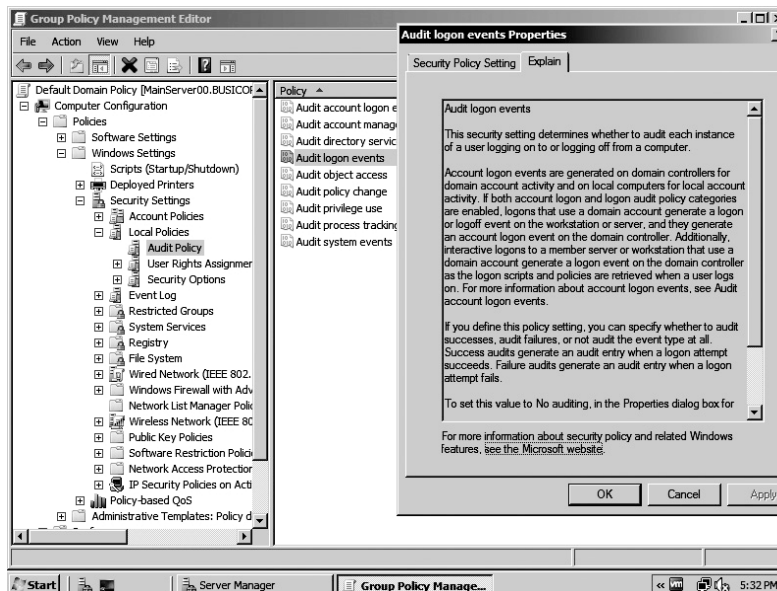


Figure 11-4: Audit Logon Events

8. Read the description. What is the advantage of logging failed attempts on a domain controller?

---

**Você pode identificar uma tentativa de um brute-force attack.**

---

9. What type of valid actions, those not related to a security breach, might generate the same?

---

**Um usuário que tenha esquecido sua senha e comece a tentar diversas.**

---

10. Take time to read the remaining audit policies in the Help window and answer the following questions:

- a. When would an Audit logon event be generated on domain controller?

---

**Toda vez que uxieste uma atividade em uma conta de dominio.**

---

- b. What types of events are generated by the Audit system events policy?

---

**Eventos de Logon e Logoff.**

---

11. Click *OK* to close the **Explain** window.
12. Double-click **Audit account logon events**, enable the policy if not enabled, and check both **Success** and **Failure**. Click *OK*.
13. Double-click **Audit account management**, enable the policy if not enabled, and check both **Success** and **Failure**. Click *OK*.
14. Double-click **Audit Directory Service Access events**, enable the policy if not enabled, and check both **Success** and **Failure**. Click *OK*.
15. Double-click **Audit logon events**, enable the policy if not enabled, and check both **Success** and **Failure**. Click *OK*.
16. Double-click **Audit policy change**, enable the policy if not enabled, and check both **Success** and **Failure**. Click *OK*.
17. Double-click **Audit system events**, enable the policy if not enabled, and check both **Success** and **Failure**. Click *OK*.

**Note:** Do not close **Group Policy Management Console**.

## ■ Part B: Configure Security Policies for Audit Logs

In Part B, you will view and modify policies that affect security logs.

1. Under **Local Policies**, click **User Rights Assignment**.
2. Scroll down, locate, and select **Manage auditing and security logs**, as shown in Figure 11-5.

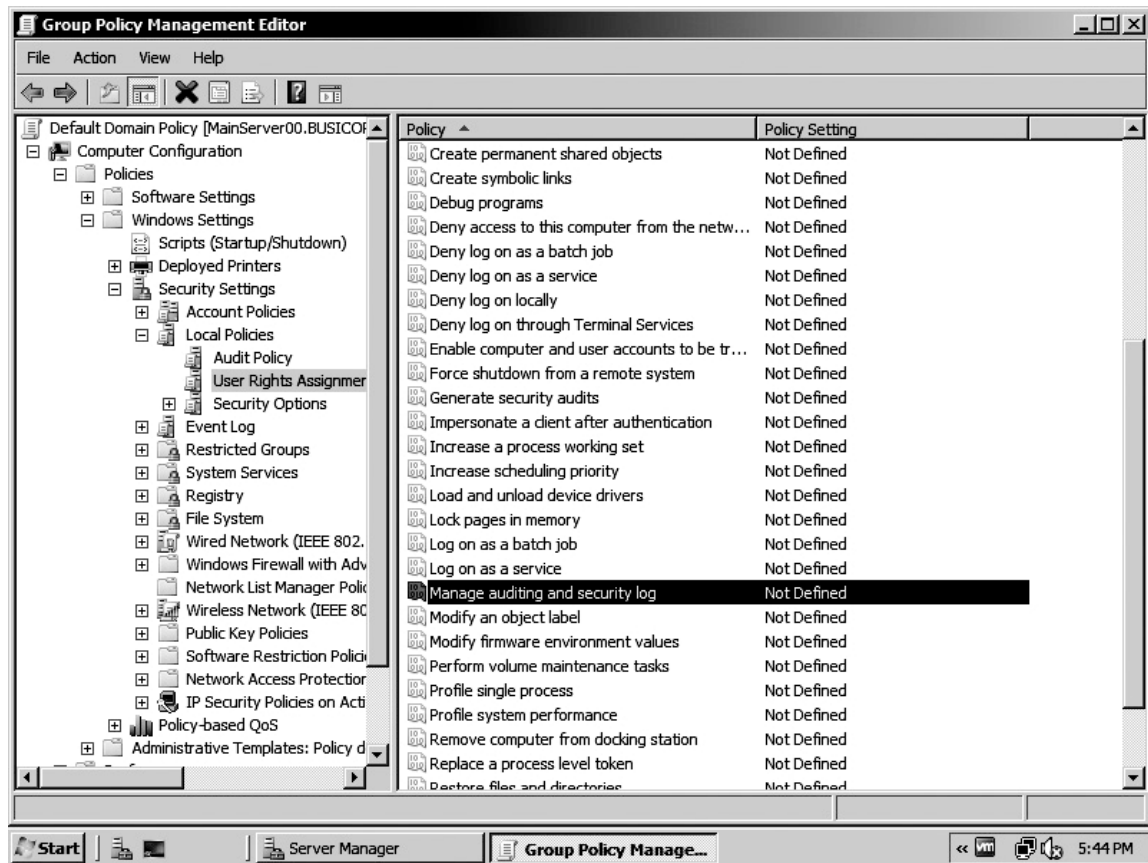


Figure 11-5: Manage auditing and security logs rights assignment

- Double-click to open the policy. What users have the right to manage auditing and security logs?

Os Adminsitrators do sistema tem esse privilegio por padrão, contudo nenhum outro usuario o possui.

- What is the potential risk of granting this right to other users or groups?

Um usuario com esse "right" pode apagar todos os logs de segurança, em caso de um possivel ataque, não existiram registros deles.

- Under **Local Policies**, click **Security Options**.



