Getting Started with
Windows Server Security

Windows Server 2012 provides security features and solutions that can be used as standalone security solutions as well as integrated solutions with your existing security or auditing tools.

To begin, you will learn how to implement baseline security using Microsoft Security Configuration Wizard and how to lock down unwanted services, along with how to configure your Windows firewall. You will see how to enable and use native tools including AppLocker to identify and mitigate risks and tighten up your Windows Server infrastructure security.

This book also walks you through best practices for designing and building a secure Microsoft server platform, with instructions on configuration and managing Dynamic Access Control and policies.

At the end of the book, installation and configuration of Windows Server Update Services, which plays a crucial role in the security space, is covered.

Who this book is written for

If you are a security or Windows Server administrator wanting to learn or advance your knowledge in Microsoft security and secure your Windows Server infrastructure effectively, this book is for you.

What you will learn from this book

- Design a secure Windows Server platform based on the best practices and industry standard recommendations
- Identify and mitigate security risks using tools such as Security Configurations Wizard, ASA, AppLocker, BitLocker, and EMET
- Follow step-by-step instructions to tighten the security of your Active Directory file, print server, Hyper-V and IIS servers, and application roles
- Develop a secure access control mechanism using the Dynamic Access Control (DAC) feature
- Learn how to maintain security and deliver new security updates and patches using the Windows Server Update Service (WSUS)
- Discover how PowerShell cmdlets and custom scripts can support your day-to-day security admin tasks

In this package, you will find:

- The author biography
- A preview chapter from the book, Chapter 6 'Access Control'
- A synopsis of the book’s content
- More information on Getting Started with Windows Server Security

About the Author

Santhosh Sivarajan is a recognized subject matter expert in the Microsoft technology arena. He has extensive experience in designing, migrating, developing, and implementing enterprise solutions using Microsoft products and technologies. He holds a master's degree in computer information systems from the University of Houston, Texas. His certifications include MCITP, MCTS, MCSE, MCSA, Network+, CCNA, ITIL, and many more. He is also a certified migration expert in Quest Migration Manager products.

His blog (http://blogs.sivarajan.com) and SS Technology Forum (http://www.sivarajan.com/forum) are well known in the industry for providing free technical information and support. You can follow Santhosh on Twitter via @santhosh_sivara.

He is the author of the book Migration from Windows Server 2008 to Windows Server 2012, Packt Publishing. He has also published hundreds of articles on various technology sites.

Microsoft has recognized Santhosh with the Microsoft Most Valuable Professional (MVP) award multiple times for his exceptional contribution to the technical community. He lives in Sugarland, Texas, with his wife, Anjali, who is also an IT professional, and their 3-year-old daughter, Gayathri.
Acknowledgments

First and foremost, I would like to thank God for giving me the power to believe in myself and pursue my dreams.

My IT enterprise journey started from Camp Doha with the US Army (now known as Camp Arifjan) in Kuwait. The support and encouragement from the ADPE group and other army personnel at Camp Doha helped me start my career with a strong foundation. I am dedicating this book to my old friends and colleagues in Camp Doha.

Of course, I could not have completed this book without the support and encouragement of my family, especially my wife, Anjali, and my daughter, Gayathri, for giving up some of our time together so that I could share my ideas through this book.

I am grateful to all my friends and colleagues for their support throughout my career. A special thanks to my Microsoft MVP friends for listening to me and supporting my ideas. A special thanks to the book reviewers, Yuri Diogenes, Richard Hicks, Richard Diver, and Jack Cobben, for providing their constructive criticism and feedback. I would also like to express my gratitude and thanks to the entire Packt Publishing team for this opportunity and their support throughout this process.
Getting Started with Windows Server Security

Welcome to Getting Started with Windows Server Security is a critical component for any organization. It can be implemented in various levels. Every organization has its own security policies based on their business and technical requirements. These policies must apply to end-to-end devices and services to effectively secure your IT infrastructure. As a security administrator, it is your responsibility to convert these business requirements into technical requirements. This book provides various methods to analyze your requirements and convert them based on the best practices and industry standards.

