

**2<sup>nd</sup>**  
Edition

# Microsoft Azure Administrator Exam Prep (AZ-104)

Practice Labs, Mock Exams, and Real Scenarios to Get You Certified  
on the Microsoft Azure Platform

**Lalit Rawat**







# Microsoft Azure Administrator Exam Prep (AZ-104) 2nd Edition

---

*Practice Labs, Mock Exams, and Real Scenarios to  
Get You Certified on the Microsoft Azure Platform*

---

**Lalit Rawat**



[www.bpbonline.com](http://www.bpbonline.com)

Copyright © 2023 BPB Online

*All rights reserved.* No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor BPB Online or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

BPB Online has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, BPB Online cannot guarantee the accuracy of this information.

First published: 2021

Second published: 2023

Published by BPB Online

WeWork

119 Marylebone Road

London NW1 5PU

**UK | UAE | INDIA | SINGAPORE**

ISBN 978-93-55512-291

[www.bpbonline.com](http://www.bpbonline.com)

**Dedicated to**

***Narendra Kumar Rawat and Narmada Rawat***

*To my Parents: Thank you for your unconditional  
support in any and every situation.*

*Thanks for your blessings and support.*

*My Wife **Punita Rawat***

*&*

***Radhika and Mayra Rawat***

*My daughters who have made my life easy!*

## About the Author

**Lalit** is a Cloud Architect, Azure MVP, MCT, and author of the ‘Azure Interview Q and A’ book. He likes to share his knowledge through his blog (<https://azure4you.com/>) and share his technical skills in a wider community like AzureTalk, Local Meetup Group, and so on. He has written several articles on Microsoft Azure and changed many lives from his articles and his hands-on training programs and workshops.

He is “Speaker” and delivered the session on a big platform, including MS Global Bootcamp, Local user group, Expert Live India, and other events.

Moreover, and to his credit, he has delivered 500+ training sessions to professionals worldwide in Microsoft Azure technologies and other technologies, including SCOM and Windows Server. He has also provided instructor-led online training and hands-on workshops.

His technical prowess and capability of exploring new frontiers of technology and imparting them to his aspiring team members is his trademark. His execution is priceless and bringing forth his approach will help you realize your dreams, goals, and aspirations into reality.

## Acknowledgement

There are a few people I would like to thank for the continued and ongoing support they have given me during the writing of this book. First and foremost, I would like to thank my wife, Punita Rawat, and two daughters, Radhika and Mayra, for putting up with me while I was spending many weekends and evenings on writing. I could have never completed this book without their support.

This book wouldn't have happened if I hadn't got the support from my family, followers, friends, and so on. My gratitude goes to the AzureTalk core team, especially Niraj Kumar, for providing valuable insights into some of the new features and providing mentorship and guidance.

I would like to thank Gaurav Aroraa for his wonderful support, guidance and helping me while writing the Azure Administrator book.

Thank you, Deepak Rajendran Sir, for providing your guidance to do something new and contribute more and more.

Finally, I would like to thank Gaurav and BPB Publications for giving me this opportunity to write my first book for them.

## Preface

Microsoft Azure is a platform where you can start your journey of cloud learning. In this book Azure Administration (AZ-104), we have explained about the day-to-day tasks which you can take up and learn about Azure administration. We have explained Azure core concepts in this chapter and add the lab-based scenario, which will help you clear the core concepts of Microsoft Azure. We have included approx. 60 to 70 questions which will help you check your knowledge and provide a glimpse of the Azure administration exam questions. This will help you prepare for your Azure administration exam.

In this book, we have explained how to use the Azure Active Directory and create users in the Azure subscription. We have also explained about the Azure storage account, networking component like Azure Vnet, Subnet, and how to implement the network security group to restrict the traffic to secure the Azure environments. We have also explained load balance mechanics to load balance your application. We have also explained about the Azure role-based access control which will help you fine grain the Azure subscription access. We have defined the Azure subscription usage and how to save cost management. In this book, you will also learn how to create the WebApps and Azure container/Kubernetes services which will help you to learn the same, and it's a top trending subject in the market today.

We have also covered in this chapter about the hybrid connectivity using the site to site connection and express route. We have explained what is the component which been used to create the Azure virtual machine.

Once you have all of the azure resources, then azure monitoring will also important to monitor the Azure Resources. We have nicely explained and provided the step by step solutions for Azure monitor to clear you Azure monitoring concepts. We have explained how to analysis the Azure resources etc.

The primary goal of this book is to provide information and skills that are necessary to build and deploy the Azure infrastructure in your own environment. This book contains real-life examples that will show you how to clear the Azure Administration exam as well as how to integrate an on-premises environment to Azure. You will learn the following topics in this book:

**Chapter 1 Managing Azure AD Objects**, introduces the Azure AD object and discusses how to create users in Azure AD, group, and so on, which will help you understand the Azure AD. This will help you in the exam as well.

**Chapter 2 Implementing and Managing Hybrid Identities**, discusses the Azure AD connect and how to connect on-premises AD to Azure AD and sync the users. It provides the step-by-step instructions using an actual screenshot from an Azure lab environment.

**Chapter 3 Managing Role Assignments Through the RBAC Policy**, discusses the Azure role-based access to control how to manage the access in the Azure subscription and defines the access level in your organization.

**Chapter 4 Managing Azure Subscription and Resource Management**, explains the Azure subscription and its type. It also discusses how to manage the Azure subscription and reduce the cost of your subscription.

**Chapter 5 Managing and Configuring of Azure Storage Accounts**, discusses, in depth, what an Azure storage account is and how to use it. It helps users to allow them to save their own data in an Azure storage account and manage the data. It also discusses how to connect the Azure storage account using the Azure Storage Explorer.

**Chapter 6 Manage Data in AZURE Storage**, describes how to manage the data and migrate the petabytes of the data using the Azure export and import services. It discusses the Azure databox and Azure AzCopy command-line utility to move the data from on-premise to the Azure storage account or one storage account to another.

**Chapter 7 The Azure File Share**, introduces the Azure file share, which is designed to integrate your on-premises systems to migrate the files to Azure automatically using the Azure file sync. It explains the core concepts of the Azure file share and how to connect to your on-premises servers.

**Chapter 8 Creating and Configuring of Azure VMs**, describes how to create the Azure virtual machine, explains its components, and how to configure it. It provides examples with Windows/Linux OS.

**Chapter 9 Automating Deployment of VMs**, describes how to create the VM automatically using the Azure Arm template.

**Chapter 10 Creating and Configuring Container**, describes how to create containers and configure them in Azure subscriptions.

**Chapter 11 Creating and Configuring Web Apps**, describes how to create and configure Azure WebApps. It describes the App services, App services plan, and so on.

**Chapter 12 Configuring Virtual Networking and Integrating On-Premises to Azure Network**, discusses how to configure virtual networking and integrate an on-premises to the Azure network. It explains Azure Vnet and configures Vnet-to-Vnet peering.

**Chapter 13 Configuring Load Balancing Securing Access to Virtual Networks**, discusses how to configure Azure load balancing and provides the Azure load balancer, Application gateway, and DNS services.

**Chapter 14 Securing Access to Virtual Networks**, discusses how to secure access to virtual networks using the Azure network security group and an Azure firewall. It explains Azure Bastion services.

**Chapter 15 Monitoring and Troubleshooting of Virtual Networking**, discusses how to monitor and troubleshoot virtual networking using the Azure network watcher.

**Chapter 16 Analyzing Resource Utilization and Consumption**, discusses how to analyze resource utilization using the Azure monitor and explains analyzing metrics across subscription and services health.

**Chapter 17 Implementation of Azure Backup and Disaster Recovery**, discusses how to implement of Azure backup and protect the Azure VMs for accidental deletion. It explains how to perform the Azure backup and restoration process.

**Chapter 18 Exam Preparation Guidelines and Assessment Based on Live Questions**, describes exam preparation guidelines and assessments based on live questions which will help you in your exam preparation. It covers more than 70 questions, which includes the scenario-based questions as well.



## Code Bundle and Coloured Images

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

**<https://rebrand.ly/yn7w6fz>**

The code bundle for the book is also hosted on GitHub at **<https://github.com/bpbpublications/Microsoft-Azure-Administrator-Exam-Prep-AZ-104-2nd-Edition>**. 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](mailto: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](http://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](mailto:business@bpbonline.com)** for more details.

At **[www.bpbonline.com](http://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**.

# Table of Contents

|                                                             |           |
|-------------------------------------------------------------|-----------|
| <b>1. Managing Azure AD Objects.....</b>                    | <b>1</b>  |
| Introduction.....                                           | 1         |
| Structure.....                                              | 1         |
| Objectives.....                                             | 2         |
| Bulk user creation .....                                    | 2         |
| User creation.....                                          | 4         |
| Group creation .....                                        | 5         |
| Group management .....                                      | 7         |
| Guest user management .....                                 | 8         |
| Self-service password reset .....                           | 10        |
| Azure AD join.....                                          | 12        |
| Conclusion .....                                            | 12        |
| Points to remember .....                                    | 12        |
| Multiple choice questions.....                              | 13        |
| <i>Answers</i> .....                                        | 13        |
| <b>2. Implementing and Managing Hybrid Identities .....</b> | <b>15</b> |
| Introduction.....                                           | 15        |
| Structure.....                                              | 15        |
| Objectives.....                                             | 16        |
| Azure AD Connect .....                                      | 16        |
| Azure AD Connect installation.....                          | 17        |
| <i>Pre-requisites</i> .....                                 | 17        |
| Manage Azure AD Connect .....                               | 23        |
| Password writeback .....                                    | 24        |
| Enabling the Password Writeback from the Azure AD .....     | 25        |
| Enabling password writeback from the portal .....           | 28        |
| Password sync.....                                          | 30        |
| Conclusion .....                                            | 30        |

|                                                                    |           |
|--------------------------------------------------------------------|-----------|
| Points to remember .....                                           | 30        |
| Multiple choice questions.....                                     | 31        |
| <i>Answers</i> .....                                               | 31        |
| <b>3. Managing Role Assignments Through the RBAC Policy .....</b>  | <b>33</b> |
| Introduction.....                                                  | 33        |
| Structure.....                                                     | 33        |
| Objectives.....                                                    | 33        |
| Role-Based Access Control .....                                    | 34        |
| RBAC access configuration .....                                    | 35        |
| <i>Subscription access using the RBAC policy</i> .....             | 35        |
| <i>Resource group access using the RBAC policy</i> .....           | 37        |
| <i>Resource access using the RBAC policy</i> .....                 | 38        |
| Custom RBAC role .....                                             | 40        |
| <i>Creating the custom role</i> .....                              | 40        |
| Conclusion .....                                                   | 42        |
| Points to remember .....                                           | 42        |
| Multiple choice questions.....                                     | 42        |
| <i>Answers</i> .....                                               | 43        |
| <b>4. Managing Azure Subscription and Resource Management.....</b> | <b>45</b> |
| Introduction.....                                                  | 45        |
| Structure .....                                                    | 45        |
| Objectives.....                                                    | 46        |
| Azure subscription .....                                           | 46        |
| Enterprise Agreement Subscription.....                             | 47        |
| <i>Enterprise</i> .....                                            | 47        |
| <i>Departments</i> .....                                           | 47        |
| <i>Accounts</i> .....                                              | 47        |
| <i>Subscriptions</i> .....                                         | 47        |
| Azure Subscription Support Plan.....                               | 48        |
| <i>Azure Developer Support</i> .....                               | 48        |
| <i>Professional Direct Support</i> .....                           | 48        |

|                                                                    |           |
|--------------------------------------------------------------------|-----------|
| <i>Standard Support</i> .....                                      | 49        |
| <i>Azure tenant</i> .....                                          | 49        |
| Creating a Free Azure Subscription .....                           | 50        |
| Global administrator permission .....                              | 54        |
| Resources group.....                                               | 55        |
| <i>Azure Resource Group Manager</i> .....                          | 55        |
| Cost management.....                                               | 56        |
| <i>Exploring cost management</i> .....                             | 56        |
| <i>Configuration of the budget alerts</i> .....                    | 58        |
| Azure subscription policy .....                                    | 59        |
| <i>Azure policy creation, configuration, and assignment</i> .....  | 60        |
| Azure quota .....                                                  | 63        |
| Resource tag.....                                                  | 64        |
| <i>Usage of the Resource Tag</i> .....                             | 65        |
| <i>Configuration of a resource lock</i> .....                      | 65        |
| <i>Resources movement from one resource group to another</i> ..... | 67        |
| <i>Removing a resource group</i> .....                             | 68        |
| Creating and configuring management groups .....                   | 70        |
| Conclusion .....                                                   | 73        |
| Points to remember .....                                           | 73        |
| Multiple choice questions.....                                     | 74        |
| <i>Answers</i> .....                                               | 74        |
| <b>5. Managing and Configuring of Azure Storage Accounts.....</b>  | <b>75</b> |
| Introduction.....                                                  | 75        |
| Structure.....                                                     | 75        |
| Objectives.....                                                    | 76        |
| Azure storage account.....                                         | 76        |
| <i>Types of Azure storage accounts</i> .....                       | 77        |
| <i>Azure storage account creation and configuration</i> .....      | 79        |
| Implementing Azure storage replication .....                       | 82        |
| Generating and managing the shared access signature .....          | 84        |

|                                                                        |            |
|------------------------------------------------------------------------|------------|
| Managing storage account access key .....                              | 85         |
| Configuring network access to the storage account .....                | 86         |
| Installation and configuration of the storage explorer .....           | 88         |
| Conclusion .....                                                       | 91         |
| Points to remember .....                                               | 92         |
| Multiple choice questions .....                                        | 92         |
| <i>Answers</i> .....                                                   | 92         |
| <b>6. Manage Data in Azure Storage .....</b>                           | <b>93</b>  |
| Introduction .....                                                     | 93         |
| Structure .....                                                        | 93         |
| Objectives .....                                                       | 94         |
| Import and export jobs in Azure .....                                  | 94         |
| <i>Configuring Azure Blob Storage</i> .....                            | 94         |
| <i>Creating import and export job in Azure Storage</i> .....           | 97         |
| Azure Data Box .....                                                   | 100        |
| <i>Configuring Azure AD authentication for a storage account</i> ..... | 101        |
| <i>Copying data using AzCopy</i> .....                                 | 103        |
| Configure Blob object replication .....                                | 105        |
| <i>Prerequisites</i> .....                                             | 105        |
| <i>Configure object replication for block blobs</i> .....              | 105        |
| Conclusion .....                                                       | 108        |
| Points to remember .....                                               | 108        |
| Multiple choice questions .....                                        | 108        |
| <i>Answers</i> .....                                                   | 108        |
| <b>7. The Azure File Share .....</b>                                   | <b>109</b> |
| Introduction .....                                                     | 109        |
| Structure .....                                                        | 109        |
| Objectives .....                                                       | 110        |
| Azure File share .....                                                 | 110        |
| <i>Creating and configuring the Azure File share</i> .....             | 110        |
| <i>Configuration of Azure File Sync</i> .....                          | 114        |

|                                                       |            |
|-------------------------------------------------------|------------|
| <i>Azure File Sync group</i> .....                    | 115        |
| Azure File Sync troubleshooting .....                 | 118        |
| Configure blob life cycle management .....            | 118        |
| Conclusion .....                                      | 121        |
| Points to remember .....                              | 122        |
| Multiple choice questions .....                       | 122        |
| <i>Answers</i> .....                                  | 122        |
| <b>8. Creating and Configuring of Azure VMs .....</b> | <b>123</b> |
| Introduction .....                                    | 123        |
| Structure .....                                       | 123        |
| Objectives .....                                      | 124        |
| Azure Virtual Machine .....                           | 124        |
| Virtual Machine Components .....                      | 124        |
| <i>Creating a Windows Virtual Machine</i> .....       | 128        |
| <i>Creating Linux VMs</i> .....                       | 134        |
| Azure virtual machine scale set creation .....        | 134        |
| Configure Azure Disk Encryption .....                 | 138        |
| Redeploying a VM .....                                | 140        |
| Conclusion .....                                      | 141        |
| Points to remember .....                              | 142        |
| Multiple choice questions .....                       | 142        |
| <i>Answers</i> .....                                  | 142        |
| <b>9. Automating Deployment of VMs .....</b>          | <b>143</b> |
| Introduction .....                                    | 143        |
| Structure .....                                       | 143        |
| Objectives .....                                      | 143        |
| Azure ARM template .....                              | 144        |
| Modifying the ARM template .....                      | 144        |
| Template deployments .....                            | 149        |
| Conclusion .....                                      | 150        |
| Points to remember .....                              | 150        |