6. Locate and select **Audit: Shut down system immediately if unable to log security audits**, as shown in Figure 11-6.

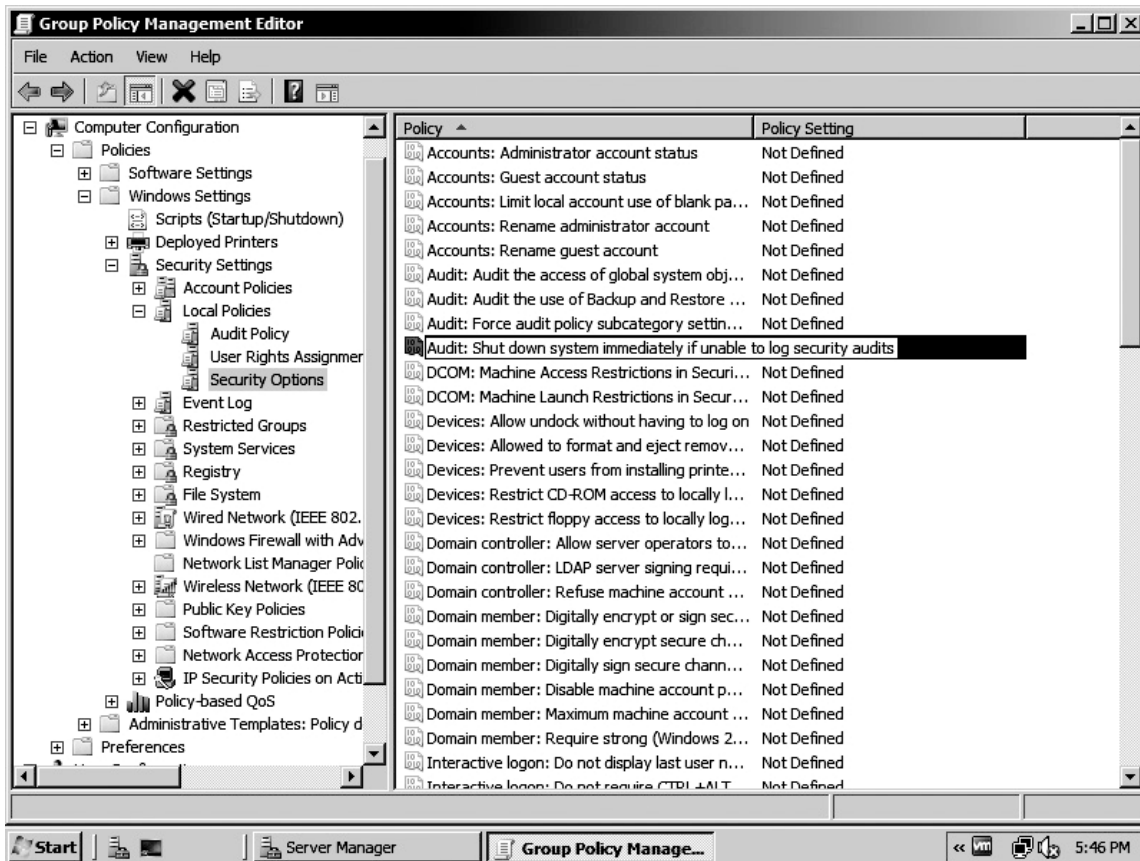


Figure 11-6: Security Options

7. What is the potential risk of enabling this policy?

Se por algum motivo o sistema não conseguir escrever um log de Audit, o sistema vai se desligar automaticamente, prejudicando usuarios que possam estar conectados.

8. Double-click and enable the policy, and then click *OK*.
9. Select **Event Log**, as shown in Figure 11-7.

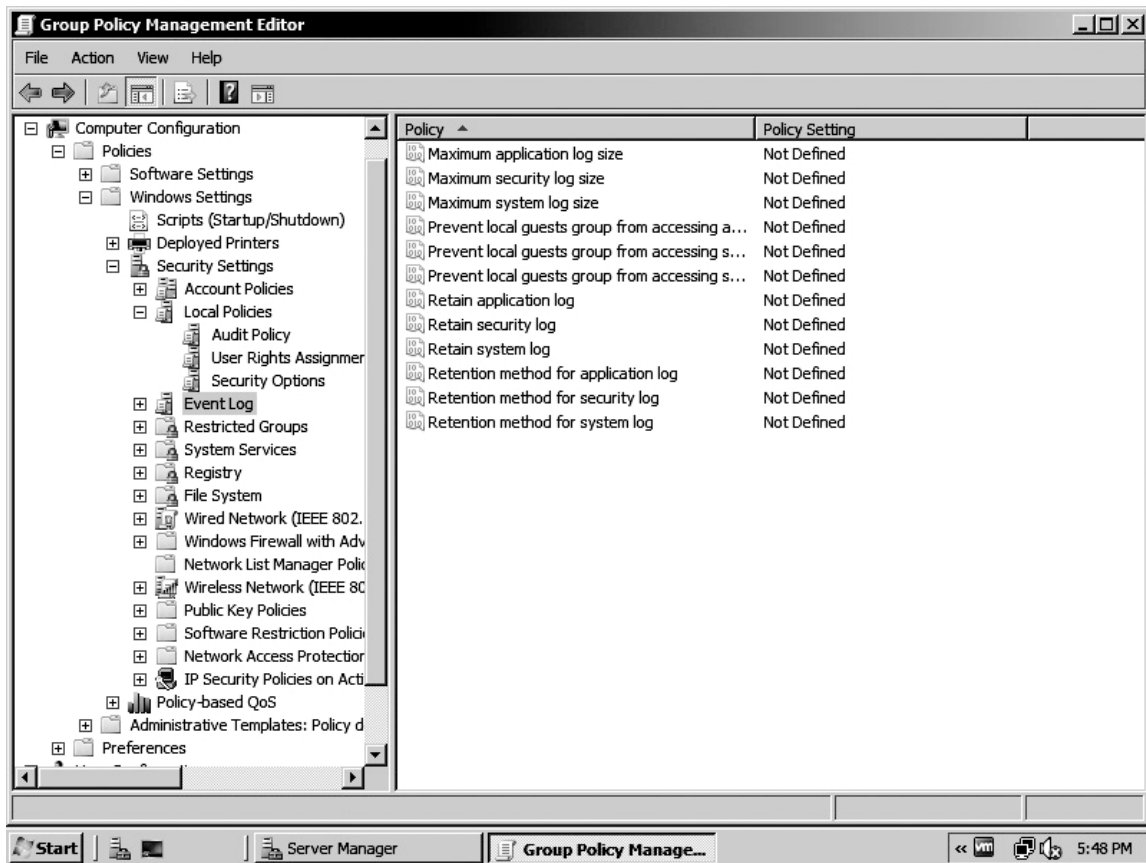


Figure 11-7: Event Log policies

10. Right-click **Maximum security log size** and select **Properties** and the **Explain** tab. What is the default log size on your domain controller?

O tamanho padrão é de 16MB.

11. In the **Help** window, select and review **Retain security log** and **Retention method for security log**.
12. Close the **Help** window.
13. Double-click **Retain security log** and check **Define this policy setting**.

14. What is the default period?

7 dias

---

15. Click *OK*.

16. What policy setting will be enabled automatically?

"Retention method for security log".

---

17. Click *OK*.

18. What is the potential risk if you don't archive the security log every week?

Você não terá registros de algo que possa ter dado de errado em seu servidor.

---

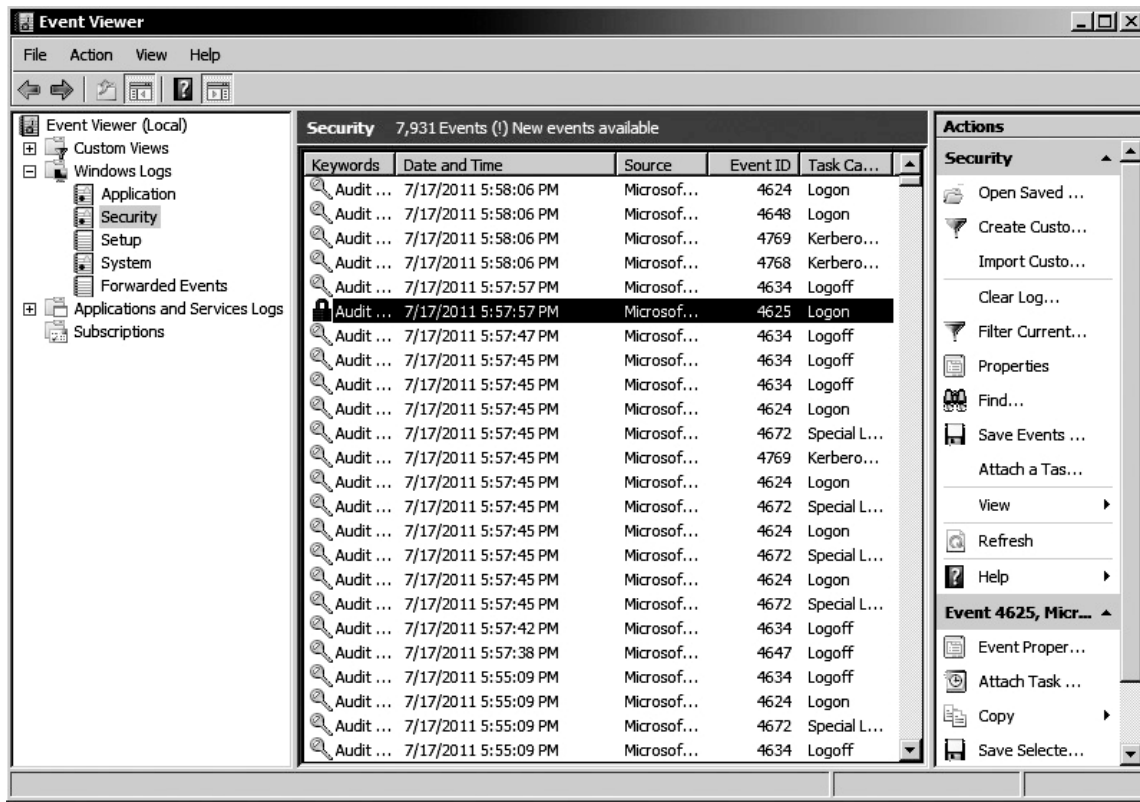
19. Close **Group Policy Management Editor** and then click *OK* to close **Server Manager**.