This book will walk you through different security tools and their configurations and implementation details based on my real-world experience. The goal is to have a protected and secure Microsoft Server infrastructure platform at the end of this journey. To achieve this goal in an efficient way, this book is divided into various chapters. Each chapter will provide you step-by-step instructions to secure your server infrastructure based on the installed components and applications on the server. For a security or Windows Server administrator, this book can be used as a reference manual when securing or hardening your server infrastructure.

What This Book Covers

*Chapter 1, Operating System and Baseline Security,* provides the details to translate your business requirements into a technical policy and implement these security policies in a Microsoft infrastructure environment. This chapter also covers instructions on creating and implementing Windows baseline policies using Microsoft Security Configuration Wizard.

*Chapter 2, Native MS Security Tools and Configuration,* provides an overview of various Microsoft tools and explains how they can be used in an enterprise to support your compliance and security needs. This chapter converts the configuration and implementation details of the Microsoft Security Compliance Manager, Attack Surface Analyzer, application control, and other auditing policies.

*Chapter 3, Server Roles and Protocols,* provides the details and methods to select correct server types and roles and identify and control unwanted services based on your requirements. It also provides a PowerShell-based solution to create and analyze baseline images based on the application or server type.

*Chapter 4, Application Security,* provides various options to create a secure server infrastructure platform for your application using Microsoft technologies. This chapter also covers the details to secure file and data servers, print servers, Hyper-V, web servers and encryption, and BitLocker technologies.
Chapter 5, Network Service Security, provides the details of protecting and controlling Microsoft network services. This chapter provides step-by-step instructions on securing Active Directory, Domain Controller, DNS, DHCP and configuration, and implementation details of gMSA and EMET.

Chapter 6, Access Control, provides an overview of the new access control mechanisms in Windows Server 2012. The step-by-step installation and configuration details of Dynamic Access Control are also included in this chapter.

Chapter 7, Patch Management, provides the details of maintaining the security and integrity of your Windows server using various Microsoft technologies. The step-by-step instructions on implementing and administering WSUS are also included in this chapter.

Chapter 8, Auditing and Monitoring, provides different options to audit and monitor your server infrastructure using various technologies. The details of auditing polices, GPOs, event forwarding, event alerting, and Best Practices Analyzer are also included in this chapter.
Access Control

Protecting data and maintaining sensitive data inside the organization is a challenge for any enterprise. Information or data leakage can adversely affect an organization in many ways. Minimizing or controlling access is key in maintaining the integrity and confidentiality of these types of data. In this chapter, you will learn about a new and secure access control mechanism for data and file servers. In a traditional method, there is no easy way to implement an access control mechanism based on the type or class of data. Also, the permissions are based on a static value of the control mechanism.

In Windows Server 2012, Microsoft introduced a new concept called Dynamic Access Control. As it sounds, this method can be used to implement a dynamic access mechanism on an Active Directory resource. This access mechanism can be implemented based on the types and properties of the resources.

The implementation and configuration details of DAC are included in the following sections.

Dynamic Access Control

As mentioned before, Dynamic Access Control (DAC) was introduced in Windows Server 2012. There are some requirements to support DAC in an enterprise. You need to have at least one Windows Server 2012 Domain Controller and the Active Directory Forest Functional Level (FFL) must be at least Windows 2003. Also, before you can start using the benefits of DAC, the Kerberos Key Distribution Center (KDC) support for claims, compound authentication and Kerberos armoring setting must be enabled on all Domain Controllers.
The details of DAC can be found at http://blogs.technet.com/b/windowsserver/archive/2012/05/22/introduction-to-windows-server-2012-dynamic-access-control.aspx.

On a higher level, the following steps are required to configure and implement a DAC mechanism in an Active Directory environment:

- Enable KDC support
- Create claim type
- Create resource properties
- Create Central Access Rule (CAR)
- Create Central Access Policy (CAP)
- Deploy Central Access Policy using GPO
- Configure file shares using Central Access Policy

The following sections provide step-by-step instructions on configuring these components.