---

|                                                                  |            |
|------------------------------------------------------------------|------------|
| Multiple choice questions.....                                   | 151        |
| <i>Answers</i> .....                                             | 151        |
| <b>10. Creating and Configuring Container.....</b>               | <b>153</b> |
| Introduction.....                                                | 153        |
| Structure.....                                                   | 153        |
| Objectives.....                                                  | 154        |
| Azure Container.....                                             | 154        |
| <i>Use of an Azure Container</i> .....                           | 154        |
| <i>Creating a Container</i> .....                                | 154        |
| <i>Configure scaling and sizing for Container services</i> ..... | 158        |
| <i>App Container creation</i> .....                              | 158        |
| Scaling for Container App Instance .....                         | 160        |
| Sizing Container App instance.....                               | 162        |
| Azure Kubernetes.....                                            | 165        |
| <i>Creating Azure Kubernetes</i> .....                           | 165        |
| <i>Configure Scaling for AKS</i> .....                           | 171        |
| <i>Upgrade the AKS Cluster</i> .....                             | 173        |
| Conclusion .....                                                 | 175        |
| Points to remember .....                                         | 176        |
| Multiple choice questions.....                                   | 176        |
| <i>Answers</i> .....                                             | 176        |
| <b>11. Creating and Configuring Web Apps .....</b>               | <b>177</b> |
| Introduction.....                                                | 177        |
| Structure.....                                                   | 177        |
| Objectives.....                                                  | 178        |
| App services .....                                               | 178        |
| <i>App services plan</i> .....                                   | 178        |
| Create and configure app services .....                          | 181        |
| <i>Custom domain configuration</i> .....                         | 184        |
| <i>App Services Security</i> .....                               | 185        |
| <i>Authentication</i> .....                                      | 185        |



|                                                                                 |            |
|---------------------------------------------------------------------------------|------------|
| <i>TLS/SSL Configuration</i> .....                                              | 186        |
| <i>Configure network setting of app services</i> .....                          | 186        |
| <i>App services backup</i> .....                                                | 191        |
| <i>Configure scaling setting in an App Service plan</i> .....                   | 193        |
| <i>Configure deployment slots</i> .....                                         | 197        |
| Conclusion .....                                                                | 200        |
| Points to remember .....                                                        | 200        |
| Multiple choice questions.....                                                  | 200        |
| <i>Answers</i> .....                                                            | 201        |
| <b>12. Virtual Network Configuration and Integration On-Prem to Azure</b> ..... | <b>203</b> |
| Introduction.....                                                               | 203        |
| Structure.....                                                                  | 203        |
| Objectives.....                                                                 | 204        |
| Azure Virtual Network.....                                                      | 204        |
| <i>Azure Virtual Network creation</i> .....                                     | 204        |
| <i>Azure VNet peering</i> .....                                                 | 206        |
| <i>Virtual network gateway</i> .....                                            | 209        |
| <i>Site-to-site VPN</i> .....                                                   | 213        |
| <i>Site-to-site VPN connection creation</i> .....                               | 215        |
| <i>VNet-to-VNet connectivity creation</i> .....                                 | 218        |
| ExpressRoute connection.....                                                    | 220        |
| ExpressRoute configuration.....                                                 | 221        |
| Configure Azure Virtual WAN .....                                               | 222        |
| Conclusion .....                                                                | 228        |
| Points to remember .....                                                        | 228        |
| Multiple choice questions.....                                                  | 228        |
| <i>Answers</i> .....                                                            | 228        |
| <b>13. Configuring Load Balancing</b> .....                                     | <b>229</b> |
| Introduction.....                                                               | 229        |
| Structure.....                                                                  | 229        |
| Objectives.....                                                                 | 230        |

---

|                                                        |            |
|--------------------------------------------------------|------------|
| Azure DNS.....                                         | 230        |
| <i>Azure DNS Creation</i> .....                        | 231        |
| <i>Azure DNS record creation</i> .....                 | 233        |
| <i>Azure Load Balancer</i> .....                       | 234        |
| <i>Azure Internal Load Balancer</i> .....              | 235        |
| Front-end IP configuration.....                        | 237        |
| <i>Azure backend pool</i> .....                        | 238        |
| <i>Health probes</i> .....                             | 238        |
| <i>Application gateway</i> .....                       | 240        |
| Azure Traffic Manager .....                            | 248        |
| Conclusion .....                                       | 250        |
| Points to remember .....                               | 250        |
| Multiple choice questions.....                         | 250        |
| <i>Answers</i> .....                                   | 250        |
| <b>14. Securing Access to Virtual Networks .....</b>   | <b>251</b> |
| Introduction.....                                      | 251        |
| Structure.....                                         | 251        |
| Objectives.....                                        | 252        |
| Configuration of private and public IP addresses ..... | 252        |
| Network security group .....                           | 254        |
| <i>Network security group association</i> .....        | 257        |
| Route table .....                                      | 259        |
| Configure and deploy the Azure firewall .....          | 262        |
| Configure and deploy Azure Bastion services .....      | 266        |
| Evaluate effective security rules.....                 | 269        |
| Azure Private Network.....                             | 270        |
| Conclusion .....                                       | 275        |
| Points to remember .....                               | 275        |
| Multiple choice questions.....                         | 275        |
| <i>Answers</i> .....                                   | 276        |

|                                                                      |            |
|----------------------------------------------------------------------|------------|
| <b>15. Monitoring and Troubleshooting of Virtual Networking.....</b> | <b>277</b> |
| Introduction.....                                                    | 277        |
| Structure.....                                                       | 277        |
| Objectives.....                                                      | 277        |
| Network watcher .....                                                | 278        |
| <i>Network Watcher topology.....</i>                                 | <i>279</i> |
| Monitor on-premises connectivity .....                               | 279        |
| <i>IP flow verify .....</i>                                          | <i>281</i> |
| <i>Next hop.....</i>                                                 | <i>282</i> |
| Network performance monitor .....                                    | 283        |
| Conclusion .....                                                     | 286        |
| Points to remember .....                                             | 286        |
| Multiple choice questions.....                                       | 286        |
| <i>Answers .....</i>                                                 | <i>286</i> |
| <b>16. Analyzing Resource Utilization and Consumption .....</b>      | <b>287</b> |
| Introduction.....                                                    | 287        |
| Structure.....                                                       | 287        |
| Objectives.....                                                      | 288        |
| Azure Monitor.....                                                   | 288        |
| Setup and configuration of Azure alerts .....                        | 289        |
| Azure Metrics .....                                                  | 293        |
| Azure Services Health.....                                           | 293        |
| Diagnostic Logs.....                                                 | 294        |
| <i>Enabling the diagnostic settings.....</i>                         | <i>294</i> |
| Azure Log Analytics.....                                             | 296        |
| <i>Creating the Azure workspace .....</i>                            | <i>297</i> |
| <i>Utilize Log Search Query Functions .....</i>                      | <i>299</i> |
| Conclusion .....                                                     | 301        |
| Points to remember .....                                             | 301        |
| Multiple choice questions.....                                       | 302        |
| <i>Answers .....</i>                                                 | <i>302</i> |

|                                                                       |                |
|-----------------------------------------------------------------------|----------------|
| <b>17. Implementation of Azure Backup and Disaster Recovery .....</b> | <b>303</b>     |
| Introduction.....                                                     | 303            |
| Structure.....                                                        | 303            |
| Objectives.....                                                       | 304            |
| Azure backup .....                                                    | 304            |
| Azure backup vault creation.....                                      | 304            |
| Azure VMs backup configuration.....                                   | 306            |
| Azure backup policy .....                                             | 307            |
| Azure backup report .....                                             | 310            |
| Azure restoration of VMs .....                                        | 313            |
| Azure backup operation details .....                                  | 315            |
| Using soft delete to recover Azure VMs.....                           | 316            |
| Site-to-site recovery using Azure Site Recovery .....                 | 318            |
| Conclusion .....                                                      | 322            |
| Points to remember .....                                              | 322            |
| Multiple choice questions.....                                        | 322            |
| <i>Answers</i> .....                                                  | 323            |
| <br><b>18. Exam Preparation Guidelines and Assessment Based on</b>    |                |
| <b>Live Questions .....</b>                                           | <b>325</b>     |
| Introduction.....                                                     | 325            |
| Exam preparation guidelines.....                                      | 326            |
| AZ-104 Exam tips .....                                                | 326            |
| Exam registration.....                                                | 328            |
| Dummy objective exam questions .....                                  | 330            |
| Dummy Scenario-Based Exam Questions.....                              | 338            |
| <br><b>Index .....</b>                                                | <b>349-354</b> |

# CHAPTER 1

# Managing Azure AD Objects

## Introduction

This book will cover all the prospective AZ-104 exam study material, which will help you clear this exam. We will provide additional information in this chapter, which will further cover various topics and help you get an understanding of the topics in detail.

The following chapters will help you understand the Azure environment and help you clear the AZ-104 exam.

## Structure

The following topics will be covered in this chapter:

- Bulk user creation
- User creation
- Group creation
- Group management
- Guest user management

- Self-service password reset
- Azure AD Join

## Objectives

In this chapter, we will explain the bulk user creation in **Azure Active Directory (Azure AD)**, and group creation and management. We will discuss how to provide access to guest users and how to manage guest users. We will cover how the users can reset their passwords using the self-service password, and add the devices in Azure AD using the Azure AD join tool.

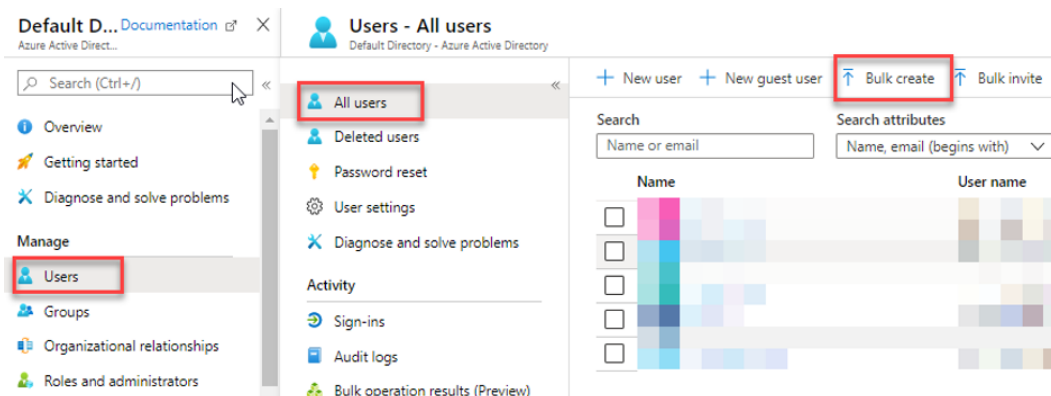
## Bulk user creation

Bulk user creation will help your organization in the onboarding process, so that it will be completed soon. Moreover, it will also help improve the user creation – both for users who have recently joined your organization, as well as existing users, in Azure. It will reduce administrative work. If you want to create the users or bulk users in Azure environments, you need a user administrator access in the Azure Active directory.

Let us try and create bulk users in Azure AD. Follow these steps to create the bulk users:

1. Go to **Azure Active Directory**.
2. Select the **Users** option and click on **All Users**.
3. Click on **Bulk Create**.

Take a look at *Figure 1.1* to see how bulk users are created:



*Figure 1.1: Bulk user creation*

4. When you click on **Bulk Create**, it will ask you to download the CSV file.
5. Fill in the following details:
  - a. Provide the name, last name, and username.
  - b. Provide the initial password and block sign-in (Yes/No) which is a mandatory field.
  - c. Provide the department and user location.
  - d. Provide the job title and country code.
  - e. Provide the official phone number, mobile number, and so on.
6. You have to put all the details in a single line as per the **.csv** file. In this case, the column has been changed to show the properties of the CSV file. Take a look at *Figure 1.2* for bulk user creation details:

**Bulk create user (Preview)**  
Default Directory - Azure Active Directory

1. Download csv template (optional)  
[Download](#)

2. Edit your csv file

3. Upload your csv file  
[Select a file](#)

[Learn more about bulk import users](#)

| version:v1.0                                |                                                              |
|---------------------------------------------|--------------------------------------------------------------|
| Name (example: Chris Green) [displayName] * | User name (example: chris@contoso.com) [userPrincipalName] * |
| Initial password [passwordProfile] *        | Block sign in (Yes/No) [accountEnabled] *                    |
| Last name [surname]                         | Job title [jobTitle]                                         |
| Initial password [passwordProfile] *        | Block sign in (Yes/No) [accountEnabled] *                    |
| First name [givenName]                      |                                                              |
| Department [department]                     | Usage location [usageLocation]                               |

*Figure 1.2: Bulk user creation details*

7. Once you fill all the details and upload the **.csv** file, click on **Submit**. It will start processing the user creation. It will take some time to create the users, and you can see all those users under the user's tab. Refer to *Figure 1.3*:

**Bulk create user (Preview)**  
Default Directory - Azure Active Directory

1. Download csv template (optional)  
[Download](#)
2. Edit your csv file
3. Upload your csv file  
"UserCreateTemplate (2).csv"  
File uploaded successfully
4. In progress

[Click here to view the status of each operation](#)

[Learn more about bulk import users](#)

[Submit](#)

*Figure 1.3: Bulk user creation Submit*

## User creation

In the bulk user creation, we studied the use of the bulk user creation. However, the question then arises: how do you create an individual user?

To create an individual user, follow these steps:

1. Go to **Azure Active Directory**.
2. Select the **Users** and click on **All Users**.
3. Click on the **New user**.
4. Enter the **User Name**.
5. Provide the **Name, First name**, and **Last Name**.
6. You can also provide the department number, location, and job title.



- Once you provide all the preceding details, click on **Create** and your users will be created.

Refer to *Figure 1.4* for more details:

**Users | All users (Preview)**

**New user**  
lalit01rawatoutlook (Default Directory)

Create a new user in your organization. This user will have a user name like `alice@lalit01rawatoutlook.onmicrosoft.com`.  
[I want to create users in bulk](#)

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.  
[I want to invite guest users in bulk](#)

**Identity**

User name \*

Name \*

First name

Last name

**Create**

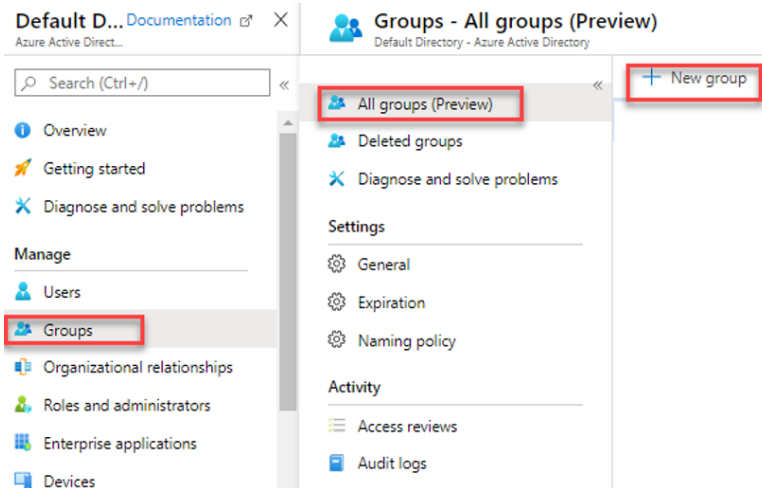
*Figure 1.4: User creation*

## Group creation

To create the Azure AD group, follow these steps:

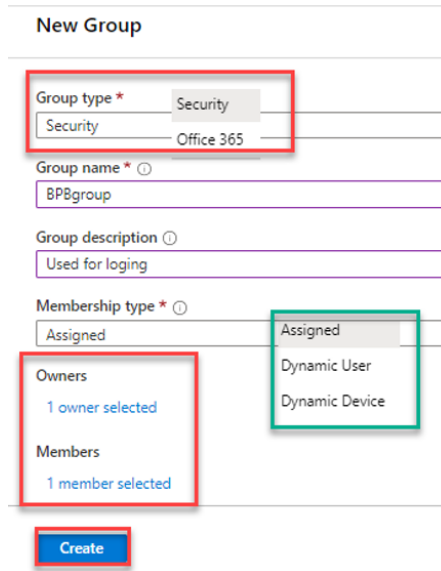
- Click on the Azure AD.
- Select the groups from the **Manage** tab.
- Select **All Groups**.
- Click on the **New Group**.