20. Exit **Active Directory Users and Computers**.

## ■ Part C: Generate and View Events

In Part C, you will generate Account Logon events and view them in Event Viewer. You will use your domain controller.

1. Log off your domain controller.
2. Press *Ctrl + Alt + Del* to display the logon dialog.
3. Enter the password for Administrator incorrectly and click *OK*.
4. Click *OK* to clear the warning.
5. Enter the password for Administrator correctly and click *OK*.
6. Open the **Start** menu, and select **Administrative Tools** and then **Event Viewer**.
7. Select **Security**. You should see entries similar to those shown in Figure 11-8.



### Figure 11-8: Security log

8. Locate and double-click the most recent **Failure Audit** event. What does it tell you?

O evento diz: "An account failed to log on."

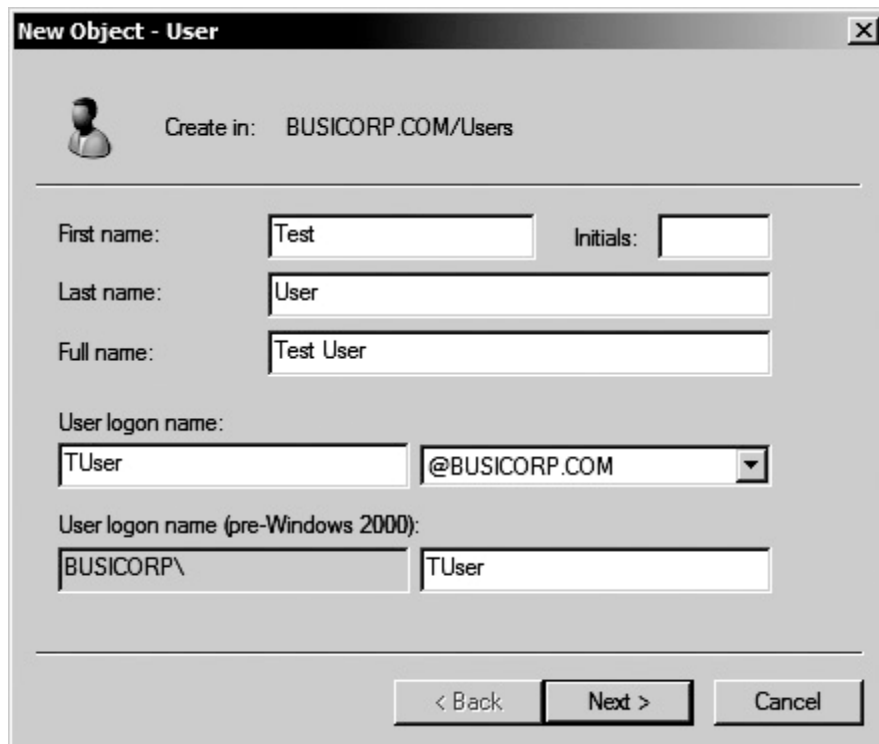
9. What is given as the client address?

O endereço dado é o 127.0.0.1

10. What does this tell you and why?

Diz que alguém o localhost (127.0.0.1) tentou entrar na máquina e não conseguiu.  
O porque disso é o fato de termos digitado a senha de maneira errada.

11. Click *Cancel*.
12. Launch **Active Directory Users and Computers**.
13. Position the windows so you can see both **Event Viewer** and **Active Directory Users and Computers**.
14. Right-click **Users** and choose **New User**.
15. Fill in the dialog box, as shown in Figure 11-9, and then click *Next*.



The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: BUSICORP.COM/Users'. Below this, there are several input fields: 'First name:' with 'Test', 'Initials:' (empty), 'Last name:' with 'User', and 'Full name:' with 'Test User'. Underneath, 'User logon name:' has 'TUser' in the text box and '@BUSICORP.COM' in the dropdown menu. Below that, 'User logon name (pre-Windows 2000):' has 'BUSICORP\' in the text box and 'TUser' in the adjacent text box. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 11-9: Test User

16. Enter and confirm **P@SSw0rd** as the password and click *Next*.
17. Click *Finish*.
18. In the **Event Viewer** window, right-click **Security** and choose **Refresh**.
19. Double-click the bottom **Account Management** event (the first **Account Management** event after the events generated by the Administrator logon), as shown in Figure 11-10.

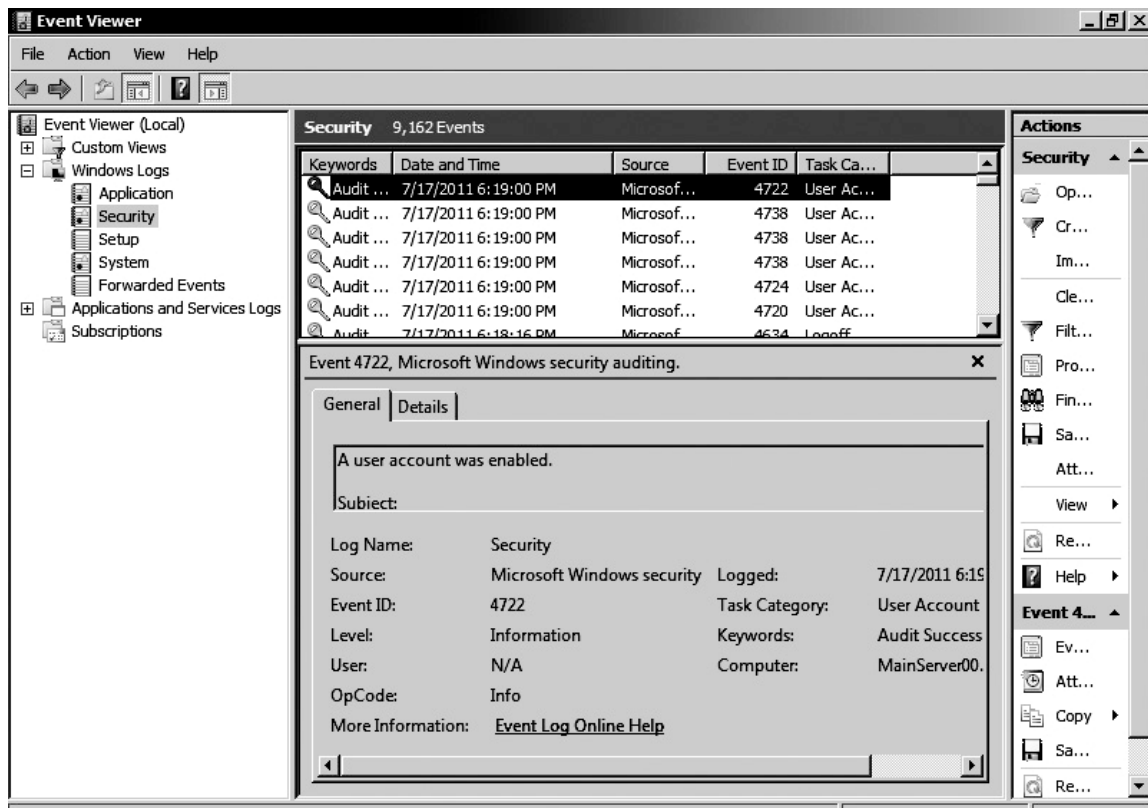


Figure 11-10: Account management events

20. Double-click the event. What does it tell you?  
Diz que uma conta de usuario foi criada.
21. Click the *Up* arrow until you get to the next **Account Management** event. What does this event tell you?  
Diz que uma conta de usuario foi habilitada.
22. Click the *Up* arrow and review through the remaining **Account Management** events.
23. After reviewing the events, click *Cancel*.
24. Close **Active Directory Users and Computers** and **Event Viewer**.