**Enabling the KDC support**

We will start with Kerberos Key Distribution Center (KDC) support. This is a GPO-based configuration on Domain Controllers. The following instructions can be used to complete this configuration:

1. Open Group Policy Management Console.
2. Expand the Domain Name node and right-click on Default Domain Policy GPO. Select Edit.
3. It will open the Group Policy Management Editor window. Navigate to Computer Configuration | Policies | Administrative Template | System | KDC.
4. Select the KDC node. From the middle pane, double-click on the KDC support for claims, compound authentication and Kerberos armoring setting.
5. Change the configuration type to Enabled. Click on OK.
6. Close the **Group Policy Management Editor** window.

If required, update the Group Policy using the `GPUPDATE/Force` command or wait for the AD replication to complete. You need to make sure the new KDC support has been successfully applied on to the Domain Controllers. Once you have the KDC support, you can get started by creating the Dynamic Access Control components. Unlike other options and technologies, there is no dedicated management console for Dynamic Access Control. It is configured by using **Active Directory Administrative Center** (ADAC).

In this exercise, your goal is to protect employee information on your file server. You will need to make sure that only employees from the HR group can access the data.

### Creating claim types

As the first step in DAC configuration, you will be creating claim types based on your requirements. In this scenario, you need to create a claim type based on department values (HR). So you will be creating a claim type based on the **Department** attribute in Active Directory. The following section provides these instructions.
**Access Control**

The details of claim-based identify and access control can be found at https://msdn.microsoft.com/en-us/library/ff423674.aspx. Perform the following steps:

1. Open the **Active Directory Administrative Center** console.
2. Select the **Dynamic Access Control** node from the left pane.
3. Select **Claim Type** from the middle pane. From the right pane, select **New** and then **Claim Type**.
4. From the attribute list, select **Department**.
5. In the **Display Name** and **Description** boxes, select an appropriate name and description.

6. From the **Suggested Value** section, click on **Add**. Enter the department name in the **Add a suggested value dialog** box. Click on **OK**.
7. Leave **Claim Type** as **User** for this scenario. Click on **OK** to complete the claim type creation process.

---

**Creating and enabling resource properties**

The instructions in the following section provide the details of creating and enabling **resource properties** for the claim type:

1. Select **Resource Property** from the middle pane. From the right pane, select **New** and then select **Reference Resource Properties**.

2. In the **Create Reference Resource Properties** window, select the previously created claim type. Click on **OK**.
Creating a central access rule

At this stage, you have a claim type and resource properties. Based on this information, you can create access rules. The following instructions can be used to complete this process:

1. Select Central Access Rule from the middle pane. From the right pane, select New and then Central Access Rule.
2. In the **Create Central Access Rule** window:
   - Enter an appropriate name for the access rule in the **Name** box.
   - Leave **Target Resources** as **All Resources**.
   - From the **Permission** section, select the **Edit** button.

   - Select the **Add** option from the **Advanced Security Settings for Permission** window.
   - Click on the **Select a Principal** button to select the appropriate practical account. In this scenario, you will be selecting **Authenticated Users** as the principal.
   - From **Basic Permission section**, select **Full Control**.
From the bottom pane, select the **Add a Condition** link and enter the appropriate access rules here. In this scenario, you will be using the **Department=HR** condition, as shown in the following screenshot:

Click on **OK** twice to complete the operation.

3. Click on **OK** to complete the rule-creation process.

**Creating a central access policy**

The central access policy comprises of a central access rule. The following instructions provide the details of creating a central access policy based on a previously created central access rule:

1. Select **Central Access Policy** from the middle pane. From the right pane, select **New** and then **Central Access Policy**.

2. On the **Create Central Access Policy** window:
   - Enter an appropriate name for the access policy in the **Name** box.
   - From the **Member Central Access Rules** section, select the **Add** button and select the previously created access rule.

   The **General Policy** window displays the central access rules, as shown in the following screenshot. Click on **OK** to close the windows.
Deploying a central access policy

At this point, you have your access policy ready to be deployed. The deployment of access polices takes place through GPOs. The following section provides an option to deploy these central access polices using the GPMC:

1. Open **Group Policy Management Console**.
2. Expand the **Domain** option and select the appropriate OU. In this scenario, you will be creating a new GPO in **Servers OU**. If you have an existing OU, you can add these settings using the **Edit** option.
3. Right-click on **Servers OU** and select the **Create a GPO in this Domain, and link it here** option.