Take a look at *Figure 1.5*:



*Figure 1.5: Group creation*

5. When you click on group creation, select either of the two options:
  - a. **Security group:** It helps to manage users and computer access to shared resources, for a specific group.
  - b. **O365 Group:** Using this group, we can provide access to users for a shared mailbox, calendar, files, SharePoint site, and so on.
6. You can assign the owner to the group administrator and then click on the membership.
7. When you click on the membership, it will ask you to select either of the three available options:
  - a) **Assigned:** The administrator will add specific users to the group.
  - b) **Dynamic user:** It allows users to use dynamic membership rules and add automatically to the group.
  - c) **Dynamic device:** It uses the dynamic group rules to add and remove the devices automatically.
8. Please select the assigned member as default as shown in *Figure 1.6*:



**New Group**

Group type \* Security

Group name \* BPBgroup

Group description Used for logging

Membership type \* Assigned

Owners  
1 owner selected

Members  
1 member selected

**Create**

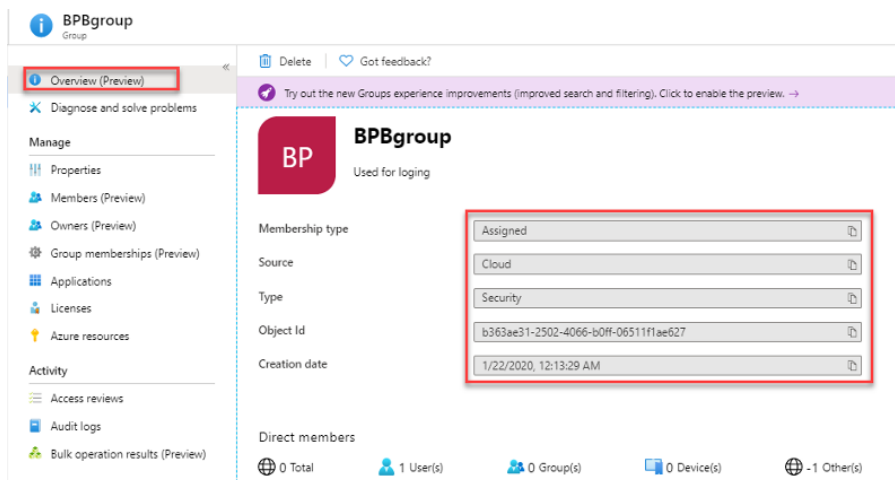
Figure 1.6: Group creation details

- Once you click on create, your groups will be created successfully. Let us see how to manage the group and its properties.

## Group management

Perform the following steps:

Once the group is created, you can click on the group and see the properties of the group, such as membership type, source ID, and so on, as shown in Figure 1.7:



**BPBgroup**  
Group

Overview (Preview) | Delete | Got feedback?

Try out the new Groups experience improvements (improved search and filtering). Click to enable the preview. →

**BPBgroup**  
Used for logging

Membership type: Assigned

Source: Cloud

Type: Security

Object Id: b363ae31-2502-4066-b0ff-06511f1ae627

Creation date: 1/22/2020, 12:13:29 AM

Direct members

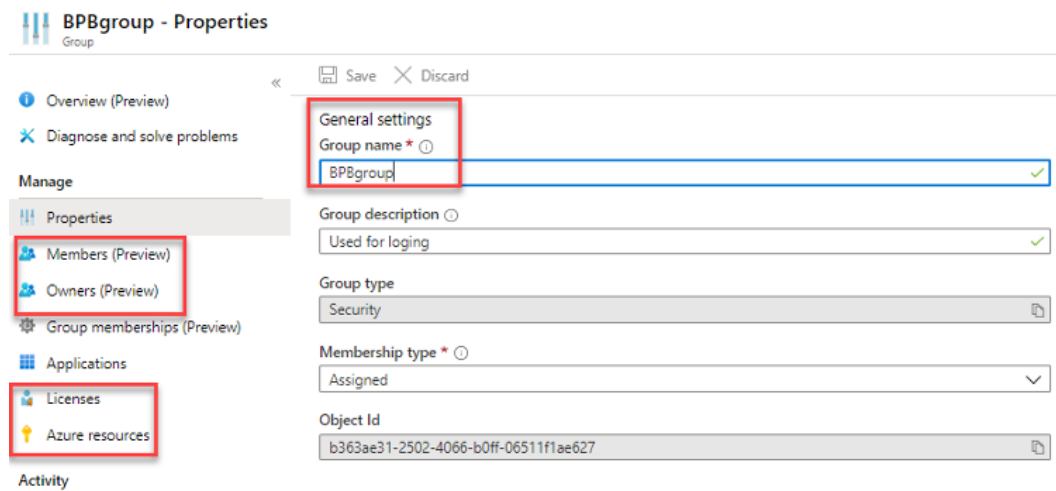
0 Total | 1 User(s) | 0 Group(s) | 0 Device(s) | -1 Other(s)

Figure 1.7: Group management

1. Based on the requirements, users can change the group.
2. Click on the **Members** tab and add the new members.
3. Click on the **Owners** tab to add the multiple owners.
4. You can assign the application and see the Azure resources which have been accessed by these group members.
5. You can see the application accessed by this group and manage it.

In this section, we discussed the Azure group creation and learned how to manage the groups. We explained the Azure security group and O365 group.

We also discussed group management. Refer to *Figure 1.8* for more details:



*Figure 1.8: Group management general settings*

## Guest user management

Azure AD supports Business to Customer (B2C) and Business to Business (B2B), where we can allow customers to have access to our Azure AD. The customer ID can be their organization ID, Outlook, Facebook, LinkedIn, Amazon Gmail ID, and so on. You can invite those users as guests, and provide access as a request to perform the task. If you want to invite guests, then the user should have the user administrator role assigned to him.

Let us see how to invite guest users. Follow these steps:

1. Go to Azure AD and click on **All Users**.
2. In the right pane, click on **New Guest Users**. Take a look at *Figure 1.9*:

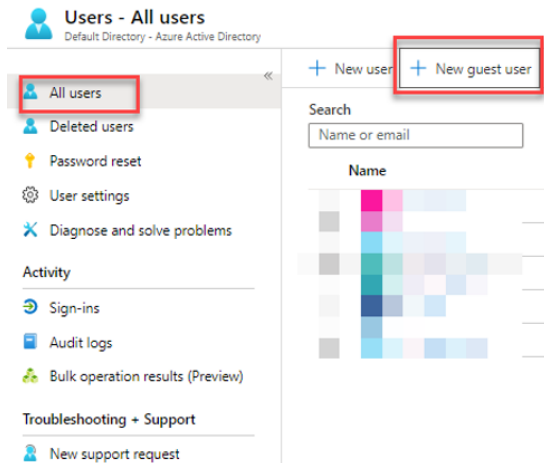


Figure 1.9: Guest user access

### 3. Select **Invite Users**.

- Provide the name and email ID of the user you want to invite.
- The rest of the fields are optional. You can then click on **Invite**.

Now, you will be able to invite all the B2B and B2C users. Take a look at Figure 1.10:

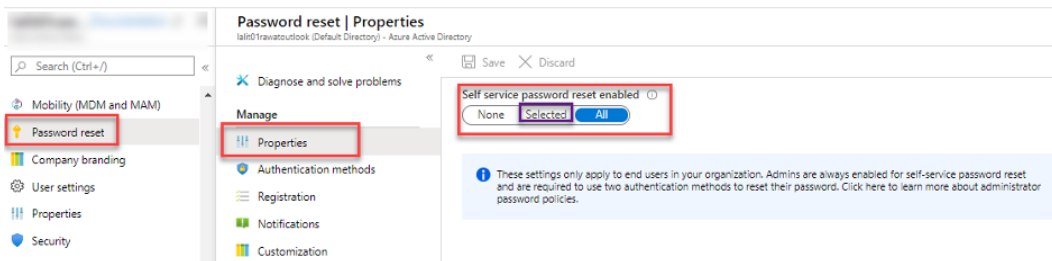
Figure 1.10: Guest user access invite

## Self-service password reset

Azure self-service password reset will help users to reset their password without the help of a help desk administrator. If the user account is locked or if the password expires, the user can unlock/reset the password using a self-service password reset.

If you want to configure the self-service password reset, you should have global administrator rights in Azure AD. Follow the given steps to configure the self-service password reset:

1. Please go to your Azure AD.
2. Click on the **Password reset** tab.
3. Select the users: either **All** or **Selected**. If you click on selected users, it will ask you to choose the group name.
4. Once you are done with this, click on the **Save** button, as shown in *Figure 1.11*:

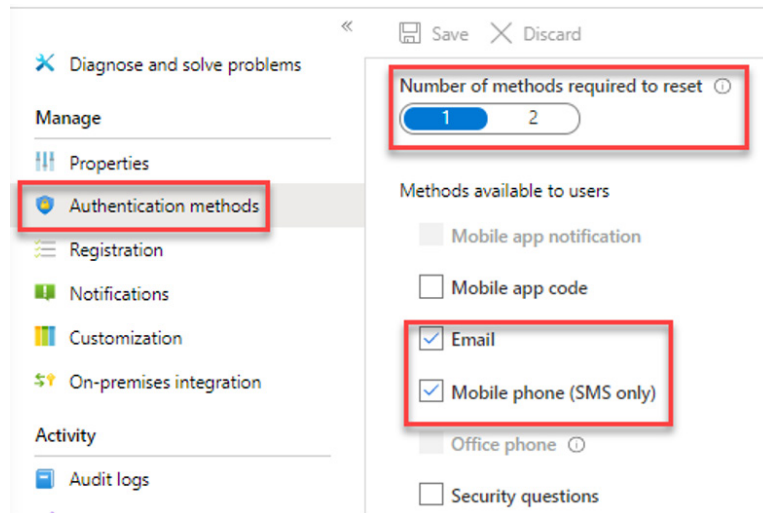


*Figure 1.11: Password reset*

Go to **Authentication methods** and follow the given steps:

1. Select the authentication methods required as **1** or **2**, and then set it according to your wish, from the list of available options:
  - a. Mobile app code
  - b. Email
  - c. Phone -SMS only
  - d. Mobile app notification
  - e. Office phone
  - f. Security question
2. Once you select the method, your user will be able to reset the password using the multifactor authentication.

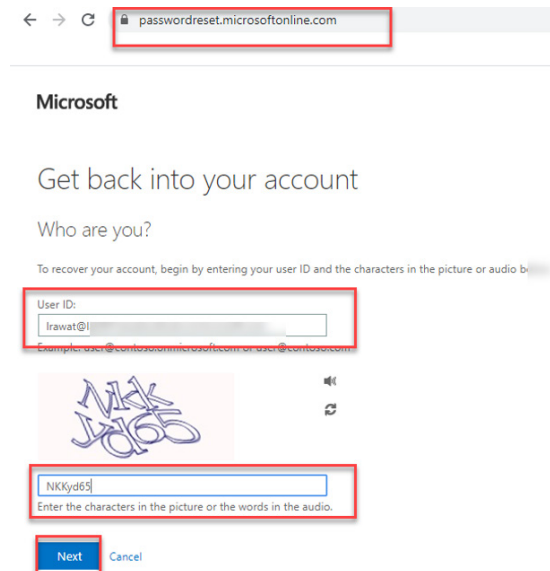
Refer to *Figure 1.12*:



*Figure 1.12: Authentication method*

Once you configure this, you can go to <https://passwordreset.microsoftonline.com> to reset the password. Then, follow the given steps:

1. Provide your **User ID**.
2. Enter the characters as per the image and click on the **Next** button, as shown in *Figure 1.13*:



*Figure 1.13: Password reset method*

3. Now, you will be able to reset the password.

## Azure AD join

Azure AD Join provides the feature to register your mobile, laptop, and other devices to Azure AD, with respect to the size of the device or industry. Azure AD Join works in hybrid environments as well. It enables access to both cloud and on-premises apps.

If you want to manage and configure the Azure AD join, then you have to use the MDM and Intune solution, which requires an Azure AD P2 license. We can use the Azure AD join in the following few scenarios:

- Windows deployment for your owned devices.
- Access to organizational apps and resources from your device.
- Cloud-based management of owned devices.
- To configure the user, sign in to their devices with Azure AD or synced Azure AD work or school accounts.

## Conclusion

In this chapter, we discussed how to create bulk users and group management. We explained how to invite guest users and how to manage them using Azure AD. We also explained Azure AD Join and learned how to set up the self-service password reset.

In the next chapter, we will discuss Azure AD connect and its installation.

We will also discuss how to manage Azure AD connect and learn how to manage the passwords of users and enable the password writeback.

## Points to remember

- Bulk user creation will help to create 1000+ users with just a single click.
- Group creation and configuration will help to manage the user's security permissions.
- You can invite external users using the guest user management.
- Azure self-service password reset will help users to reset their password without the help of a help desk administrator.
- Azure AD Join helps users join their devices to Azure Active Directory. It works on hybrid environments as well.



## Multiple choice questions

1. **What are requirements to configure self-services password reset?**
  - a. User should have some device.
  - b. 2-Method Authentication.
  - c. Device registration to Azure AD.
2. **What is use of Azure AD?**
  - a. Authentication and authorization.
  - b. Apps connectivity.
  - c. On-premises connectivity.
3. **Your customer requested you to create 1500 users in Azure Active directory. Which method will you use to create the users?**
  - a. Go to Azure AD and add all the users manually.
  - b. Go to the Azure ad and invite all the users as bulk guest users.
  - c. Go to the Azure ad and import all the users as bulk users.

## Answers

1. **b**
2. **a**
3. **c**



# CHAPTER 2

# Implementing and Managing Hybrid Identities

## Introduction

In the previous chapter, we discussed how to create bulk users and group management. We also discussed how to invite the guest users.

In this chapter, we will discuss how to implement and manage hybrid identities. We will also discuss how to install and configure the **Azure Active Directory (Azure AD) Connect**, and how to configure the federation services with on-premises AD. We will also cover the managed password sync, password writeback, and so on.

## Structure

The following topics will be covered in this chapter:

- Azure Ad Connect
- Azure Ad Connect Installation
- Manage Azure Ad Connect
- Password Writeback
- Password Sync

# Objectives

In this chapter, we will discuss Azure AD Connect and see how to configure and sync the on-premises identity to Azure AD. We will explain the password writeback and password sync that will help to sync the Azure password to on-premises.

## Azure AD Connect

The Azure AD Connect service can be used to synchronize your on-premises active directory identities to Azure AD. It helps to connect your on-premises users to Azure and other applications, to get authentication with Azure AD, and is also called **hybrid connectivity**.

Integrating the on-premises identity with Azure AD provides a common identity for accessing cloud and on-premises resources. We can use the single identity to access the on-premises and cloud-based applications like **Office 365**, **SharePoint Online**, and so on. It provides the following features:

- **Password Hash Synchronization:** It provides the **single sign-on (SSO)** method to synchronize the password of on-premises users to Azure AD in the hash format.
- **Pass-Through Authentication:** It allows users to use the same password of on-premises and cloud, for signing in to applications. Only the pass-through agent gets installed, and as per the number of authentications per second, we may need more than one agent.
- **Federation Integration:** Federation services can be used to configure the setup of the hybrid environment and SSO, while configuring on-premises **Active Directory Federation Services (ADFS)** which further require an additional server.
- **Synchronization:** It helps to create users, groups, and other objects. It verifies if the identity information of on-premises users and groups, match with the cloud identity. It synchronizes password hashes as well.
- **Health Monitoring:** Azure AD Connect Health provides monitoring for Azure AD Connect, and we can see Azure AD Connect health-related information/errors on the Azure portal.