<b>Project 11.3      Managing Account Lockout Policy</b>	
Overview	<p>Account lockout policy is one of the best tools available for preventing unauthorized access attempts. You can set the number of attempts before the account is locked, the time-out period before account locking resets itself, and the length of time the account remains locked.</p> <p>During this project you will configure and test account lockout policy for your domain.</p>
Outcomes	<p>After completing this project, you will know how to:</p> <ul style="list-style-type: none"> <li>▲ configure account lockout policy</li> <li>▲ test account lockout policy</li> </ul>
What you'll need	<p>To complete this project, you will need:</p> <ul style="list-style-type: none"> <li>▲ a domain controller running Windows Server 2008</li> <li>▲ a computer running Windows 7 Professional or Windows 7 Enterprise</li> <li>▲ to complete Project 11.2</li> <li>▲ this following worksheet</li> </ul>
Completion time	30 minutes
Precautions	<p>The instructions in this project assume you are working on a two-node network with one computer running Windows 7 Professional or Windows 7 Enterprise and one computer running Windows Server 2008. If these computers are part of a larger classroom network, your instructor will provide you with alternate instructions.</p> <p>If working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.</p>

### ■ Part A: Configure Account Lockout Policy

In this part of the project, you will configure account lockout policy for the domain. You should be logged on to your domain controller as Administrator.

1. **Start** menu, selecting **Administrative Tools** and then **Group Policy Management**, as in Figure 11-11.

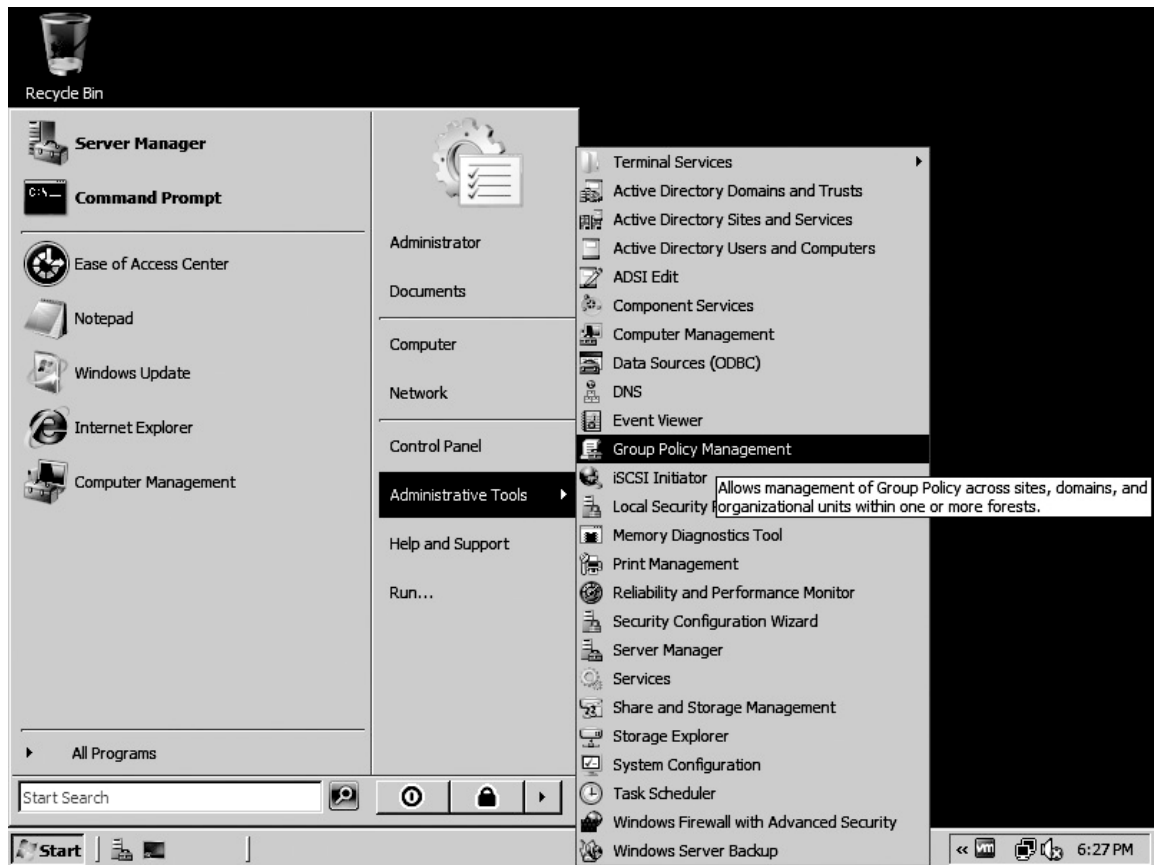


Figure 11-11: Default Domain Policy

2. Right-click on **Default Domain Policy** and select *Edit*.



- Under **Computer Configuration**, expand **Windows Settings**, **Security Settings**, and **Account Policies**. Select **Account Lockout**, as in Figure 11-12.