   ![](The%20Create%20a%20GPO%20in%20this%20Domain,%20and%20link%20it%20here%20option.png)

4. In the **New GPO** window, enter the name for this GPO. Click on **OK**.
5. Right-click on the newly created GPO and select the **Edit** option.

6. This will open a **Group Policy Management Editor** window.

7. Expand the **Computer Configuration** node and navigate to **Policies** | **Windows Settings** | **Security Settings** | **File System** | **Central Access Policy**.

8. Right-click on **Central Access Policy** and select the **Manage Central Access Policies** option.
9. From the **Central Access Policy Configuration** window, select the previously created access policy. Click on **Add**, and then on **OK** to complete this operation.

![Central Access Policies Configuration](image)

10. Close the **Group Policy Management Editor** window.

The GPO will be applied to all computer objects in **Servers OU**. The GPO can be manually updated by using the `gpupdate /force` command. The `gpresult /r` command can be used to verify the applied GPOs on the file server, as shown in the following screenshot:

![Computer Settings](image)
Configuring folder permissions on a file server

From an access policy perspective, you have completed all the required tasks. The next step in this process is to apply these access policies to a folder or share them on a file server. The following section explains the steps in detail:

1. Log on to the file server using administrative permission.
2. Right-click on Folder/Share and select Properties.
3. Select the Security tab and click on Advanced.
4. In the Advanced Security Settings window, you will see a new tab called Central Policy. If you don't see the Central Policy tab, verify the GPO settings and make sure that they applied on your servers.
5. Select the Central Policy tab.
6. From the Central Policy window, select the Change button.
7. From the drop-down box, select the previously created central access policy. You can click on the policy name to see the permission express configuration details.

8. Click on OK to complete the configuration.
Verifying access the control configuration and permission

The access control policy and effective permission can be verified by using the **Effective Access** option from the **Advanced Security** window:

1. Select **Effective Access** from the **Advanced Security** window.
2. From the **User/Group** section, click on the **Select a user** link.
3. From the **Select Users, Computer, Service Account, or Group** window, select the appropriate user and click on **OK**.
4. Click on **View Effective Access** from the **Advanced Security** window.
5. As shown in the following screenshot, you will see a red X indicating the access denied message along with the reason on the right-most column. In this scenario, the access policy was blocking the folder access based on the condition.

![Advanced Security Settings for HR_Share1](image-url)

- **Effective Access** allows you to view the effective permissions for a user, group, or device account. If the account is a member of a domain, you can also evaluate the impact of potential additions to the security token for the account. When you evaluate the impact of adding a group, any group that the intended group is a member of must be added separately.

- **Include group membership**
  - **Click Add**
  - **Add Items**

- **Include a user claim**
  - **Include a device claim**

- **Effective access**
  - **Full control**
  - **Write attributes**
  - **Read extended attributes**
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**

- **HR_Access_Rule1**

- **Access limited by**
6. Since our access policy was on the Department value, for testing purposes, you can change the Department value to HR to validate the result.

7. As shown in the following screenshot, you will see a green checkmark indicting that full access is granted based on the updated department value in Active Directory.
Summary

The goal of this chapter was to establish a secure access mechanism for protecting the data. I believe we can accomplish this task by introducing the concept called Dynamic Access Control. We looked at the DAC configuration and implementation details from an access and security mechanism perspective. File screening and classification can also be integrated with DAC to secure file servers and data. If interested, more information about these technologies can be found at http://technet.microsoft.com/en-us/library/dn383587.aspx.

In the next chapter, you will learn how to continually protect your server and server infrastructure using Windows Server Update Service (WSUS). The automation, implementation, and configuration details of WSUS are included in the following chapter.
Where to buy this book

You can buy Getting Started with Windows Server Security from the Packt Publishing website.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.

Click here for ordering and shipping details.