Active Directory and PowerShell for Jobseekers

Learn how to create, manage, and secure user accounts

Mariusz Wróbel

www.bpbonline.com

First Edition 2024

Copyright © BPB Publications, India

ISBN: 978-93-55515-872

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

To View Complete
BPB Publications Catalogue
Scan the QR Code:

www.bpbonline.com

Dedicated to

My beloved wife:

Ola

&

My lovely daughters:

Natalia *and* ***Nikola***

&

My mom:

Genowefa

About the Author

Marius Wróbel has 13 years of experience in IT, which includes 12 years of Active Directory experience as well. He began his career in smaller companies in Poland and later transitioned to larger organizations with offices and clients worldwide. Always prioritizing workload automation, he has been involved in numerous migration and integration projects that required strong scripting skills. Learning from experienced colleagues, he became a Security Engineer and transitioned into Active Directory and Security DevOps, upon joining one of the leading European cloud providers.

Now, as the owner of his own consulting company, he serves both domestic and international customers, focusing primarily on Cloud identity solutions that include Azure AD and Active Directory. Mariusz holds the position of Lead Directory Services Engineer at Adecco. He is also a graduate of Wroclaw University of Technology, having completed both a Bachelor's degree and a Master's degree in Computer Engineering. Meanwhile, he has successfully obtained many Microsoft certifications in Azure and Security and Identity technologies.

About the Reviewers

- **Miguel Regalado** is an Identity and Access management engineer. With a wealth of expertise in MFA, SSPR, Azure Active Directory, and more, this seasoned IT professional has navigated the dynamic landscape of technology. Armed with a solid understanding of Windows Server, strong authentication methods, and a certified Identity and Access Management Administrator with Security+, he forged his path at leading global enterprises. Rising from a graduate to lead Azure/Entra ID services, he oversaw contractors and championed innovations like SSPR and MFA. In his current role he continued to spearhead advancements in Azure AD/Entra ID. Actively engaging in technical reviews of internal documents, their narrative is one of unwavering dedication to staying on the cutting edge of technology, embracing challenges, and envisaging a connected future.

- **Vladimir Prokop** is a Microsoft System Design and Architecture expert with a robust background in platforms installation, configuration, and migration. His proficiency extends to Exchange Servers, Management Servers, and basic knowledge of SharePoint Portal. With hands-on experience in systems and network engineering, Vladimir excels in troubleshooting and problem analysis, as well as client and server-based machine repair and maintenance. He is well-versed in backup and disaster recovery procedures, anti-virus, and content filtering technologies, along with software firewalls and routers configuration. Vladimir specializes in Microsoft Windows Operating Systems, MS ISA Server, Exchange Server, System Management Server, Software Update Server, and Internet Information Server (IIS), including Apache Configuration. His expertise also covers Microsoft Office applications, Symantec Antivirus solutions, and Veritas Enterprise High Availability solutions. Vladimir Prokop is a highly skilled professional, bringing a comprehensive skill set to any organization's IT landscape.

Acknowledgement

I want to express my gratitude to my entire family for their immense support and encouragement throughout this book's writing. I extend my appreciation, especially to my wife Ola and my daughters and mother, Natalia and Nikola and Genowefa.

Without the support of my family I would not have been in a position to start working on this publication. Without their help and support, through my educational and professional career, I would not get anywhere close to the position I am in. Their continued encouragement has led to me completing this project successfully.

I am also grateful to BPB Publications for their support and help in bringing this book to fruition. A lot of time and effort has been put into this book; with valuable participation and collaboration of reviewers, technical reviewers, experts and editors.

Last but not the least, there would be no book, without me learning from many experienced colleagues in various companies that I had the pleasure to work with and work in. I tried to absorb as much information as possible. Moreover, working in different industries has helped me write this book from many different perspectives and I hope it is of help to all.