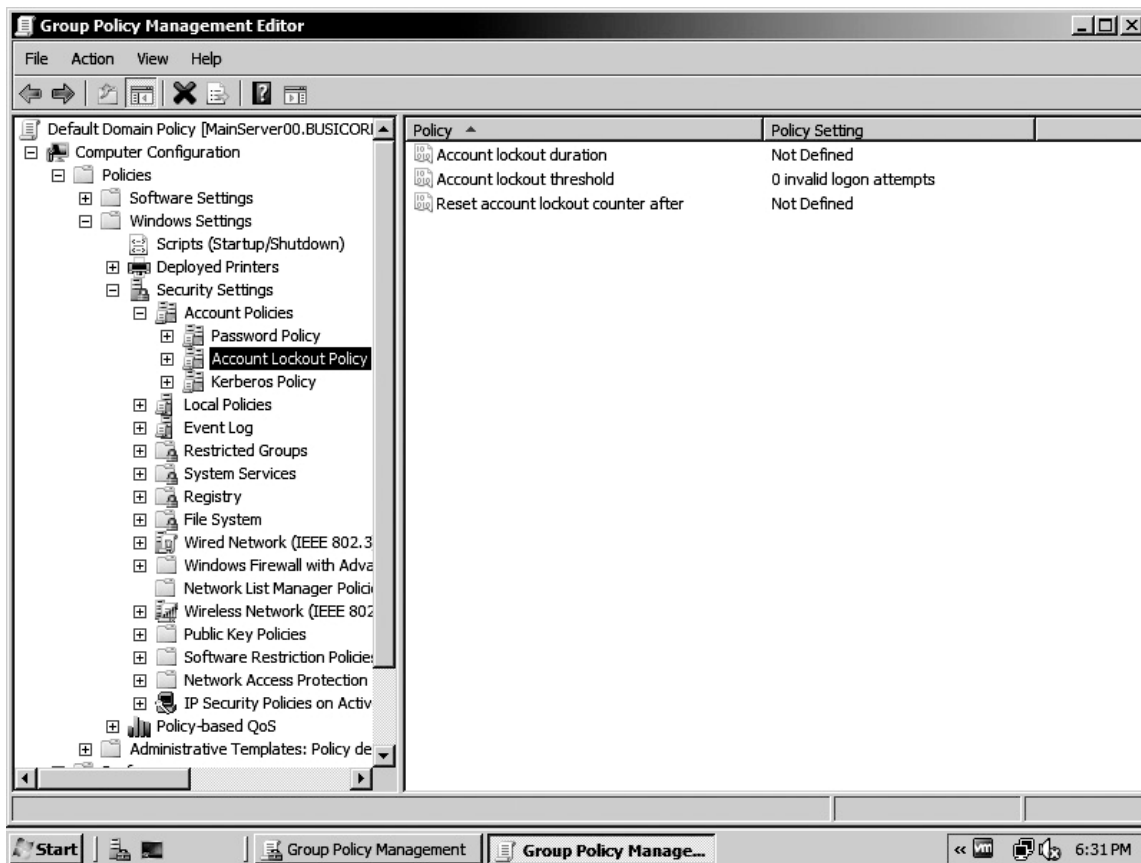


Figure 11-12: Account Lockout policies

- How is account lockout currently configured?  
Todas as suas configurações estão como "Não Definidas".
- Double-click **Account lockout duration**. Click **Define this policy setting** and set the lockout duration 10 minutes.
- Click **OK**. What other suggested values are displayed?  
Account lockout threshold com 5 invalid logon attempts e Reset account lockout counter after com 10 minutos.
- Click **OK**.

8. Double-click **Account lockout threshold** and change the value to **2**, and then click **OK**. Your policy settings should look like Figure 11-13.

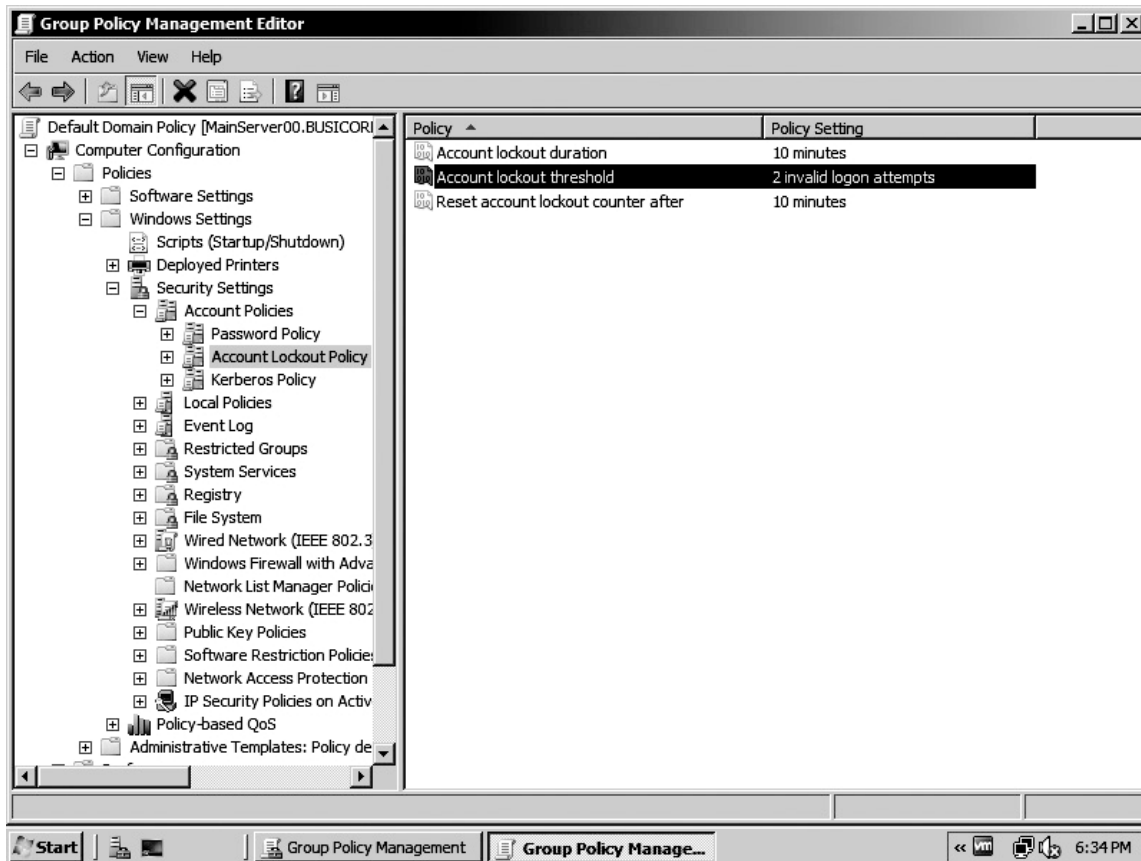


Figure 11-13: Account lockout enabled

9. Close the **Group Policy Management Editor** and exit **Group Policy Management Console**.
10. Launch **Event Viewer** and select the **Security** log. You are going to clear the log to make it easier to see entries generated by account lockout.
11. Select **Action** and then **Clear all events**. Click *No* when prompted to save the log contents.
12. What does the event that was entered tell you?

Que todos os logs de auditoria foram limpos do sistema.

**Note:** Do not exit **Event Viewer**.

## ■ Part B: Test Account Lockout Policy

You will lock a user account and generate lockout events in Part B. Shut down and restart the computer running Windows 7 Professional or Windows 7 Enterprise before starting this part of the project.

1. Attempt to log on as **TUser**. Enter the wrong password. What does the dialog box tell you?  
Diz: "The user name or password is incorrect."
2. Click *OK* and attempt to log on again as **TUser** with the wrong password. What happens?  
Diz: "The user name or password is incorrect."
3. Click *OK* and attempt to log on again as **TUser** with the wrong password. What happens?  
Diz: "The referenced account is currently locked out and may not be logged on to".
4. Click *OK* and attempt to log on again as **TUser** with the correct password. What happens?  
Diz: "The referenced account is currently locked out and may not be logged on to".
5. Click *OK* to clear the dialog box.

## ■ Part C: Unlock the Account and Cover Your Tracks

During Part C, you will unlock the user account and take actions to cover your tracks.

1. In **Event Viewer**, right-click **Security** and select **Refresh**.
2. Locate and open the first failure audit event. It should look similar to the example shown in Figure 11-14.



Figure 11-14: Failure audit event

3. What does this event tell you?

Que a Pre-autenticação do Kerberos falhou.

4. Click the *Up* arrow. What does the next event tell you?

**Que a Pre-autenticação do Kerberos falhou.**

---

5. Click the *Up* arrow until you locate the event showing the account locked out, like the example shown in Figure 11-15.



Figure 11-15: Account locked out event

6. Is this a successful event instead of a failed event?

**Sim, esse é considerado um evento "Success".**

---

7. Click *Cancel*.
8. Launch **Active Directory Users and Computer**. Select the **Users** container and locate **Test User**.
9. Right-click **Test User** and select **Properties**.
10. Select the **Account** tab. Notice that the account is locked, as shown in Figure 11-16.



Figure 11-16: Locked account

11. Check **Unlock Account** and then click **Apply/OK**.
12. Exit **Active Directory Users and Computers**.
13. Refresh the **Security** log. Should the events generated when you unlocked the account be Success or Failed Audit events, and why?

É um evento do tipo "Success" pois a alteração pode ser feita.

14. Open the most recent event. It should show that the account was unlocked. If not, click the *Down* arrow until you locate the account unlock events.
15. Using the procedures described earlier, clear the **Security** log. What events are now in the log?

Apenas um evento dizendo que o log foi limpo.

16. What would another administrator be able to tell about the attempted security breach that just occurred?

Que alguém com acesso ao Administrator foi capaz de apagar todos os registros.

17. What might cause an administrator to think that someone has just tried to clear his or her tracks?

Difícilmente o Adminsitrador do sistema vai apagar todos os logs existentes.

