Domain Controlling

Group Policy with Active Directory Part II

Matt Kirkland & Jonathan Buch

March 10, 2017
Version 1.5

University of Idaho

CS 439: Applied Security Concepts

Abstract

The purpose of this document is to be a continuation of the material of the Domain Controlling: Group Policy with Active directory document. The tutorial outlined in this document expands on basic knowledge of AD and GPO by having the learner perform AD account management, auditing of group policy, add new group policy, and modify those policies further. The purpose is to acquaint the learner with AD and GPO systems in a very practical sense.

Contents

1 Objectives of this Tutorial >

1. AD account management
2. Auditing with GPO
3. Program level policy configuration

2 Required Background <>

1. Basic understanding of AD and Group Policy objects
2. Ability to work with virtual machines (i.e. Virtual Box, VMware, etc.)
3. Basic understanding of security concepts

3 Review of AD and GPO <>

Last time we worked with...

1. Password Policy
2. Passwords in AD
3. AppLocker

4 Questions 1,2 <>

Q1: What utility does AD and GPO provide with regard to password management?

Q2: Why would you use AppLocker?

Answer to Q1:
It allows AD admin(s) to set the acceptable length, complexity, and password history along with other options that apply to password creation and use. It can also dictate how passwords are stored and their encryption method.

Answer to Q2:
AppLocker has a incredible amount of power over access to files, folders, and applications. It allows a server admin to dictate access to certain parts of a system. As was seen in the last tutorial, AppLocker has the ability to block nearly anything. If used incorrectly, it can cause severe problems for a system. (Principle of Least Privilege)

5 Challenge: Reactivate Account <>

Darth's account is locked out. Unlock his account using the Domain Controller (i.e. Windows Server)

6 Task: Alice's logons <>

Find Alice's last successful logon attempt
On the Windows 7 VM:

1. Open up File Manager
2. Navigate to C: → Windows → System32 → winevt → Logs → Security
3. Read the logs and find the last success for Alice

7 Task: Auditing Policy Change <>

1. Open Group Policy Management
2. Within radicl.security, edit Default Domain Policy
3. Navigate to → Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy
4. Change Audit Policy Change to audit on success

8 Challenge: Account Lockout <>

Discover why Darth's account was locked out.

9 Task: Adding Group Policy (Win Server VM)<>

1. Open the policy_templates folder on the desktop. Navigate to windows → admx and copy chrome.admx
2. Then, navigate to Computer → Local Disk C: → Windows → PolicyDefinitions and paste the chrome.admx here
3. Navigate back to policy_templates → windows → admx → en-US and copy the chrome.adml file
4. Go back to Computer → Local Disk C: → Windows → PolicyDefinitions → en-US and paste the chrome.adml here

[1]

10 Questions - 3,4 <>

Q3: Why are audits and logs useful?

Q4: What is the benefit to adding new group policies?

Answer to Q3:
Audits and Logs are useful because they allow a way to figure out who caused what if a problem occurs. Also, it helps keep users accountable for their actions while on the server. Checking logs and auditing regularly can also catch problems before they occur.

Answer to Q4:
The benefit to adding new group policies is being able to configure applications that you add to the server. It lets you choose how an application will function and how a user will be able to use it.

11 Challenge: Configure Chrome Policy <>

1. Disable developer mode
2. Set startup pages
3. Disable ending processes in Chrome Task Manager
4. Black list "Google"
5. Set Google Chrome to default browser

12 Questions - 5 <>

Q5: Why is configuring application-level policy important to understand and implement as a server administrator?

Answer to Q5:
If an administrator couldn't configure Group Policy at the application level, they would have to either completely allow or disallow an application. This gives the administrator a greater degree of granularity when distributing access and usage rights to users.

13 Conclusion <>

We have looked at...

1. Managing Active Directory accounts
2. Auditing policy changes and AD users activity
3. Configuring application level group policy

14 Bonus Challenge: Configure IE <>

1. Disable developer mode
2. Disable searching from address bar & disable search box
3. Enforce protected mode

15 Appendix <

1. Solutions to challenges
2. Network Diagram
3. Setup details
4. Change log
5. References

Solutions to Challenges

1. **Challenge: Reactivate Account**
   (a) On the Windows Sever follow these steps.
   (b) In **Server Manager** go to **tools** and select **Active Directory Users and Computers**.
   (c) Navigate to **radicl.security** → **Users** → **Darth**.
   (d) Right click and select **Properties**. Select the **Account** tab.
   (e) Check the box **Unlock account**. Click **Apply**.