Preface

Managing Active Directory in large enterprise companies can be difficult to cope with as it comes with a complex set of responsibilities. A deep understanding of Windows Server and the Active Directory service is necessary to maintain a highly available and secure environment that meets the needs of customers.

As the approach to Windows Server administration is shifting towards scalability and automation, a comprehension of PowerShell is essential. This enables administrators to effectively manage Active Directory within extensive environments and facilitates the automation and standardization of deployments through a DevOps approach and cloud capabilities.

This book provides a detailed guide on how to build an Active Directory environment within a cloud infrastructure and configure it using standard tools and/or PowerShell automation. Throughout the book, readers will gain insights into the key features of Active Directory and learn how to leverage PowerShell for the administration of Active Directory environments. Additionally, the book covers security best practices and cloud automation, enhancing daily AD administration for greater efficiency and repeatability.

Moreover, this book is intended for anyone looking to start their career as a sysadmin and wishes to become familiar with Active Directory and PowerShell Automation, which requires basic Windows Server administration knowledge.

The following is what we will be covering in the chapters:

Chapter 1: Introduction - This chapter will cover the book's concepts, and acts as an invitation to embark on a journey to fully managed Active Directory, elucidating the nature of Active Directory and detailing methods for its management, using PowerShell. It will also showcase various tools applicable to PowerShell automation development, script execution on servers, and the management of Azure cloud infrastructure, with an example test environment deployment.

Chapter 2: Setting up the Development Environment - This chapter will provide a step-by-step guide on establishing the development environment, encompassing the creation of Azure IaaS for Active Directory deployment. It will also explain the process of setting up an Azure subscription, connecting the console to Azure, staging necessary VMs, and preparing resources using Azure PowerShell.

Chapter 3: Active Directory Environment Creation - This chapter will delve into the deployment of the Active Directory Forest, detailing the creation of the Root and child domains. It will elucidate design concepts and offer example scripts for automating the deployment process.

Chapter 4: Active Directory Environment Configuration - This chapter will cover the configuration and creation of the basic AD structure, including OUs, Sites, and Delegation. It will also explain FSMO roles and guide readers through the configuration process.

Chapter 5: Active Directory User Management- This chapter will encompass commonly performed tasks for user management, demonstrating both manual operations and automation using PowerShell.

Chapter 6: Active Directory Group Management - Focusing on Active Directory security tasks, this chapter will guide readers on automating these processes with PowerShell. It will also cover security auditing for sensitive accounts, including Kerberos delegation.

Chapter 7: Active Directory Security Management - This chapter, echoing the previous one, will further explore Active Directory security tasks and their automation using PowerShell. It will delve into security auditing for sensitive accounts, including Kerberos delegation.

Chapter 8: Monitor Active Directory- Explaining how to monitor the state of Active Directory services, this chapter will outline the automation of monitoring tasks using PowerShell scripts and tasks.

Chapter 9: Active Directory Disaster Recovery - Covering various disaster and recovery scenarios for Active Directory environments, this chapter will introduce scenarios ranging from single object and Domain Controller failures to entire domain/forest disasters. It will also provide guidance on protecting the AD environment in such cases.

Chapter 10: Manage Windows Server Using PowerShell- This chapter will guide readers on managing Windows Servers solely using PowerShell. It will introduce concepts like Windows Server Core and remote PowerShell sessions for management, as well as explain the utilization of Windows Admin Center for Active Directory Management.

Chapter 11: Securing PowerShell for AD Management - Detailing methods to maximize security for PowerShell operations, especially in terms of WINRM configuration and scheduled task permissions.

Chapter 12: PowerShell DSC for AD Configuration Management - Explaining the use of PowerShell DSC for maximizing security in Active Directory configuration management.