18. Exit **Event Viewer**.

Project 11.4 Managing Password Policy	
Overview	<p>User accounts and passwords are part of your first line of defense against unauthorized access. Each user should have his or her own user account. Each user account should be protected by a password, and passwords should be changed on a periodic basis.</p> <p>One potential problem is that many users tend to select weak, or easily guessed, passwords. You can use password policies to control password length, complexity, and how often users must change passwords.</p> <p>During this project, you will configure and test password policies. You will set domain policies that apply to all domain user accounts.</p>
Outcomes	<p>After completing this project, you will know how to:</p> <ul style="list-style-type: none"> <li>▲ configure password policy</li> <li>▲ test password policy</li> </ul>
What you'll need	<p>To complete this project, you will need:</p> <ul style="list-style-type: none"> <li>▲ a domain controller running Windows Server 2008</li> <li>▲ a Windows 7 Professional or Windows 7 Enterprise domain member</li> <li>▲ a domain user account</li> <li>▲ to complete Project 11.2</li> <li>▲ the following worksheet</li> </ul>
Completion time	30 minutes
Precautions	<p>The instructions in this project assume you are working on a two-node network with one computer running Windows 7 Professional or Windows 7 Enterprise and one computer running Windows Server 2008. If these computers are part of a larger classroom network, your instructor will provide you with alternate instructions.</p> <p>If working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.</p>

## ■ Part A: Configure Password Policy

In Part A, you will configure the default domain policy to set your password policy. The password policy, unless it has been changed, is at the Active Directory domain default settings.

1. Click **Start**, click **Administrative Tools**, and then choose **Group Policy Management** as shown in Figure 11.11 earlier in this chapter.
2. Right-click on **Default Domain Policy** and select *Edit*.
3. Under **Computer Configuration**, expand **Windows Settings**, **Security Settings**, and **Account Policies**. Select **Password Policy**, as shown in Figure 11-17. This figure also shows default password policies. Your settings should be similar.

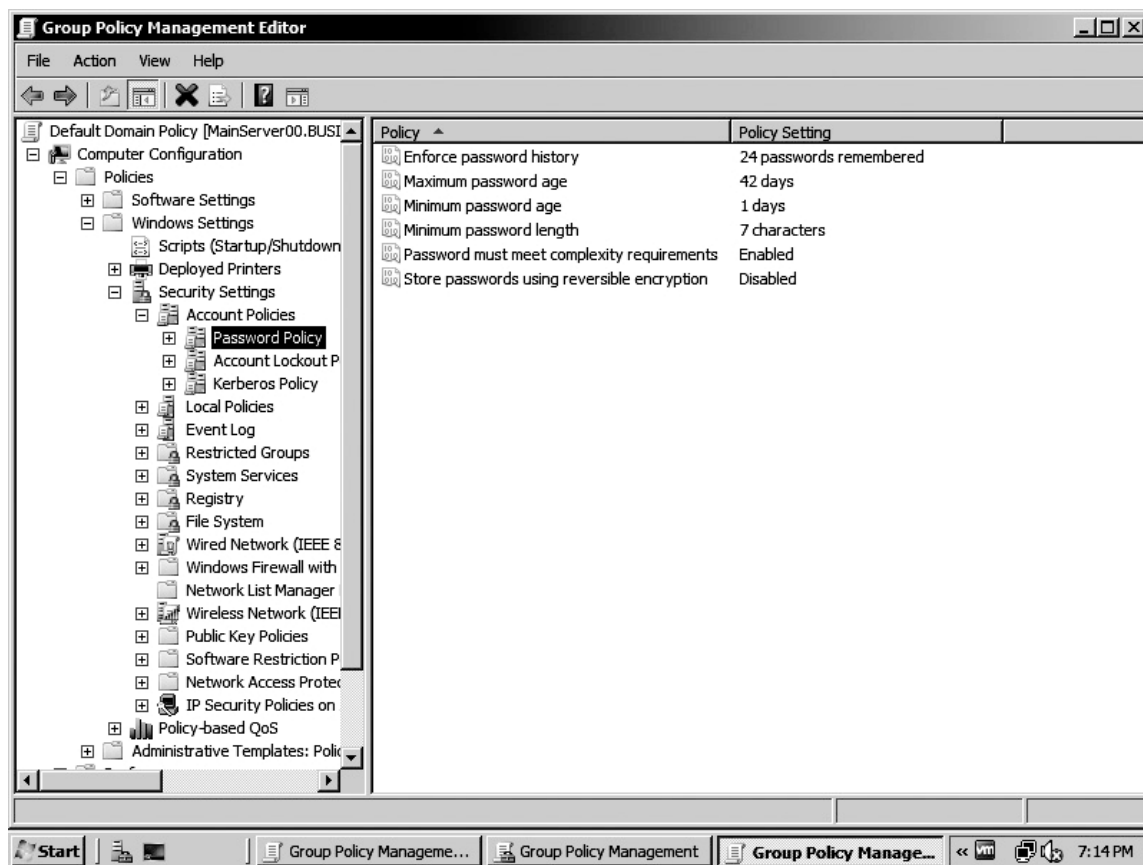


Figure 11-17: Domain password policy



4. Select **Enforce password history**, right-click on it, select **Properties** and the **Explain** Tab Review for each of the password policies, and then close the window.

- a. What is the possible risk in setting the maximum password age policy to too great a value?

Quanto maior o tempo para expirar a senha, mais tempo um cracker vai ter para tentar crackear a senha de um usuário da rede.

---

- b. What is the possible risk in setting the minimum password length too long?

Nessa configuração o usuário vai ter um tempo mínimo para poder trocar a senha caso esse valor seja alto, ele não poderá trocar a senha até que esse valor em dias seja atingido. Ou seja, se o valor for 100, ele deve esperar 100 dias para trocar a senha.

---

- c. What is the impact, if any, on existing passwords when you change password length or complexity so that they are no longer valid?

As senhas que não se adequarem as mudanças vão ser redefinidas obrigatoriamente no próximo login do usuário.

---

- d. What is the maximum value for **Enforce password history**?

O valor máximo é 24.

---

5. Open **Maximum password age**, increase the value to **60**, and click *OK*.
6. Open **Minimum password length**, increase the value to **8**, and click *OK*. Your password policies should look like Figure 11-18.