Azure AD Connect services can be installed in a separate server in the on-premises AD, and can be tightly integrated with Azure AD after installation and configuration. Azure sync services will sync the on-premise AD component to Azure AD. On-premises and Azure users can use the same credentials to log in to Azure and on-premises. For more details, you can refer to [Azure AD Connect](#), which helps you to understand the components. Refer to *Figure 2.1*:

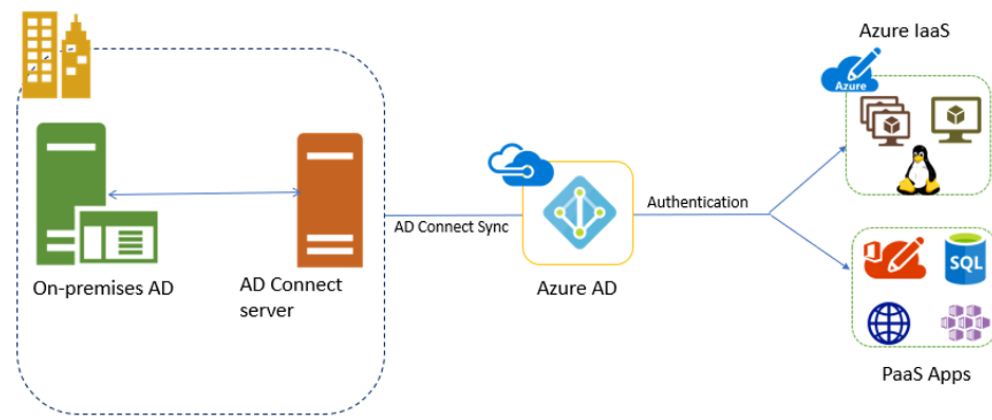


Figure 2.1: Azure AD Connect architecture

## Azure AD Connect installation

Before you install the Azure AD Connect, you need to have the following pre-requisites.

### Pre-requisites

Without the following pre-requisites, you will not be able to configure Azure AD. The following requirements are mandatory. We can see these properties being asked during configuration:

- You should have an Azure AD services/user account, which has global admin rights, to configure the Azure AD Connect to Azure AD.
- You should have an on-premises services/user account which has enterprise admin rights to configure the Azure AD Connect to Azure AD.
- Please download the Azure AD Connect from <https://www.microsoft.com/en-us/download/details.aspx?id=47594>.
- Whenever you configure the AD Connect, the domain name should match with a public domain name, or else, you will get a warning message.

We have created lab environments for demonstration as well as the VMs. We then installed the AD on this server. You can also try the same for testing purpose. It is not recommended for production, but the steps of the Azure AD configuration can be performed. Please follow the given steps to configure the Azure AD Connect:

1. Download the Azure AD Connect (<https://www.microsoft.com/en-us/download/details.aspx?id=47594>). You can also download it from the Azure portal.

2. Click on the AD Connect MSI setup and then click on **Install**, as shown in Figure 2.2:

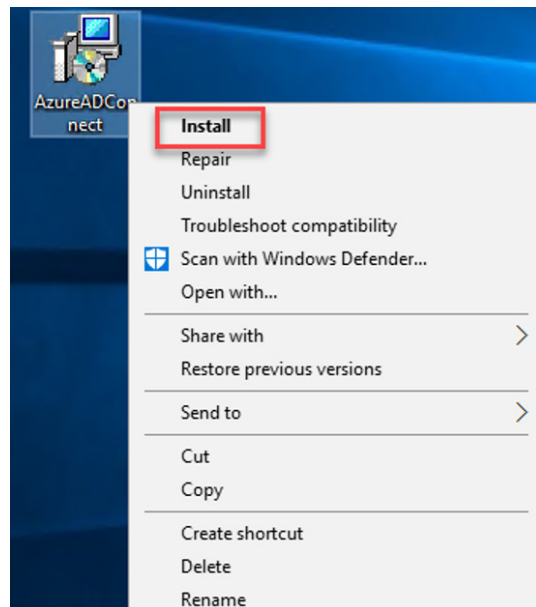


Figure 2.2: Azure AD Connect installation

3. Once you click on the **Install** option, the installation wizard will open.
4. Please agree to the license terms and policy, and click on the **Continue** button, as shown in Figure 2.3:

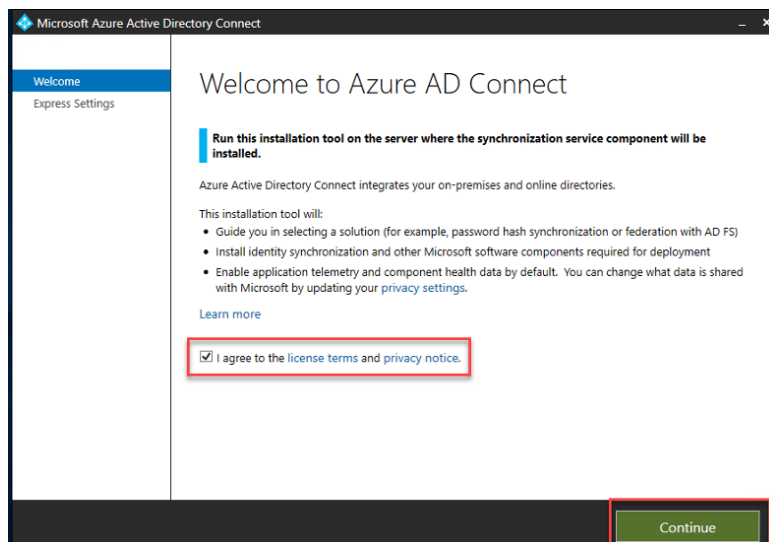
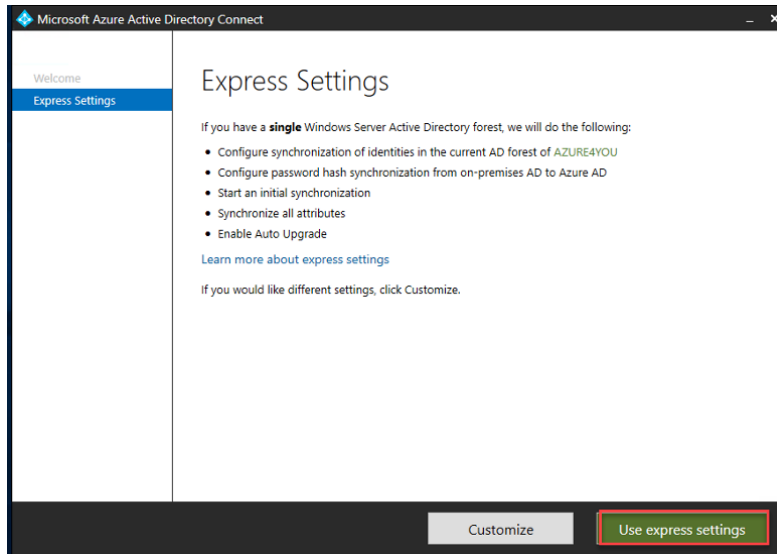


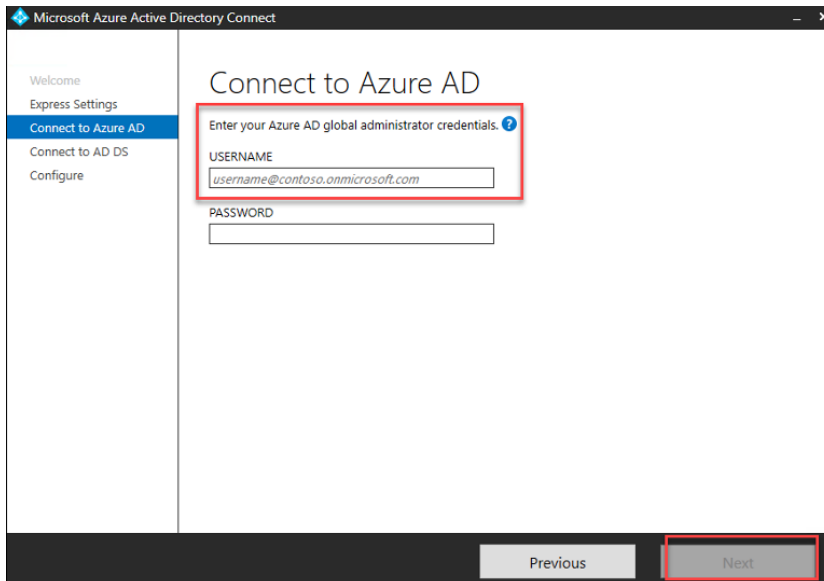
Figure 2.3: Azure AD Connect installation wizard

5. Once done, select the **Express Settings** to configure the Azure AD Connect, as shown in *Figure 2.4*:



*Figure 2.4: Azure AD Connect installation express settings*

6. When you click on the use express settings, it will ask you to provide the global administrator credentials which have `.onmicrosoft.com` in the user ID, as shown in the *Figure 2.5*. It will connect to the Azure AD and verify the credentials before we proceed to the next step.



*Figure 2.5: Azure AD Connect installation connect to Azure AD*

7. Provide the services admin credentials, which have enterprise admin rights.
8. While providing the credentials, please follow syntax: domainname.com/userid.
9. Once you provide the credentials, click on the **Next** button, as shown in Figure 2.6:

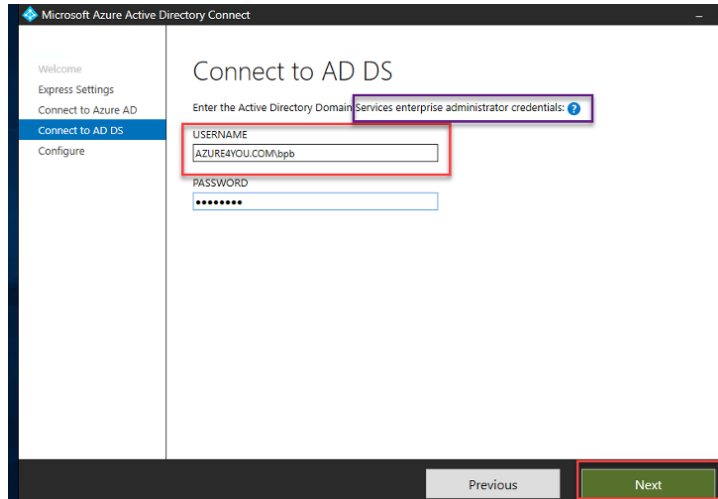


Figure 2.6: Azure AD Connect installation connect to AD DS

10. The user will then be asked to verify the UPN suffix. If you are doing this installation in production, then make sure to match the UPN suffix and move forward. Refer to Figure 2.7:

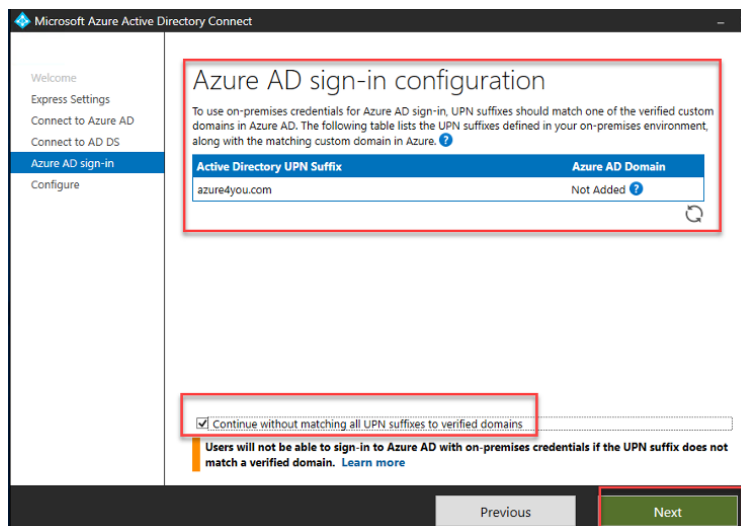
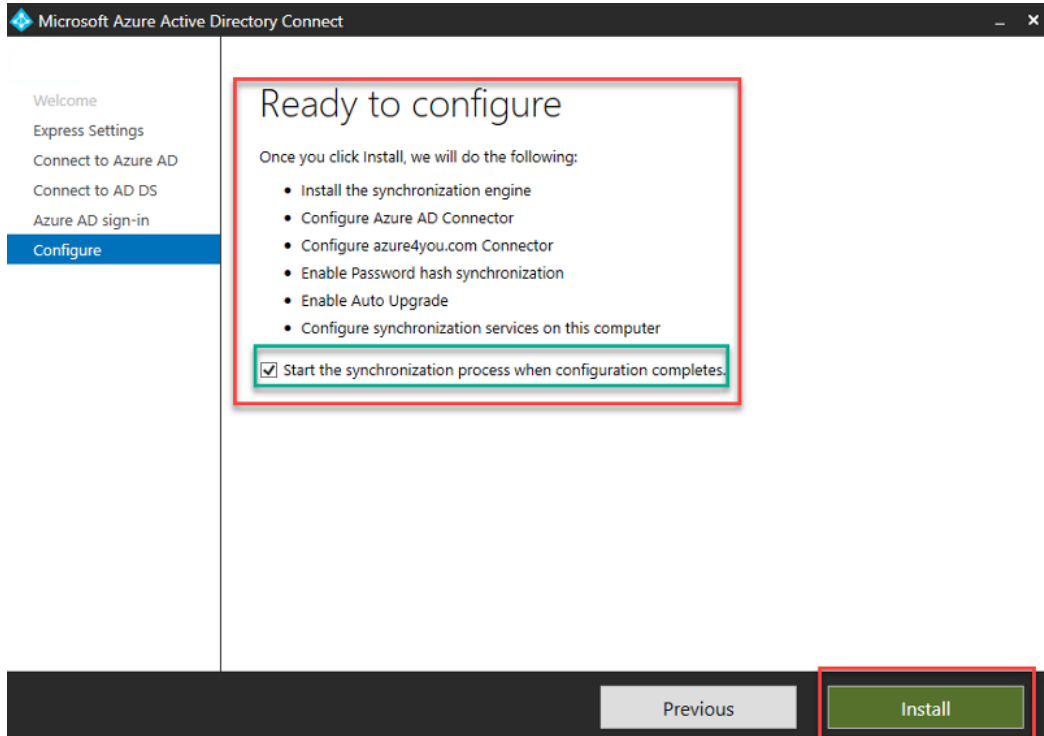


Figure 2.7: Azure AD Connect AD sign-in configuration



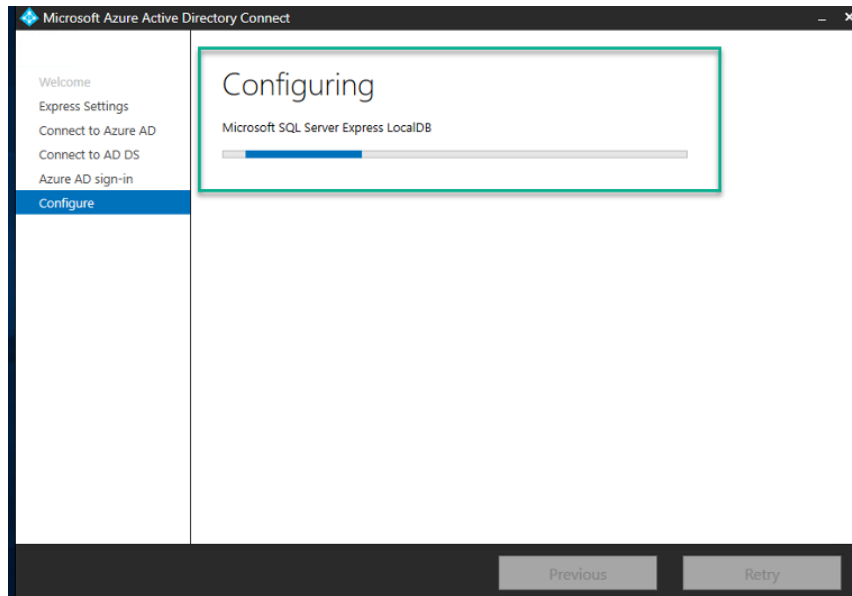
11. Once you click on **Next**, you are ready for configuration.
12. Start the synchronization process when the configuration is completed. However, in production, it is recommended that you start the synchronization process only after the AD Connect installation is completed. Refer to the following *Figure 2.8*:



*Figure 2.8: Azure AD Connect ready configuration*

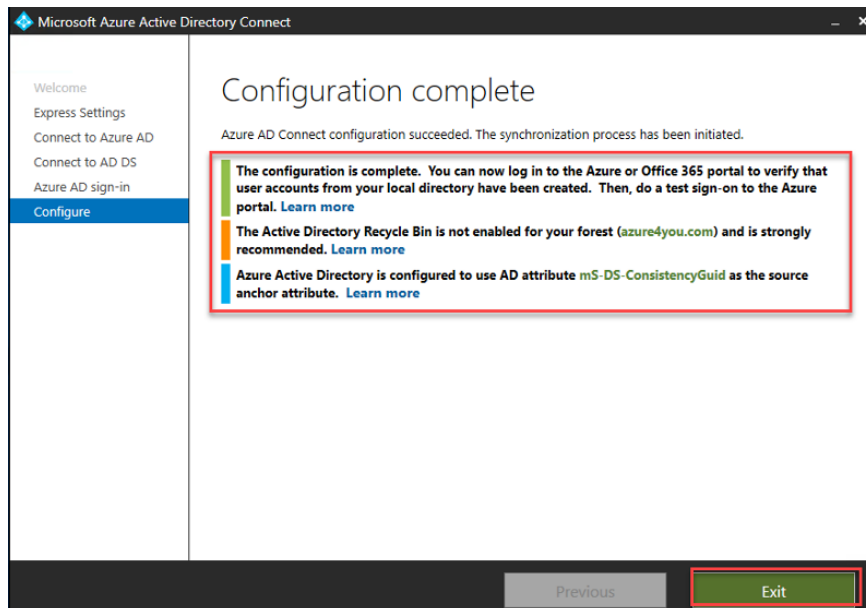
13. When you click on next, it will first verify the connectivity between Azure AD and on-premise. Then, it will configure the connection between Azure AD and on-premises AD. It will install the sync services and verify the Azure AD.
14. Now, it will configure the Azure AD and update the sync.
15. Following that, it will configure the setup to the on-premise domain.
16. After that, it will enable the password hash sync.
17. Now, it will save the sync settings.