Chapter 13: Interview Questions - This chapter will share the author's experiences during their AD Sysadmin career, providing insights into the interview process.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/t7cg1qt

The code bundle for the book is also hosted on GitHub at **https://github.com/bpbpublications/Active-Directory-and-PowerShell-for-Jobseekers**. In case there's an update to the code, it will be updated on the existing GitHub repository. We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Introduction

Inspiration

Working in different companies, industries, divisions and teams can teach us many different types of Active Directory architecture. In various organizations, there are multiple ways of implementing robust, lean and high performance Directory Service solution. Starting with later versions of Windows, PowerShell scripting gained popularity and provided a great advantage to manage the Active Directory infrastructure. It also provided users with a way to improve the service from several perspectives.

There were several publications around Active Directory, most of them explained different areas of the solution and details of the implementation. The part that we missed was always thinking of the bigger picture along with how to interpolate Active Directory, what can be archived with different AD capabilities, and what are the best practices from the security point of view. It is beneficial that AD becomes a part of the security services in some companies, which shifted the focus from the enablement service to a more restrictive point of view.

There was also caution about implementing automation. PowerShell remoting was used in popular types of attacks, and big organizations were planning to disable it completely from their IT estate. On the other hand, smaller companies that grow dynamically needed to have an even more automated approach for managing Windows and AD infrastructure.

Understanding all the aspects of Active Directory and having the mindset of the person who always wants to automate IT work is very important. We can switch our effort from manual operations and use energy for different parts of the service, like security enhancement, monitoring and automation.

The purpose of this book is to explain and demonstrate all major aspects of implementation, maintenance and automation of Active Directory service and the underlying server infrastructure. It is a summary of the knowledge I gained while working in different industries, implementing different aspects of Active Directory Services and infrastructure required to host the AD service.

Introduction

So, you would like to know more about **Active Directory** (**AD**) and how to manage it effectively using PowerShell? If yes, this is the right book for you! There is lot of literature that explains either AD or PowerShell. In this book we try to provide a comprehensive overview of all necessary knowledge that is required for any sysadmin, that would need to pick up the workload of Active Directory administration and automation of AD management using PowerShell.

Today, AD is mostly used by organizations of all sizes that are utilizing Microsoft operating systems and software products. As a result, the demand of experienced IT professionals who can support such technology is significant; choosing that career path is remarkably interesting and can be a particularly good start before becoming a sysadmin or specializing in access management and becoming an identity and access management expert.

In different companies, there could be various types of AD solutions. From small, single-domain implementations to multi-domain, multi-forest organizations, learning PowerShell automation is a huge benefit to any administrator in any company. It allows you to switch your thinking about how you are managing your Windows Server and AD infrastructure, allowing you to be more proactive, reduce management overhead, and focus on more critical issues that need to be solved.

Of course, PowerShell is not the answer to every problem that is to be solved when implementing AD. When scripting is not the best option, you should focus on customer needs rather than pushing for PowerShell. Understanding all the possibilities will allow you to choose the best solution.

You do not need to have any previous knowledge about AD or scripting before diving into this book. This will be a good first step to helping you become an AD sysadmin familiar with how to utilize PowerShell in daily work. Let us get started!

Structure

This chapter will cover the following topics:

- Active Directory Overview
- Several types of Active Directory services
- AD domain and forest implementations
- PowerShell overview
- Getting started with PowerShell editors
- Diverse ways of Active Directory management using PowerShell
- Development environment overview

Objectives

This chapter will give you basic information on Active Directory and PowerShell. We will explain the basic Active Directory architectures and provide a basic overview of PowerShell History and versioning. We will get familiar with PowerShell Editor and define the requirements for AD test environment that will be managed using scripting and automation.

Active Directory overview

What is Active Directory? Well, there are many definitions of AD, but it is a directory service that can be implemented on the Windows Server Operating system. After completing the operating system configuration, you can enable the Active Directory Domain Services Role and start deploying AD.