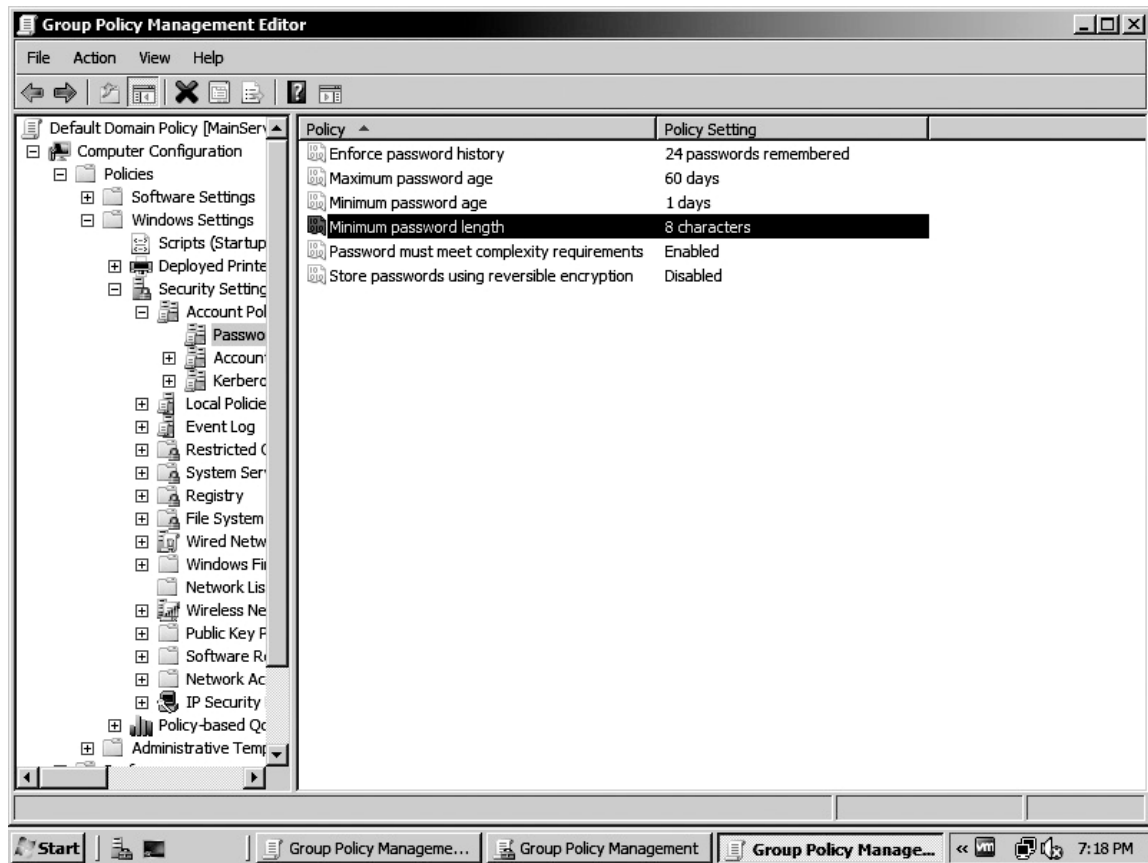


Figure 11-18: Modified policies

7. Close the **Group Policy Management Editor**, and then click *OK* to close the domain **Properties** dialog box.

*Note:* Do not exit **Active Directory User and Computers**.

## ■ Part B: Test Password Policy

In Part B, you will test which password policies apply when an administrator resets a user's password. Open **Start/ Administrative Tools/Active Directory User and Computers**.

1. Select the **Users** container and locate **Test User**.
2. Right-click **Test User** and select **Reset Password** to open the **Reset Password** dialog box, as shown in Figure 11-19.

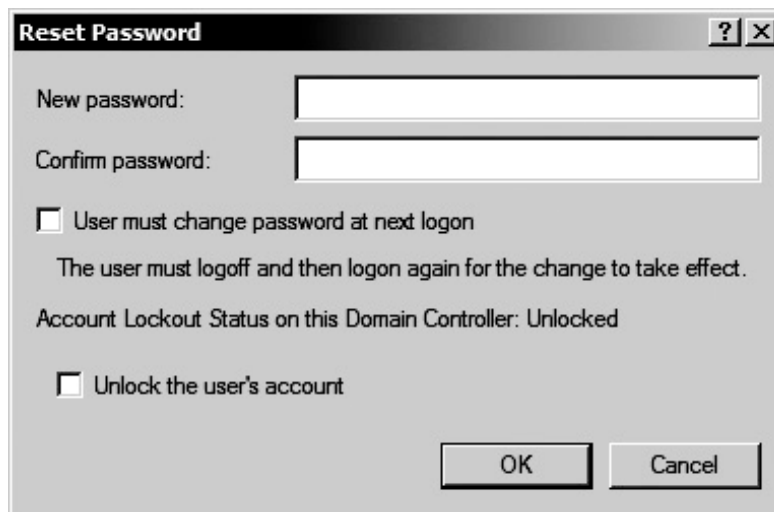


Figure 11-19: Reset Password dialog box

3. Enter and confirm the password *Password* and click *OK*.
4. What happens?

**Um aviso diz que a senha digitada não atende aos requisitos.**

---

5. Click *OK*.
6. Test the following passwords:

P*ssword	One234&5
P@\$\$WORD	1@#rr
tHisIzMin2	ne234567
One234%	

7. Which passwords are accepted as valid?

**P\*ssword , tHisIzMin2 , One234% , One234&5**

---



---



---



---

8. For the remaining passwords, explain why they were not accepted.

P@\$WORD não contém nenhuma letra minúscula.

1@#rr não contém nenhuma letra maiúscula e não possui 8 caracteres.

ne234567 não contém nenhuma letra maiúscula.

9. Set the password to **P@SSw0rd**.

10. Check **User must change password at next logon** (see Figure 11-20) and click **OK**.

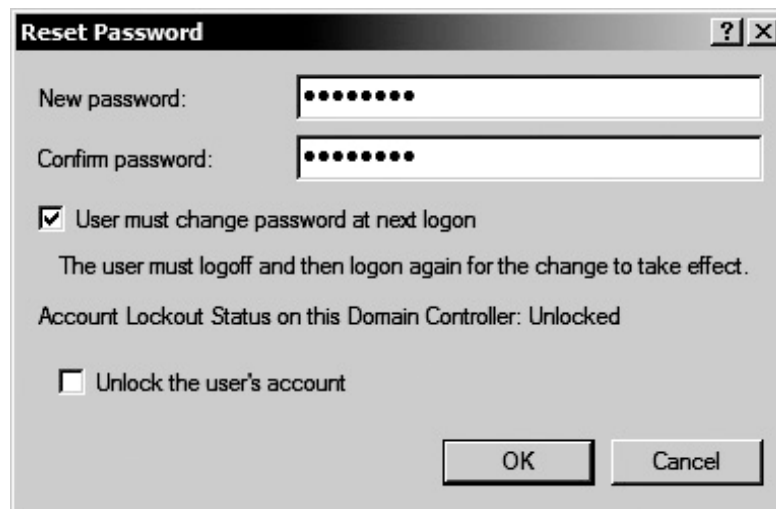


Figure 11-20: Forcing password change

11. What is the advantage to checking **User must change password at next logon** when resetting a user's password?

A pessoa que resetou a senha do usuário pode colocar uma senha fácil e temporária pois o usuário vai ser obrigado a muda-la depois.

12. Which password policies are not enforced when an administrator resets a user's password and how do you know this?

---



---



---

13. Exit **Active Directory Users and Computers**.

## ■ Part C: Test Passwords

In Part C, you will test which password policies apply when a user makes password changes. You will complete this part of the project on the computer running Windows 7 Professional or Windows 7 Enterprise. If logged on to the computer, log off.

1. Press *Ctrl + Alt + Del* (*Ctrl + Alt + Insert*) to open the **Log On to Windows/Other User** and use **TUSER**, as shown in the dialog box shown in Figure 11-21.



Figure 11-21: Log On to Windows dialog box

2. Log on using the password **P@SSw0rd**. What happens?  
 Uma mensagem informando que devo mudar minha senha antes de logar.
3. Why?  
 Pois o administrador requisitou isso ao resetar a senha do usuario.
4. Click **OK**.
5. Enter **password** as the new password and click **OK**.
6. What happens?  
 Diz que a senha não é válida para a password policy.
7. How does this password violate password policy?  
 Ela não possui letras maiúsculas, números e caracteres especiais.

8. Click *OK* to close the warning. Enter the old password (**P@SSw0rd**) and then **P@SSw0rd** as the new password and click *OK*.

9. What happens?

Diz que a senha não é valida para a password policy.

10. How does this password violate password policy?

É uma senha usada anteriormente, isso não respeita o History da Password Policy.

11. Click *OK* to close the warning. Enter the old password (**P@SSw0rd**) and **P@\$\$word** as the new password and click *OK*.

12. What happens?

Um aviso informando que a senha foi alterada é exibido.

13. Click *OK*.

14. After logon is complete, press *Ctrl + Alt + Del* to open the **Windows Security** dialog box.

15. Click *Change Password*.

16. Enter the old password and **passW@4d** as the new password (see Figure 11-22), and then click *OK*.



Figure 11-22: Change Password dialog box

17. What happens?

**Diz que a senha não é valida para a password policy.**

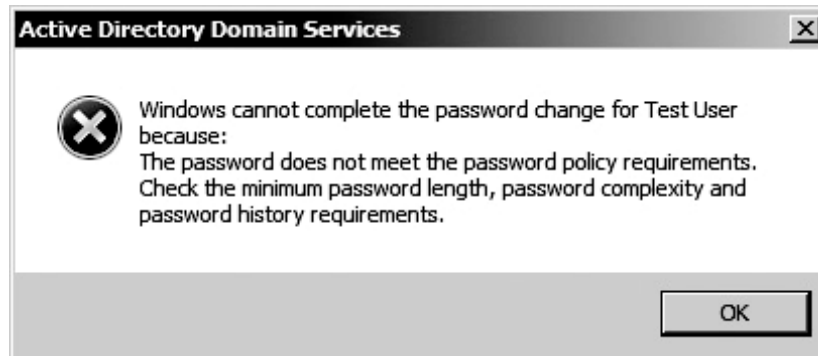
---

18. How does this password violate password policy?

**O tempo minimo para mudar a senha ainda não foi atingido.**

---

19. Click *Cancel* and then click *Cancel* again. The dialog box displayed for any password change error is shown in Figure 11-23.