18. After that, the final steps will be performed by the AD Connect setup to install and configure the AD Connect Health agent for sync services, as shown in *Figure 2.9*:



*Figure 2.9: Azure AD Connect configuration*

19. The setup has been completed. Exit from the setup as shown in *Figure 2.10*:



*Figure 2.10: Azure AD Connect setup completed*

## Manage Azure AD Connect

We can manage the Azure AD Connect from the portal after installation, and we can see the configuration details of the on-premises AD. To ensure that, follow the given steps:

1. Log in to the Azure portal.
2. Go to **Azure AD Connect** under the **Manage** tab and click on the **Azure AD Connect**. You will be able to see that the last sync is less than 1 hour ago and the sync status has been enabled as shown in *Figure 2.11*:

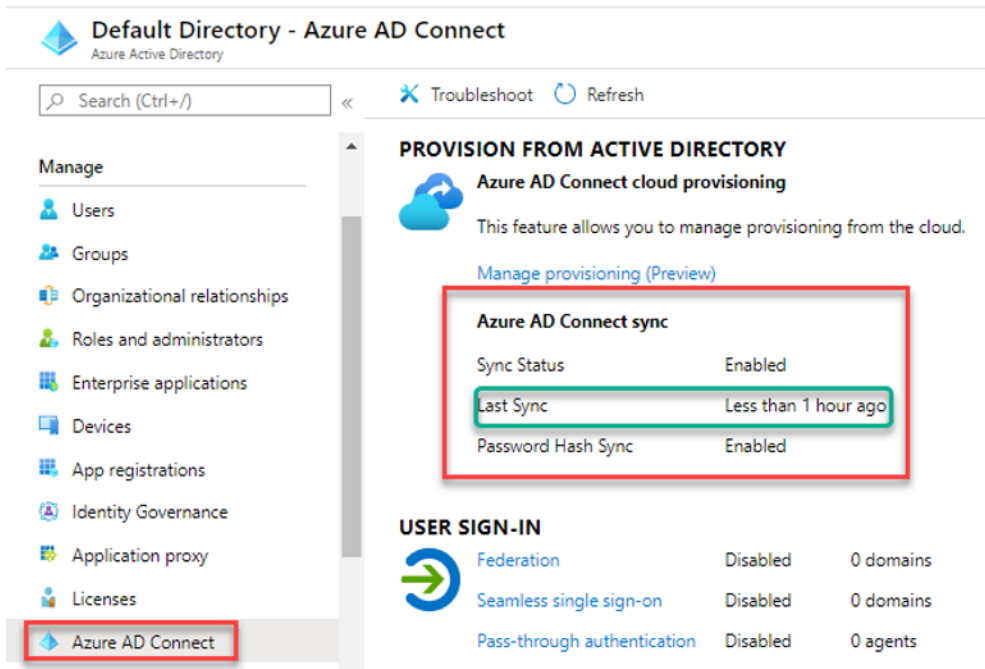


Figure 2.11: Managing Azure AD

3. We can also set up the **Federation**, **Seamless single sign-on**, and **Pass-through authentication** services.
4. Azure AD health services can be managed from the same portal.
5. Let us check whether the users have been synced to Azure AD or not. We will go to the **Users** tab and check the on-premise users, which are synced from your on-premises AD.

6. Now, in Figure 2.12, you can see the user **bpb32** source is **Windows Server AD**, and if you can see Azure AD users, the sources are Azure AD:

| Name                                  | User name                                   | User type | Source                 |
|---------------------------------------|---------------------------------------------|-----------|------------------------|
| bpb32                                 | bpb@lali01rawatoutlookonmicrosoft.com       | Member    | Windows Server AD      |
| On-Premises Directory Synchronization | Sync_bpbAD_9a702d577cd2@lali01rawatoutlo... | Member    | Windows Server AD      |
|                                       |                                             |           | Azure Active Directory |
|                                       |                                             |           | Microsoft Account      |
|                                       |                                             |           | Microsoft Account      |
|                                       |                                             |           | Azure Active Directory |
|                                       |                                             |           | Microsoft Account      |

Figure 2.12: Azure AD user verification

## Password writeback

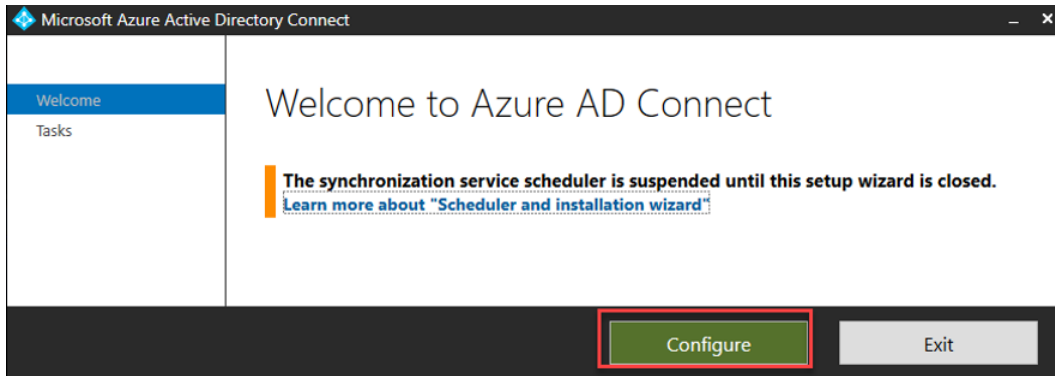
Password writeback will help you synchronize the password which has been changed in Azure AD to on-premises AD. This feature needs to be enabled from the Azure AD Connect and it provides the security mechanism to send the password from Azure AD to the on-premises AD. It provides the following features:

- **Enforcement of on-premises AD password policies:** If users reset their passwords, then it is ensured to meet your on-premises AD policy before committing it to the directory. This review process includes history, complexity, age, password filters, and other password restrictions which have been defined in your on-premises AD.
- **Zero-delay feedback:** Password writeback syncs the operations, and users are notified immediately if their password does not meet the password policy or cannot be changed for any reason.
- **Supports password changes from the Access Panel and Office 365:** When federated or password hash synchronized users need to change their expired or non-expired passwords, those passwords are written back to the local AD environment.
- **Supports password writeback when an Admin resets them from the Azure Portal:** When an admin resets a user's password in the Azure portal, if that user is federated or password hash synchronized, the password is written back to on-premises AD. However, this functionality is not supported from the office admin portal.
- **Does not require any inbound firewall rules:** Password writeback uses an Azure service relay as an underlying communication channel, and all commutation is outbound over port 443.

# Enabling the Password Writeback from the Azure AD

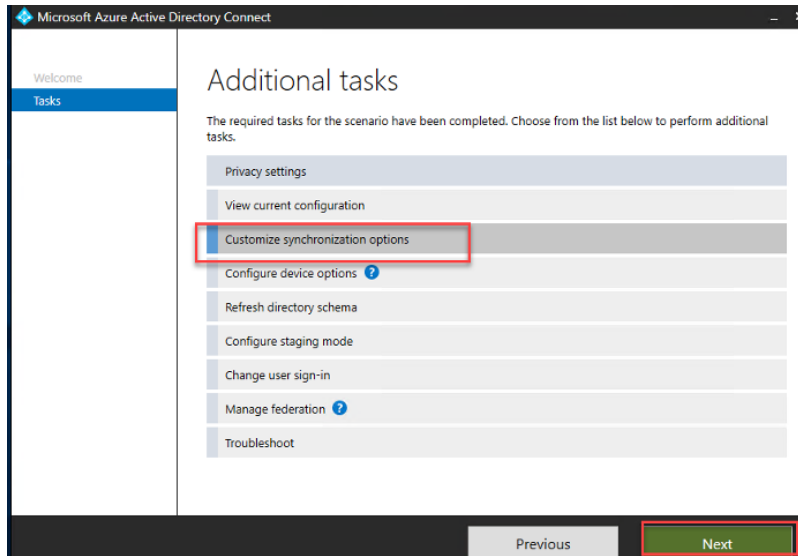
Follow these steps:

1. Log in to on-premises machines where you have installed the Azure AD.
2. Open the Azure AD Connect, and you will see the welcome wizard.
3. Click on **Configure** as shown in *Figure 2.13*:



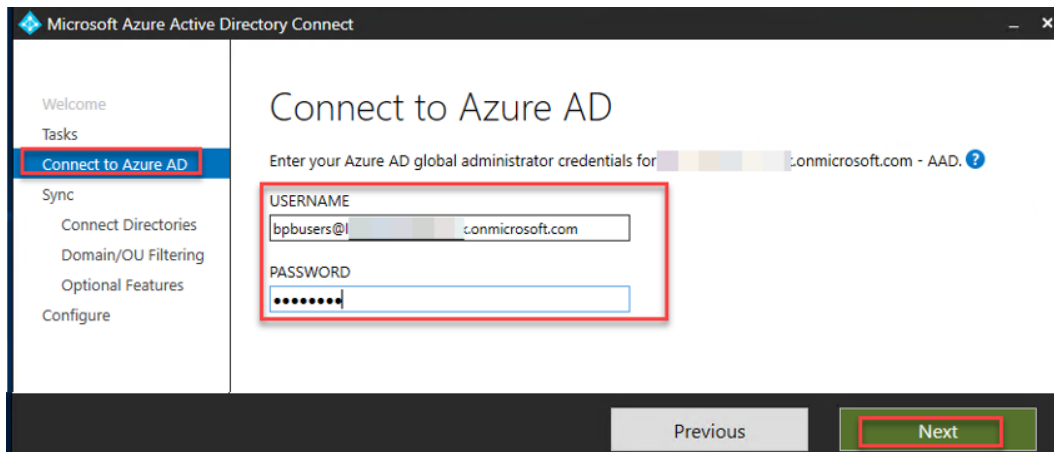
*Figure 2.13: Password writeback*

4. Click on **Customize synchronization options** to configure the password writeback. Refer to *Figure 2.14*:



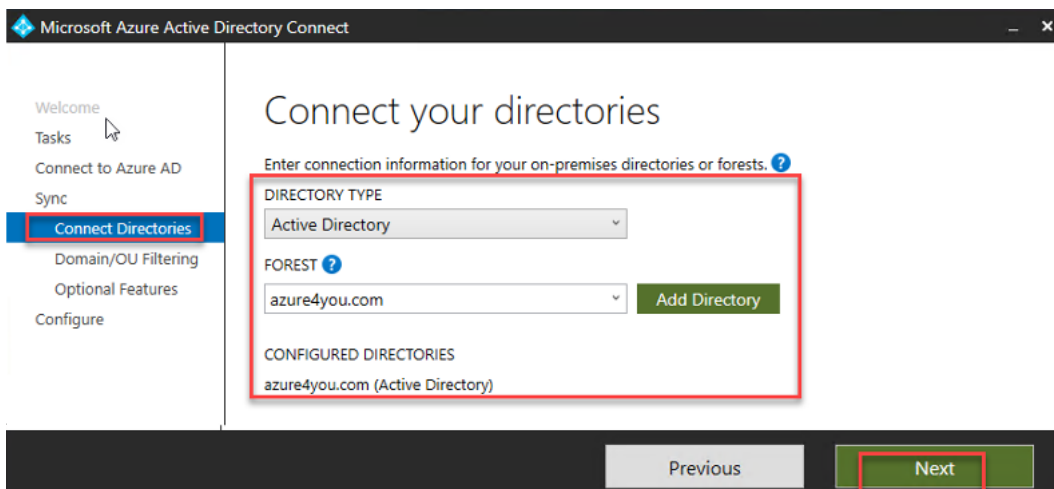
*Figure 2.14: Customize the sync option*

5. It will ask you to connect to the Azure AD and provide the credentials to configure, as shown as *Figure 2.15*:



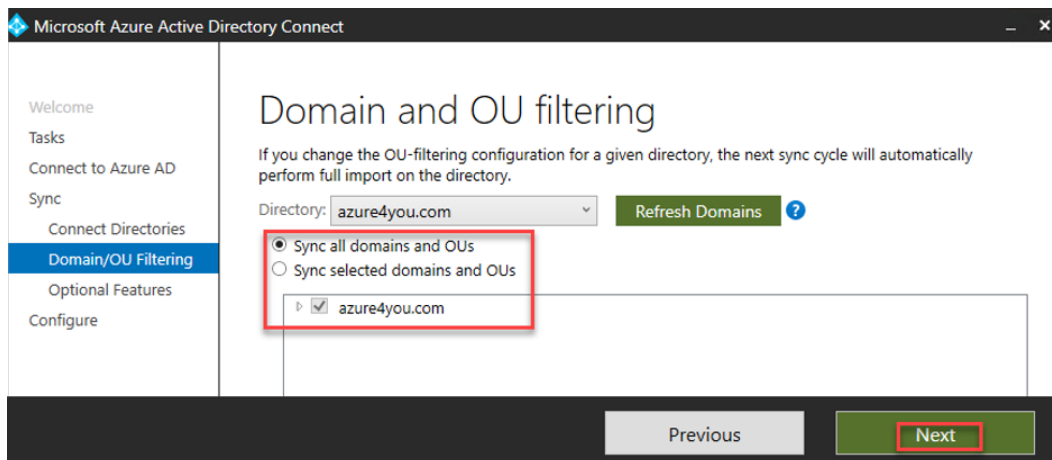
*Figure 2.15: Connect to Azure AD*

6. Now select the type of the directory and forest. Click on the **Next** button as shown in *Figure 2.16*:



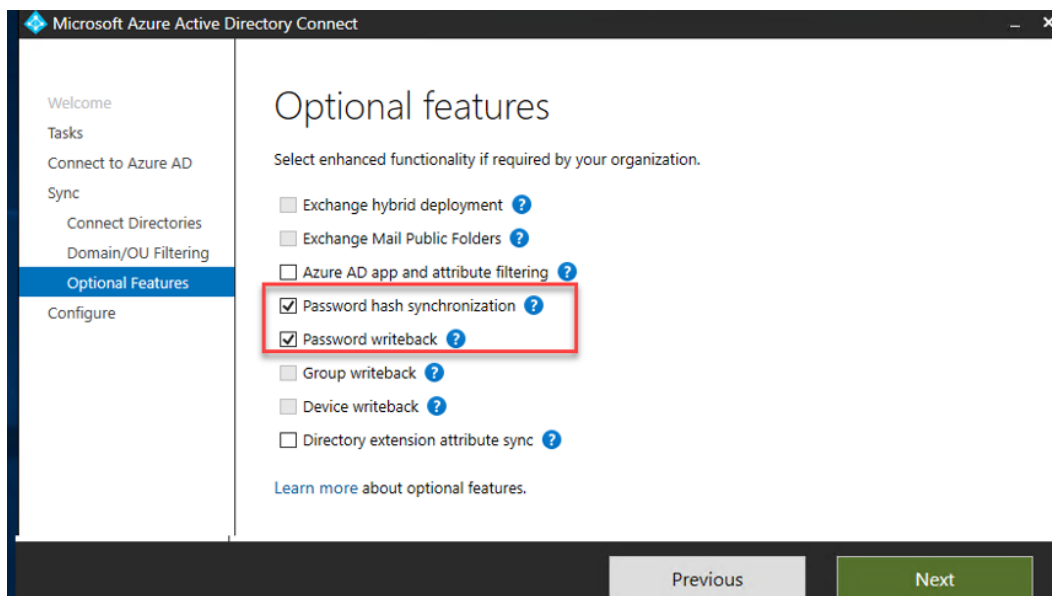
*Figure 2.16: Connect your directories*

7. You can select **Sync all domains and OUs** and your domain as well, as shown in *Figure 2.17*:



*Figure 2.17: Domain and OU filtering*

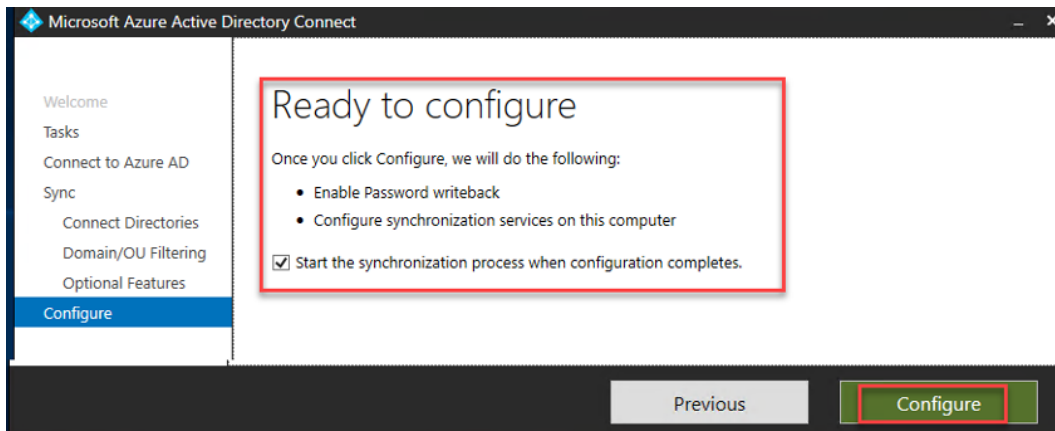
8. Select the password writeback and click on the **Next** button as shown in *Figure 2.18*:



*Figure 2.18: Password writeback enable*

9. Once you are done, click on **Next**, and it will verify all the settings and be ready for configuration.

10. Click on the **Configure** button. It will take a few minutes to complete the sync process and enable the password writeback, as shown in *Figure 2.19*:



*Figure 2.19: Ready to configure*

In this section, we explained and demonstrated how to configure the password writeback. In the next section, we will demonstrate enabling the password writeback from the portal.