There are multiple Active Directory services:

- **Active Directory Domain Services (ADDS)**: It is the base Active Directory service is required for an AD infrastructure. If Active Directory skill is required in the job description, it is about ADDS. Other services are optional, but the rest of Active Directory services require ADDS to be present.
- **Active Directory Certificate Services (ADCS)**: It is the Microsoft PKI services. PKI is the organization public key infrastructure that is based on digital certificates. When enabling that role, you can deploy private CA infrastructure that would rely on AD implementation in your organization and use the benefits of the Active Directory for certificate enrolment.
- **Active Directory Federation Services (ADFS)**: This makes it possible to federate the identities to applications as well, becoming the identity provider to other

external identity providers. It extends the Active Directory Domain Services with modern authentication protocols like SAML and Oath and limits the requirement of passing the credentials on applications.

- **Active Directory Rights Management Services (ADRMS)**: It is the service that protects information and ensures that only allowed people can read and modify specific documents and files. With an application that is integrated with RMS, you can define access policies and decide what level of access is required when working with sensitive information.
- **Active Directory Lightweight Directory Services (ADLDS)**: It is the implementation of LDAP database services. While ADDS provides extended capabilities, LDS is limited to provide LDAP directory without additional services. It allows integration of applications that require LDAP directory without Active Directory overhead. Here, you can implement multiple LDS instances on one server to support multiple applications with separate directories, while ADDS can only support one domain on one server.

When it comes to Active Directory, everyone refers to Active Directory Domain Services. That service is utilized in most organizations, and it requires the most effort for implementation and administration. ADFS and ADCS are commonly used, but learning about those services is much easier. In this book, we will focus on learning how to implement and administer Active Directory Domain Services.

Active Directory domain and forest implementations

As Active Directory was designed to support varied sizes of organizations, there could be multiple architecture implementations for AD. Most common architectures could be the following:

- Single forest, single domain
- Single forest, multiple domains
- Multiple forests, multiple domains

Single forest, single domain

This architecture is recommended by Microsoft for most small organizations. It contains only one domain that holds the entire AD forest. In this case, the single domain is the root domain, and name of the domains is the same as entire forest's name, as shown in *Figure 1.1*:

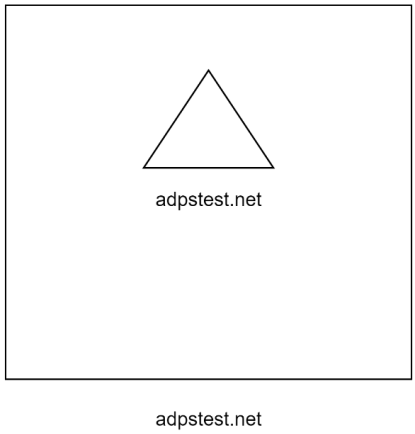

Figure 1.1: *Example of single domain Active Directory Forest*

Single forest, multiple domains

This architecture is mostly used in medium to large organizations with no requirement to split the AD into multiple forests. It provides the benefit of central administration capabilities and simple authentication scenarios within a single forest. In most cases, different domains are for geographical separation; it is not recommended to separate due to special functional use cases like manufacturing, DMZ, and the like, as shown in *Figure 1.2*:

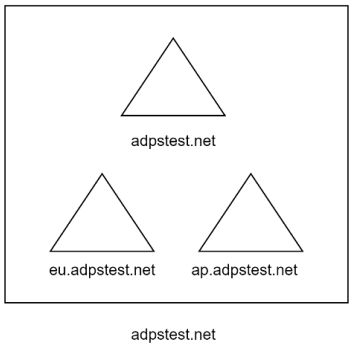

Figure 1.2*: Example of multiple domain Active Directory Forest*

Multiple forest Active Directory

Multiple forest AD architecture is typically found in large organizations that need separation of infrastructure and management between different internal teams and products. They utilize the concept of Admin Forest and DMZ forests that need separation, often acquire different companies, and decides to keep the AD infrastructure separated. Trusts between organizations are setup to support cross-forest authentications. The following example shows three forests connected with the main forest with one-way forest trusts. That type