**Figure 11-23: Password complexity error**

20. What is the advantage to displaying the same dialog box, no matter what error is preventing the user from changing the password?

**Um invasor não consegue descobrir as Password Policies configuradas.**

---

21. What option does Test User have for changing the user account password?

**Esperar um dia, ou pedir para o Administrator resetar sua senha.**

---

Project 11.5	Designing for Security
Overview	<p>An important part of securing your network is being aware of potential security problems and designing your network to be secure, which includes hardening the network as a whole, as well as individual clients and servers on the network.</p> <p>The Internet has hundreds of sources of security information and security tools. Operating system and application manufacturers have information available online for their specific products. Other sources, such as SearchSecurity.com, provide links to information and security tools. However, you need to exercise caution and download only from known sources. Some “security” Web sites are actually distribution points for viruses, Trojans, and other types of attacks.</p> <p>During this project, you will answer questions related to network security design and securing network computers.</p>

Outcomes	After completing this project, you will know how to: <ul style="list-style-type: none"> <li>▲ recognize security threats</li> <li>▲ design a network to minimize threats</li> <li>▲ configure computers to minimize threats</li> </ul>
What you'll need	To complete this project, you will need: <ul style="list-style-type: none"> <li>▲ the following worksheet</li> </ul>
Completion time	30 minutes
Precautions	None

## ■ Part A: Secure Network Design

In Part A, you will make network design decisions based on security requirements. Some of the questions refer to the network diagram shown in Figure 11-24.

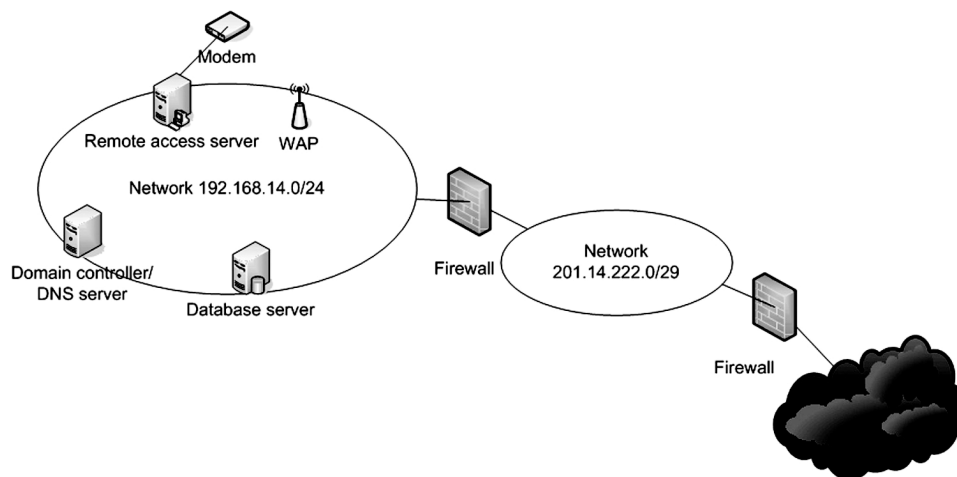


Figure 11-24: Sample network

1. What kind of network is network 201.14.222.0/29?  
**É o IP público da rede.**


---
2. What types of servers would you place on that network?  
**Nenhum.**


---
3. You are using an inner firewall that implements dynamic packet filtering. How does that impact the data passed by the firewall?  
**O firewall pode impedir que alguns dados sejam passados por ele.**


---



---



4. What would be necessary to configure the network using a single firewall?

---

---

5. What are the possible entry points into the network?

O servidor de acesso remoto e o WAP.

---

6. Which is likely the biggest security risk and why?

O servidor de acesso remoto, se ele não tiver uma configuração segura, algum invasor pode tomar conta da rede inteira invadindo ele.

---

7. The WAP supports both WEP and WPA. Which is more secure?

WPA é mais seguro.

---

8. What authentication protocol does WPA use?

TKIP (Temporal Key Integrity Protocol)

---

9. What configuration changes should you make in relation to the WAP's SSID?

Não deixar ele visível.

---

10. What can you use to have the Web server identify itself and your company to visitors?

---

---

11. The network is configured as a Windows Active Directory domain. Remote users are authenticated by the domain. You suspect that domain user names have been compromised. What policies can you implement to help detect and prevent unauthorized access and how would they help?

---

---

---

---

---

12. The network is attacked by a flood of SYN packets. What is the general term for this type of attack?

Ataque DoS.

13. What is the difference between a DoS and a DDoS attack?

O ataque DoS parte de um unico PC, o DDoS parte de uma botnet.

14. You want to add a subnetwork as a screened subnet. What would this require?

Um outro roteador.

## ■ Part B: Network Server Placement

In Part B, you will place network servers on a network diagram. You will use Figure 11-25 with this part of the project.

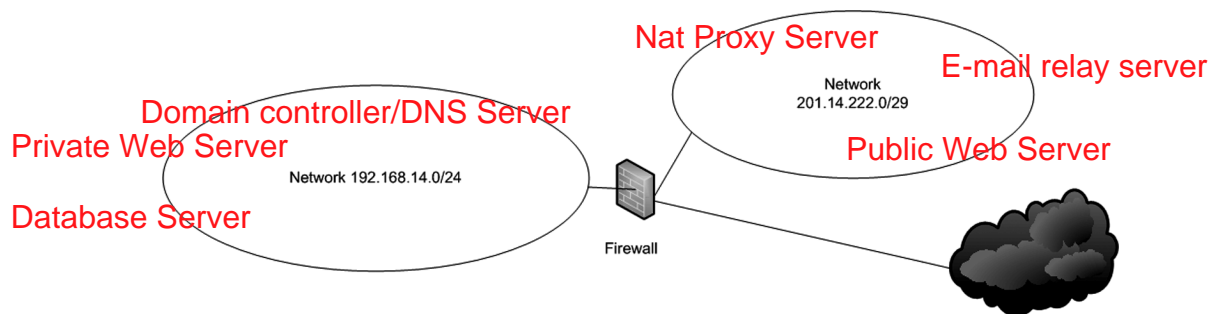


Figure 11-25: Another sample network

Indicate on Figure 11-25 where you would place the following:

- Public Web server
- Private Web server
- E-mail relay server
- Database server
- Domain controller/DNS server
- NAT Proxy server

## ■ Part C: Secure Network Computers

You will make security decisions that relate to individual network computers in Part C.

1. What steps can you take to prevent virus infection?  
**Reforçar as regras do firewall e instalar anti-virus em todas as maquinas.**  

---

---

---

---
2. What is the advantage of implementing a software-based firewall on each client computer?  
**Você aumenta a segurança individual de cada computador.**  

---
3. You want to ensure that the same password policy is used for all computers in an Active Directory domain. Where should the group policy object be linked?  
**Ao Domain Controller.**  

---
4. What is the potential risk if spyware is installed on a client computer?  
**Ele pode monitorar todas as atividades do computador, como o que o usuario digita.**  

---
5. What can a rootkit do if installed on a computer?  
**Ele pode fazer operações no sistema de forma camuflada.**  

---
6. How is a worm propagated between computers?  
**Pela rede ou pelo servidor de e-mail.**  

---

---
7. How does a spam filter protect a computer?  
**Evitando que e-mails maliciosos cheguem para o usuario.**  

---