## Enabling password writeback from the portal

Follow these steps:

1. For password writeback, we need the Azure AD P1 or P2 license.
2. Go to the portal.
3. Go to Azure AD. Under the **Manage** tab, select **Password reset** as shown in *Figure 2.20*:



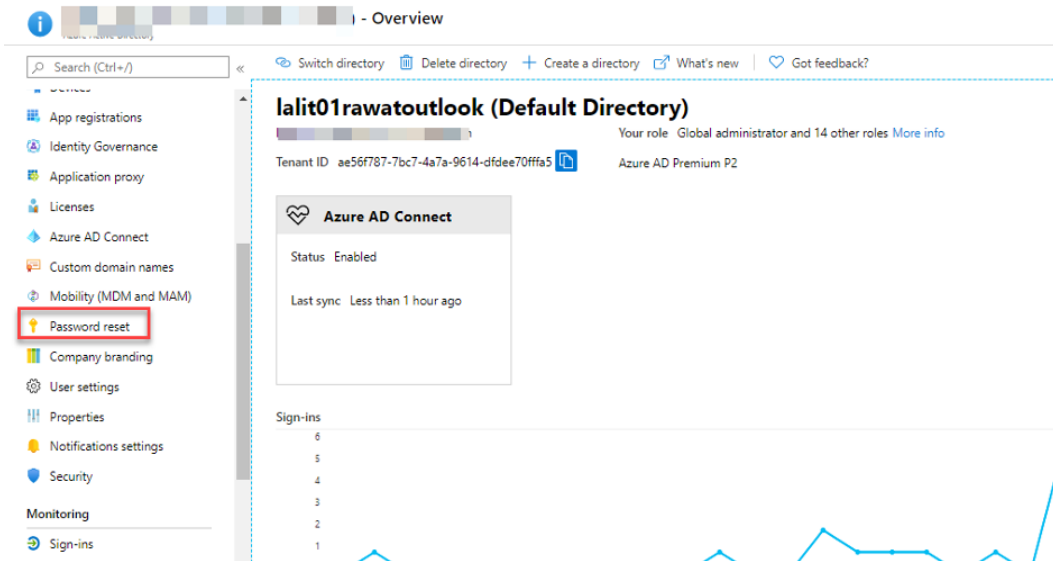


Figure 2.20: Password reset

4. In the password reset, under the **Manage** tab, select the on-premises integration and enable the writeback password to your on-premises directory, as shown in Figure 2.21:

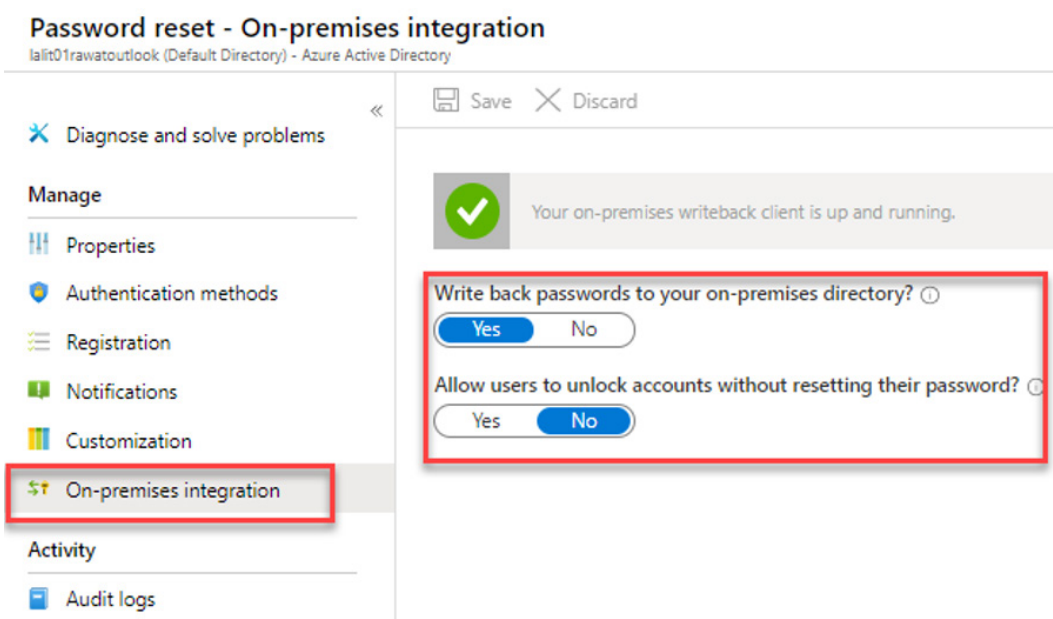
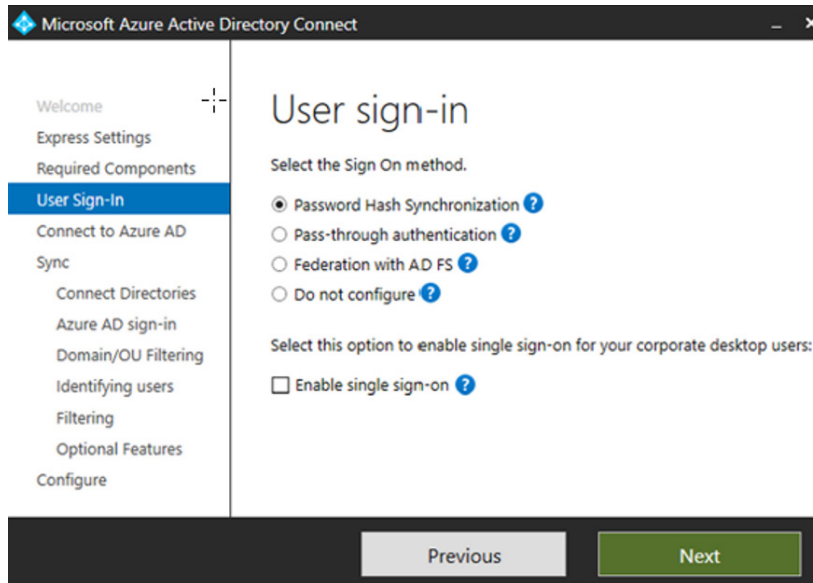


Figure 2.21: On-premises integration

## Password sync

Password sync will be enabled automatically if we select the Azure AD Connect express setting installation. If we choose the custom setting, we can select the password hash sync on the user sign-in page, and enable it, as shown in *Figure 2.22*:



*Figure 2.22: Password Hash sync*

## Conclusion

In this chapter, we discussed Azure AD Connect and how to integrate it with on-premises. We covered how to enable the password writeback from Azure as well.

In the next chapter, we will learn about Azure RBAC roles, utilization of resources and how to apply the different types of RBAC roles using various types of organization policies. We will also cover the custom Azure RBAC roles.

## Points to remember

- Azure AD Connect will help sync your on-premises identity to Azure.
- To install the Azure AD Connect, we would need global administrator and Enterprise admin role, to be assigned to user or services account.
- Password write back option will help if you change the password in Azure. This will resync to on-premises.

- Using Azure AD Connect health, you can monitor the connection health and can troubleshoot the Azure AD Connect related issue.

### Multiple choice questions

1. **What is the use of Azure AD Connect?**
  - a. Hybrid Connectivity.
  - b. On-Premises AD connect to Azure AD integration.
  - c. MFA.
2. **What entity is requested to install Azure AD Connect?**
  - a. Enterprise Admin.
  - b. Global Administrator.
  - c. Both.
3. **What is use of password writeback?**
  - a. Use to sync the users.
  - b. On-premises sync services.
  - c. Sync the password if it changes through Azure portal.

### Answers

1. **b**
2. **c**
3. **c**



# CHAPTER 3

# Managing Role Assignments Through the RBAC Policy

## Introduction

In this chapter, we will discuss Azure **Role-Based Access Control (RBAC)** roles, the custom Azure RBAC roles, their utilization of the resources, and how to apply the different types of RBAC roles using various types of organization policies such as PowerShell, and so on.

## Structure

The following topics will be covered in this chapter:

- Role-Based Access Control
- RBAC access configuration
- Custom RBAC role

## Objectives

We will discuss RBAC implementation in this chapter and see how we can use it in our organization to put control for anonymous access.

## Role-Based Access Control

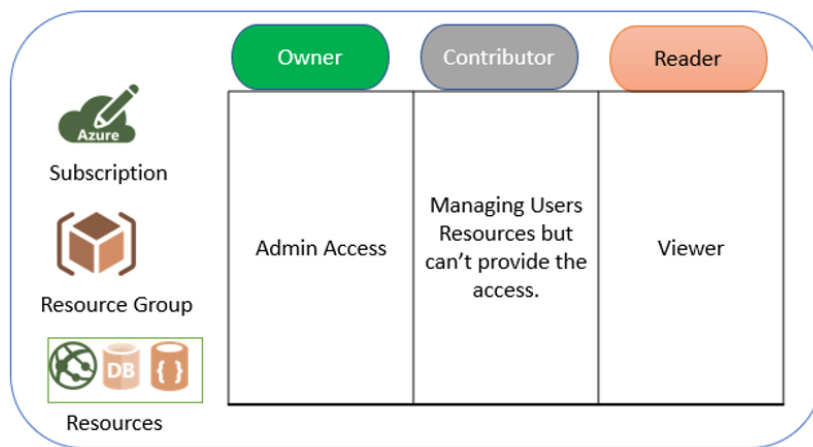
**Role-based access control (RBAC)** helps you to manage and provide access to your resources in a restricted manner.

Let us consider that in an organization, the support team, application team, and the DB team, among others, are using the same subscription. There is a possibility that if you allow everyone access to subscriptions, there might be some changes mistakenly performed by a team member. It could result in a disruptive impact on the existing environment/subscription (production or non-production).

Hence, considering such probable scenarios, MS Azure has come up with a solution called **RBAC policy**, which helps you to control the access. For example, if you want to allow the DB team to access only DB resources, it can be made possible only through RBAC. The DB team can only see the DB resources and cannot make the changes to other services. Thus, using RBAC, you can control this access.

As per the recommendation of MS Azure, the best practice that you can provide is the least role access, which will help the user by providing them the exact access which he needs. RBAC can be applied to *groups*, *applications* or *resources*, and so on.

For any services, there are built-in RBAC roles defined, as shown in *Figure 3.1*:



*Figure 3.1: Azure RBAC role*

Now, let us understand each term:

- **Owner:** The owner will have complete access to all your resources or specific resources, just like the admin of your subscription.
- **Contributor:** The contributor will have equal access like the owner, but cannot provide others the access to resources or at the subscription level. However, he can create and manage the resources.

- **Reader:** In the reader role, a user will have access to read or view permission to specific resources or subscriptions. However, he is not allowed to change or create any new resources.
- **User Access Administrator:** The user access administrator will help you to manage user access to Azure resources.

## RBAC access configuration

RBAC access can be configured from various resources such as Azure resources, Azure subscriptions, and Azure resources group as well. In this section, we will see how to implement those scenarios using RBAC.

## Subscription access using the RBAC policy

We will learn how to provide access to subscriptions as per the organization policy. Follow these steps:

1. Go to the **Subscription** option.
2. Click on **Access control (IAM)**, as highlighted in *Figure 3.2*, and select **Add role assignment**:

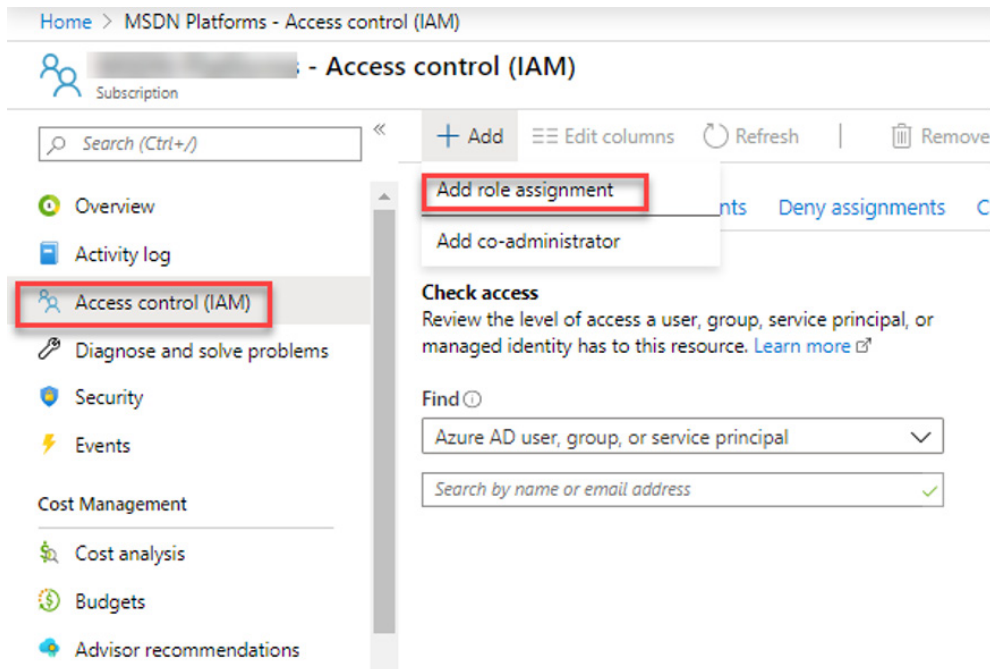


Figure 3.2: Add role assignment

3. Once you click on **Add role assignment**:
  - a. Select the **Owner**, **Contributor**, or **Reader** role as per your requirements.
  - b. Type and search the user ID for which you want to provide the access, as shown in Figure 3.3:

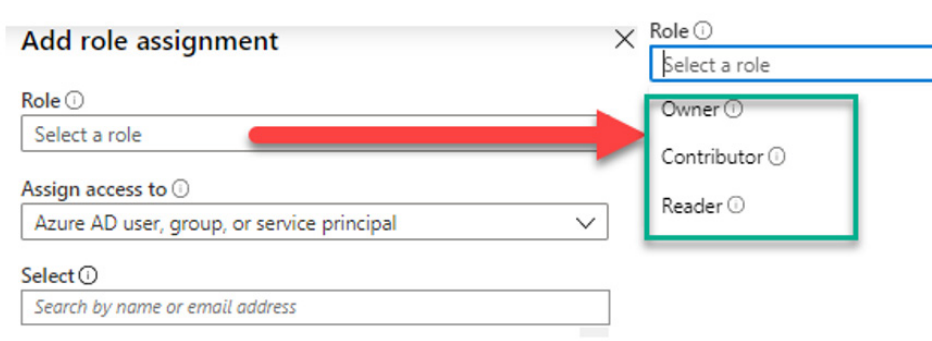


Figure 3.3: Role selection

4. When you select all the required details, your screen will look like Figure 3.4. Click on the **Save** button to apply the changes. Once done, the user will be able to log in to the subscription and access the resources.