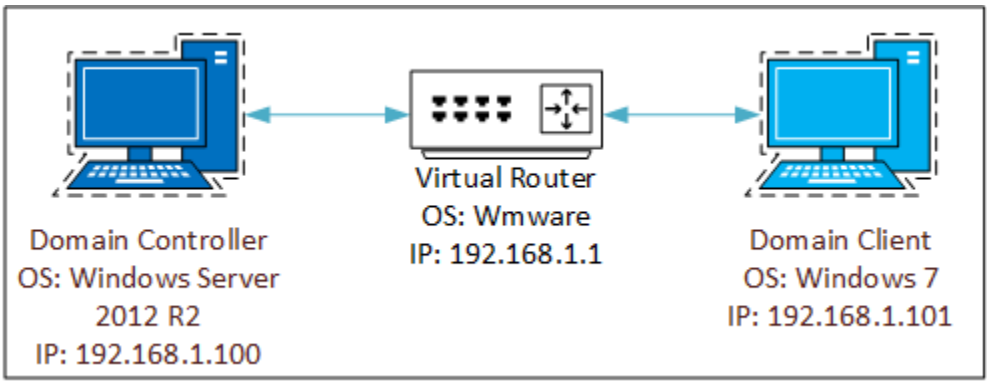
2. **Challenge: Account Lockout**
   (a) On the Windows 7 machine follow these steps.
   (b) Log in as the local administrator.
   (c) Navigate to **Local Disk (C:)** → **Windows** → **System32** → **winevt** → **Logs** → **Security**. Double click.
   (d) Search for the logs stating that Darth failed to log on 4 times. Thus he was locked out.

3. **Challenge: Configure Chrome Policy**
   Under default domain policy editor, navigate to **Computer Configuration** → **Administrative Templates** → **Google** → **Google Chrome**. All of the policies are in this folder!

4. **Bonus Challenge: Configure IE**
   Under default domain policy editor, navigate to **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Internet Explorer**. All of the policies are in this folder!

Network Diagram

In order for the tutorial to succeed, the two machines must be connected properly. The Windows Server 2012 R2 (DC) and Windows 7 (domain member) must be on the same network. Static IPs were set to both VMs. For a tutorial on setting static IPs, we recommend: **Change TCP/IP settings**. In the section on IPv4 you want to set a manual IP address. Also for the purpose of the tutorial the client needs to set it's DNS IP to be the server's IP. How that is done is also outlined on the linked document. [2]



Setup details

In this tutorial, we made use of 2 VMs: Windows Server 2012 R2 (DC) and Windows 7 (domain member). After setting up the network, as outlined in the **Network Diagram** section, the Server needs to be made a Domain Controller and the client needs to be added to it's domain. The procedure for how to do that is outlined in the previous tutorial: Domain Controlling: Group Policy with Active Directory. See the sections "Setting up Domain" and "Adding Clients".
After setting up the Server and Client, a few AD accounts must be made and account policy must be changed. Here we explain how that setup is done.

Set the account lockout threshold, timeout, and authentication failure auditing
On the Windows Server:

1. Open Group Policy Management
2. Within radicl.security, edit Default Domain Policy
3. Navigate to → Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Account Lockout Policy
4. Change "Account lockout threshold" to 3 invalid logon attempts. Click "Apply".
5. Change "Account lockout duration" to 0 minutes. Click "Apply". This will make it so that any locked account must be unlocked by an administrator.
6. Under Security Settings, navigate to Local Policies → Audit Policy.
7. Change "Audit logon events" to include audits for failures. Click "Apply". This will log failed attempts to authenticate a user to the AD server.

Create Darth and Alice's AD Accounts
On the Windows Server:

1. Open Active Directory Users and Computers
2. Within radicl.security, right click on Users and select new *rightarrow* user.
3. Fill in the some information and create a password for Darth. Click Finish once done.
4. Repeat the previous steps to create a user named Alice.

On the Windows Client:

1. Invalidly log in to the AD using Darth's account 3 times. You should receive an error message stating that the account must be unlocked by an administrator.
2. Perform only 2 invalid logon attempts for Alice. This should NOT lock her account.

Change Log

Change(s)	Contributor(s)	Effective Date
First draft of tutorial	Matthew Kirkland and Jonathan Buch	March 10th, 2017
Added abstract, network diagram, and expanded Setup details section	Matthew Kirkland	May 10th, 2017
Correct grammar and spelling errors for final publishing	Jonathan Buch	May 11th, 2017
Standardized formatting	Ananth Jillepalli	June 15th, 2017

References

[1] Windows OS Hub, "How to Configure Google Chrome via Group Policies", last accessed 10th March 2017, http://woshub.com/how-to-configure-google-chrome-via-group-policies/, 6th JANUARY 2015.

[2] Microsoft Support, "Change TCP/IP settings", last accessed 10th May 2017, https://support.microsoft.com/en-us/help/15089/windows-change-tcp-ip-settings, 31st AUGUST 2016.