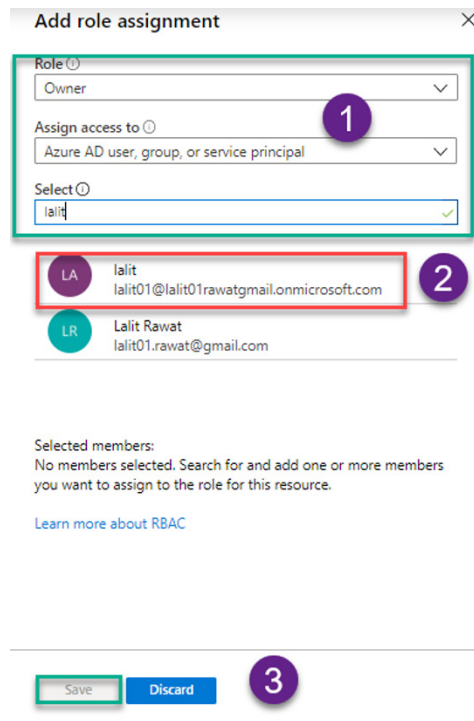


Figure 3.4: Assigning roles

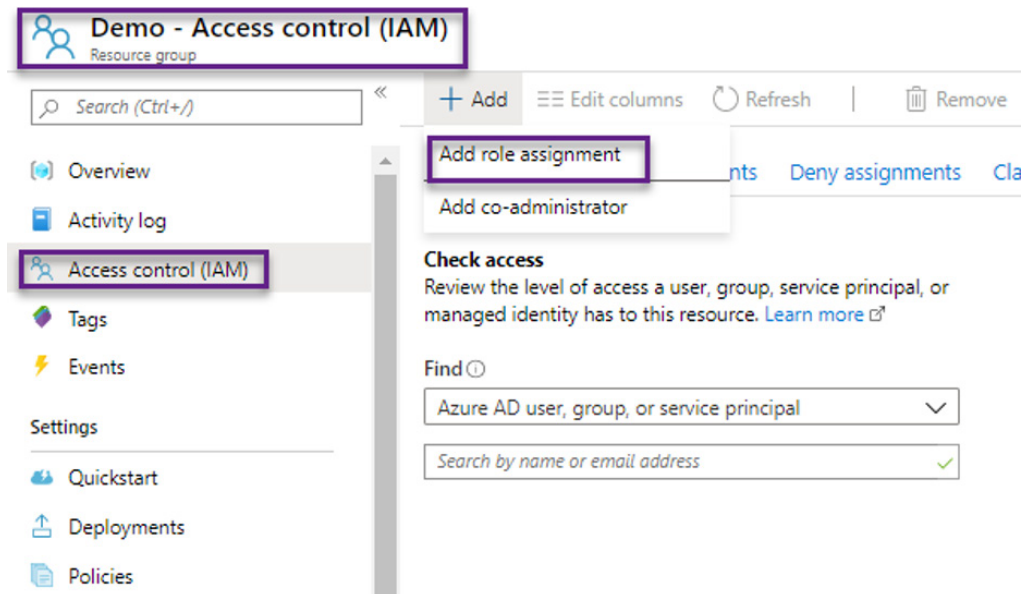


In this section, we learned how to assign the RBAC roles at the subscription level.

## Resource group access using the RBAC policy

We will learn how to provide access to the resources group as per the organization policy. Follow these steps:

1. Go to the **Resource group** option.
2. Click on **Access control (IAM)** and select **Add role assignment** as shown in *Figure 3.5*:



*Figure 3.5: Resources group role assignment*

3. Once you click on **Add role assignment**:
  - a. Select the **Owner**, **Contributor**, or **Reader** role as per your requirements.
  - b. Type and search the user ID for which you want to provide the access.
  - c. Once you select all the required details, your screen will look like *Figure 3.6*. Click on the **Save** button to apply the changes.

- d. Once done, the user will be able to see the resource group and its resources which reside in the resource group:

**Add role assignment** >

Role ⓘ  
Contributor

Assign access to ⓘ  
Azure AD user, group, or service principal

Select ⓘ  
tra ✓

No users, groups, or service principals found.

Selected members:

TR training  
training@... Remove

Save Discard

*Figure 3.6: Resource group contributor role assignment*

In this section, we learned how to assign the RBAC roles at the resource group level.

## Resource access using the RBAC policy

We will now learn how to provide access to resources like Virtual Machines (VMs), DB, and so on, as per the organization policy.

1. Go to the resource for which you would like to provide access, such as VM, DB WebApps, and so on.
2. Click on **Access control (IAM)** and select **Add role assignment**, as shown in *Figure 3.7*:

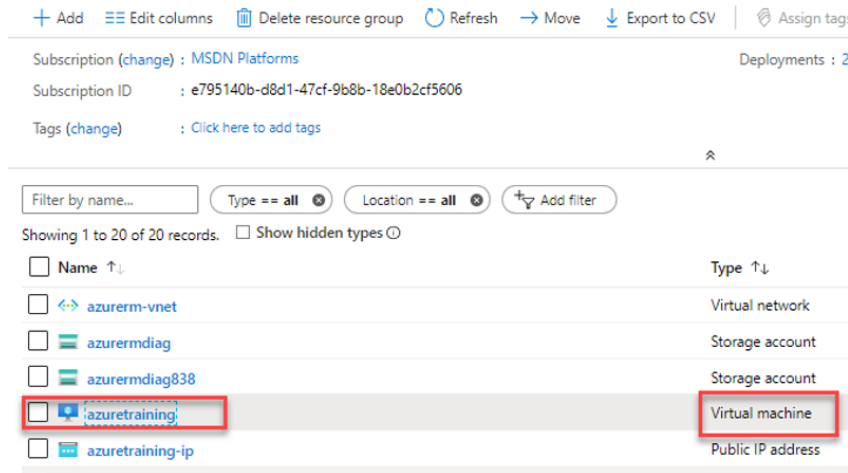


Figure 3.7: Resources role assignment

3. When you click on **Add role assignment**, select the role you want to assign the resources to:
  - a. Select the **Owner**, **Contributor**, or **Reader** role as per your requirements.
  - b. Type and search the user ID for which you want to provide the access.
  - c. Once you select all the required details, your screen will look like Figure 3.8. Click on the **Save** button to apply the changes.
  - d. Once done, the user will be able to see the resources and access the resources.

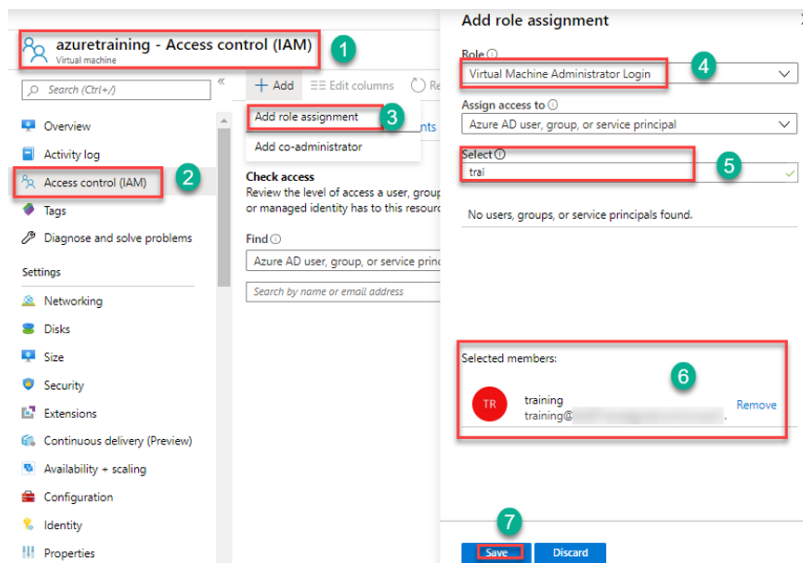


Figure 3.8: Role assignment of VM

## Custom RBAC role

Custom roles come into the picture when the built-in roles do not meet your customer or organization requirements. In that case, you can create a custom role using PowerShell, **Azure Resource Manager (ARM)** template, CLI, or REST API. You can create up to 5000 custom roles in each tenant-level, but for a government cloud such as in the case of countries, say China, Germany, and so on, you can only create up to 2000 custom roles per tenant.

## Creating the custom role

In this section, we will learn to create the RBAC custom role and how to use existing built-in rules to create a new custom role.

If you want to allow users have access to any action, it should be listed in the **Actions** section and the deny user action can be put in the NotActions section, while creating the custom RBAC.

If you would like to see what permission is available in the Azure contributor role, take a look *Figure 3.9*, for the definition of the contributor role, for more details:

```
PS Azure:\> Get-AzRoleDefinition "Contributor"

Name           : Contributor
Id             : b24988ac-6198-42a0-ab88-20f738dd24c
IsCustom       : False
Description     : Lets you manage everything except access to resources.
Actions        : (*)
NotActions     : (Microsoft.Authorization/*/*Delete, Microsoft.Authorization/*/*Write, Microsoft.Authorization/elevateAccess/Action, Microsoft.Blueprint/blueprintAssignments/write...)
DataActions    : {}
NotDataActions : {}
AssignableScopes : {/}
```

*Figure 3.9: Definition of a contributor role*

1. Run the following command in PowerShell, as can be seen in *Figure 3.10*:  
**Get-AzRoleDefinition "Contributor" | ConvertTo-Json**

```
Azure:/
PS Azure:\> Get-AzRoleDefinition "Contributor" | ConvertTo-Json
{
  "Name": "Contributor",
  "IsCustom": false,
  "Description": "Lets you manage everything except access to resources.",
  "Actions": [
    "*"
  ],
  "NotActions": [
    "Microsoft.Authorization/*/*Delete",
    "Microsoft.Authorization/*/*Write",
    "Microsoft.Authorization/elevateAccess/Action",
    "Microsoft.Blueprint/blueprintAssignments/write",
    "Microsoft.Blueprint/blueprintAssignments/delete"
  ],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ]
}
```

*Figure 3.10: Contributor role in JSON format*

Once you get the output, copy the file and change the action or not action rule accordingly. We will change the **NotActions** rule to **Actions** and create a custom role.

Save the file in the **JSON** format.

```

1. {
2.   "Name": "BPB_Contributor",
3.   "IsCustom": false,
4.   "Description": "Lets you manage everything except access to resources.",
5.   "Actions": [
6.     "Microsoft.Authorization/*/Delete",
7.     "Microsoft.Authorization/*/Write", "Microsoft.Authorization/elevateAccess/Action", "Microsoft.Blueprint/blueprintAssignments/write",
8.   ],
9.   "NotActions": [
10.    "
11. Microsoft.Blueprint/blueprintAssignments/delete"
12.   "DataActions": [],
13.   "NotDataActions": [],
14.   "AssignableScopes": [
15.    "/"
16.   ]
17. }
```

2. Go to PowerShell and connect to the subscription using the following command:

**Connect-AzSubscription**

3. Provide the user ID and password to get authenticated. Then, run the following command to create a new role:

**New-AzRoleDefinition -InputFile "C:\Temp\BPB\_Role.json"**

Once done, you will be able to create a custom role. It will look something like *Figure 3.11*:



*Figure 3.11: Contributor role*

## Conclusion

In this chapter, we covered the different types of RBAC roles and learned how to assign the RBAC custom roles in the subscription, resources group, and resources. We discussed how to create the custom role to match the organization or client requirements.

In the next chapter, we will learn about the Azure subscription and resource management. We will also focus on different types of subscriptions and see how to manage Azure resources.

## Points to remember

- Azure role-based control will help you in subscription access control.
- You can assign the RBAC in subscription, resources group and resource level.
- Custom roles can be created and assigned to specific users or group.
- RBAC role can be configured while selecting the resources group or subscription. Go to the IAM section to configure the specific role.

## Multiple choice questions

1. The customer asks for the IT admin access so that they can manage the subscription and provide access. In this case, which RBAC Role access can you provide to the user?
  - a. Owner
  - b. Contributor
  - c. Reader

2. **The client wants to provide access to just the virtual machine and not the entire subscription. How can they provide this access to the virtual machine?**
  - a. Go to subscription and click on IAM add user as contributor.
  - b. Go to Resource group and click on IAM add user as contributor.
  - c. Go to Virtual machine and click on IAM add user as contributor.
3. **The client wants to provide access to only the storage account, where the user can access blob (container). How can you make sure that we will have access to blob storage, and not to the whole storage account?**
  - a. Go to subscription and click on IAM add user as storage contributor.
  - b. Go to storage account and click on IAM add user as table contributor.
  - c. Go to Virtual machine and click on IAM add user as Blob (Container) contributor.

## Answers

1. a
2. c
3. c





# CHAPTER 4

# Managing Azure Subscription and Resource Management

## Introduction

In this chapter, we will cover Azure subscription and resource management. We will focus on the types of subscription and how to manage Azure resources. We will learn how to create a free subscription, types of subscriptions, how to manage resources using the RBAC policy. What is a quota and *how the use of the resources lock will help you from accidental deletion of resources?* Let us learn all this in this chapter.

## Structure

We will cover the following topics in this chapter:

- Azure subscription
- Enterprise Agreement subscription
- Azure Subscription Support Plan
- Creating a Free Azure Subscription
- Global Administrator Permission
- Resources Group
- Cost Management

- Azure Subscription Policy
- Azure Quota
- Resource Tag
- Creating and Configuring Management Group

## Objectives

In this chapter, we will discuss Azure subscription, and the types of subscription available. We will also discuss the step-by-step process to utilize Azure subscription, and so on. This will help all the levels of readers to get a better understanding of this topic.

## Azure subscription

Azure subscriptions are a collection of resources known as billing containers. Each subscription has a unique ID, that has been generated by **Microsoft (MS)** automatically while creating the Azure subscription. If you need to create or access the resources, then you need a subscription access. Without the subscription access, you will not be able to access the resources under Azure subscription.

Let us take a look at the different types of Azure subscriptions:

- **Free subscription:** Microsoft provides this subscription. It is free for the first 30 days and includes \$230 credit and free 25 services for 12 months. It is used for practical and learning purposes.
- **Pay-as-you-go subscription:** This mode of subscription has a flexible payment method and is widely used in organizations. However, you will have to pay only the services which you consumed in your azure subscription (Compute, network, web apps and so on). There is no limit for purpose or commitments. A customer can easily cancel the subscription as well.
- **Microsoft resellers:** The **Cloud Solution Provider (CSP)** subscription is used only at the organization level. MS provides employees the access to work with partners directly, to design and implement the solutions to meet the project requirements.
- **Open:** This subscription provides the flexibility to work with the same vendor from where we purchased the open volume license program and activated the Azure subscription.
- **Azure Government Customer:** This subscription is used for US government entities that are eligible to purpose Azure government services. They can also use the pay-as-you-go service.

- **Azure Germany Customers:** This subscription is used for European Union or **European Free Trade Association (EFTA)** entities that are eligible to purpose Azure government services. They can also use the pay-as-you-go service.

## Enterprise Agreement Subscription

The **Enterprise Agreement (EA)** is designed for organizations. In this subscription, the customer has to sign an agreement with Microsoft directly, which helps give a better discount on your Azure resources consumption. When an organization signs up for the EA agreement, a billing account is created, and the billing can be done monthly, quarterly, or yearly based on the agreement.

### Enterprise

It is most commonly known as Enterprise agreement, and it is only used by organizations. The EA subscription can be accessed from the Enterprise portal (<https://ea.Azure.com>) and used to create multiple departments to manage the subscription.

### Departments

It is a sub-account of Azure EA subscription, where we define the departments and associate a subscription to it. We can add the subscriptions under the department, which helps to bifurcate the billing department wise.

We can add multiple departments based on the organizational needs and assign a department owner who can manage the department and subscription under it.

It will also help add a cap on Azure consumption and based on the subscription utilization, the monthly or yearly budget can be decided.

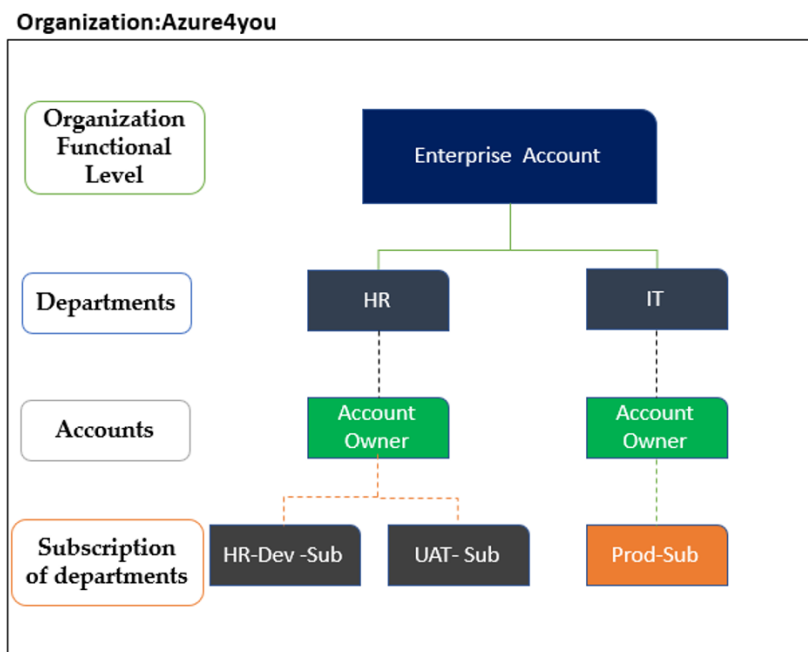
### Accounts

Accounts can be created by a different department and an account administrator can add new accounts to their departments, to provide them access to the Azure account. Even an account administrator can create the subscription.

### Subscriptions

As defined in the Azure subscription level, the subscription is a billing container and all the billing for consumed resources happens at the subscription level. We can

set up billing alerts of the budget spent, to get an early notification if there is more consumption during a specific period. Refer to *figure 4.1* for more details:



*Figure 4.1: Enterprise subscription*

## Azure Subscription Support Plan

Along with the subscriptions discussed earlier, we can also opt for the following support plan with a subscription, which will help connect to the MS support team to fix or troubleshoot the issue.

## Azure Developer Support

This kind of subscription support plan is most commonly used for Azure development/testing purposes, where MS provides the discounted rates on Azure, to support any ongoing development and testing activity.

## Professional Direct Support

This subscription support plan can be used by companies where MS includes its technical, billing, and other teams, to get a faster resolution and support.

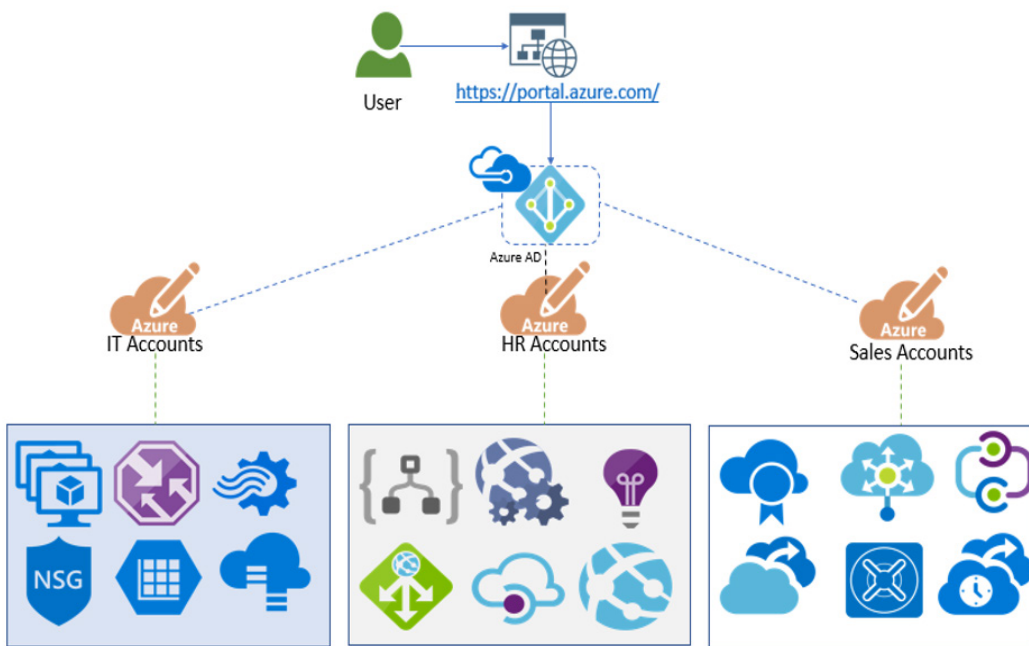
## Standard Support

This subscription support plan can be used by companies where MS includes its technical, billing, and other teams, to resolve your issues faster with 24/7 support. Most of the companies use this subscription to fix the critical dependence on the Azure subscription.

## Azure tenant

An Azure tenant is nothing but Azure AD. It is a dedicated instance of Azure AD that an organization receives and authorizes the users to various cloud services. An Azure tenant can have multiple subscriptions. However, a subscription cannot have multiple tenants.

In the following *Figure 4.2*, you can see three subscriptions and one directory. All the others are different. Once you create the subscription, the first tenant (Azure AD) will be created, and then the subscription will be associated with it. If you have a tenant, then you can create multiple subscriptions. Let us take a look at *Figure 4.2* to get an understanding of how tenants work in Azure:



*Figure 4.2: Azure tenant*

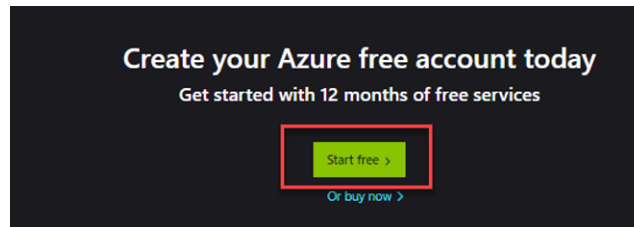
## Creating a Free Azure Subscription

While creating the free subscription, the following benefits are provided by MS Azure:

- 12 months of free popular services.
- \$200 credit to explore services within 30 days.
- 25 services are always free.

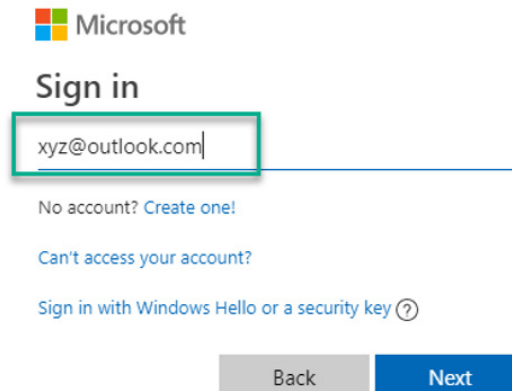
If you would like to create the free Azure subscription, follow the given steps:

1. Go to the URL <https://Azure.microsoft.com/en-us/free/>.
2. Click on **Start free** as shown in *Figure 4.3*:



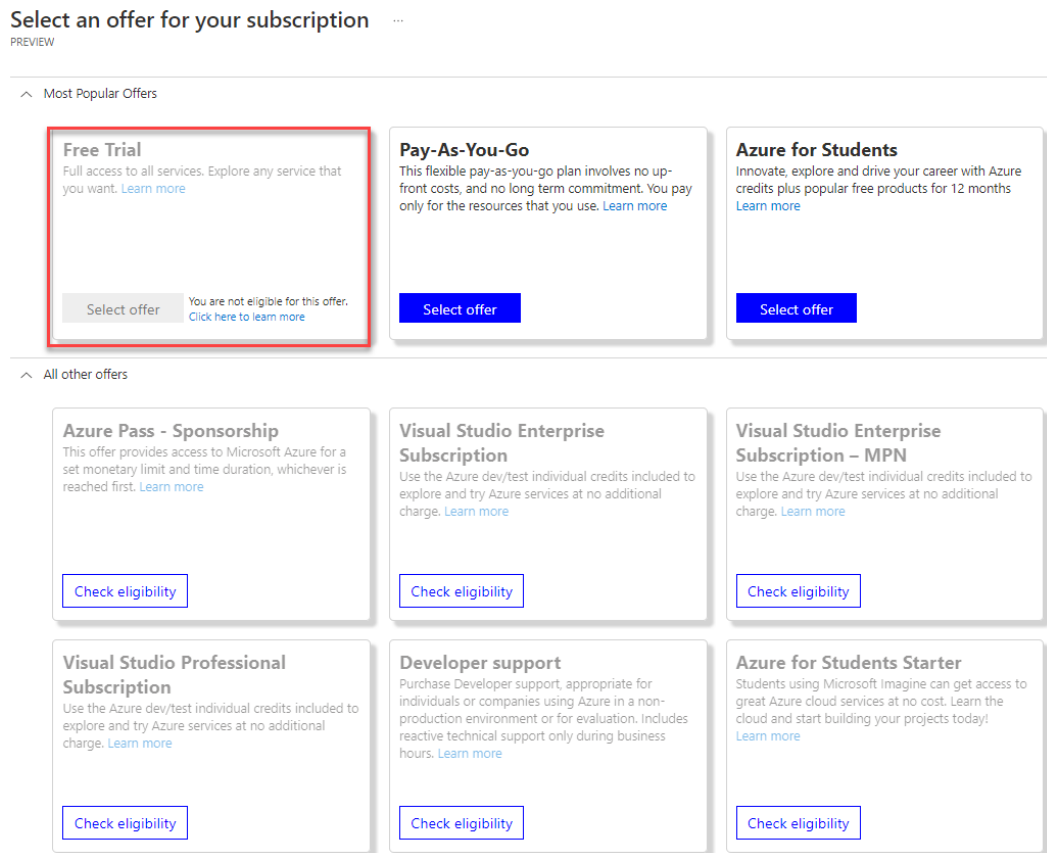
*Figure 4.3: Free subscription*

3. It will ask for the login ID and password.
4. Provide the Microsoft ID (for example, bpb@outlook.com, bpb@live.com, and so on).
5. You can even log in through your organization ID, such as [Azure4you@mycompany.com](#). Provide your details as shown in *Figure 4.4*:



*Figure 4.4: Login screen*

6. Provide the password for the same. After this, you will be able to log in to the subscriber page.
7. Click on the free subscription option.
8. Select **Free Trial** as shown in *Figure 4.5*:



*Figure 4.5: Select the subscription*

9. Select the country code.
10. Provide the mobile number and click on **Text me** or **Call me** to get the verification code.
11. Once you get the verification code, put it in the **Verification code** section. Click on the **Verify code**.
12. Once the code is verified, you will be directed to the next tab to fill the payment information.

Take a look at *Figure 4.6* for more details:

1 Identity verification by phone

A text or phone call helps us make sure this is you.

Country code

India (+91) 1

Phone number

Please provide your phone number 2

Text me 3 Call me

We delivered a code to your phone.

Verification code

Please provide your Verification number 4

This field is improperly formatted

5 Verify code I did not receive a code

*Figure 4.6: Details for subscription*

13. Refer to the numbered areas in *Figure 4.6* and fill in the payment details such as the card holder's name, the card number, expiry date, CVV number, and address details. Once done, click on the **Next** button.
14. Understand the service usage and click on **Next**.
15. If you want to add MS support plans, you can do it. (Since it is chargeable, it is better to not add this plan.)
16. Click on the **Agreement** section and then on the **Signup** button.
17. 10 minutes later, you will receive the subscription.
18. We can now utilize our subscription and create the services in Azure. Provide the details as shown in *Figure 4.7*:



**2 Payment Information**

Note, we do not accept debit or prepaid cards because they do not support monthly payments in your location. Please use a credit card.

We accept the following cards:



Cardholder Name

 Please provide the card holder name 1

Card number

 Please provide the card Number 2

Expires

MM YY Please provide the Expiry Date 3

CVV 4

 Please provide the CVV Number, what's this?

Address line 1

 5

Address line 2 (Optional)

 Please provide the Address Details

Address line 3 (Optional)

City

State

--Select--

Postal Code

Country/Region

India

Next 6

3 Service Usage Address 7

4 Add technical support 8

5 Agreement 9

Figure 4.7: Payment details and agreement

**Note:** When you create the subscription, make sure you put all the details correctly as this will be used for MS internal purpose. When you add your card initially, it will charge a minimal amount (around Rs 2), to verify your credit card and only after that will it allow you to create the free subscription.

## Global administrator permission

Users who have the global administrator permission, can access all administrative services such as Azure Active Directory, and federate services, to Azure Active Directories such as *Exchange Online*, *SharePoint Online*, and *Skype for Business Online*.

The first user ID who signs up for the Azure Active Directory tenant or subscription, becomes a global administrator and only global administrators can assign other administrator roles. We can have more than one global administrator at the organization level. Global admins can reset the password for users and all other administrators.

Follow the given steps to provide the global admin access step by step:

1. Click on the **Azure Active Directory** option.
2. Go to **Manage** and click on the **Users** option.
3. Click on **All users**.
4. Select the user or search the users you want to assign the permission.
5. Select details, as shown in *Figure 4.8*, for subscription details:

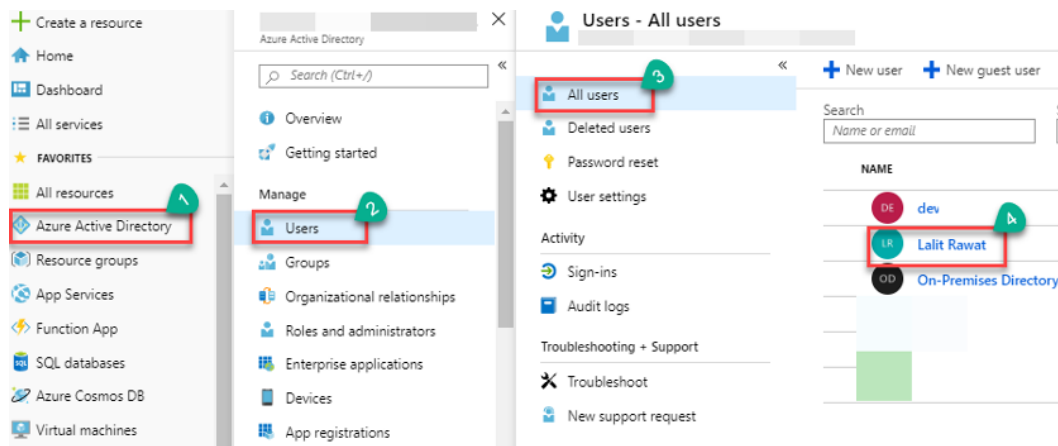
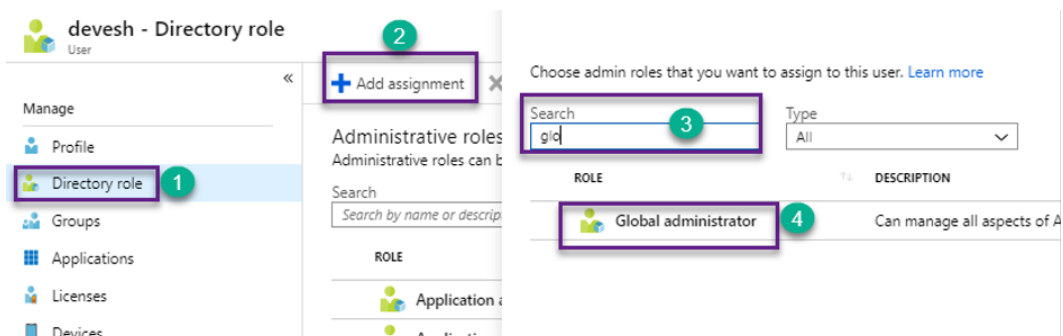


Figure 4.8: Global administrator role

6. Click on the user's name and then click on **Directory role**.
7. Then, click on **Add assignment**.
8. Click on **Search** and search for a **Global administrator** role.
9. Select the **Global administrator** role.

10. Click on the **Save** button, and your user will have global administrator access. Follow the steps as shown in *Figure 4.9*:



*Figure 4.9: Directory: global admin role*

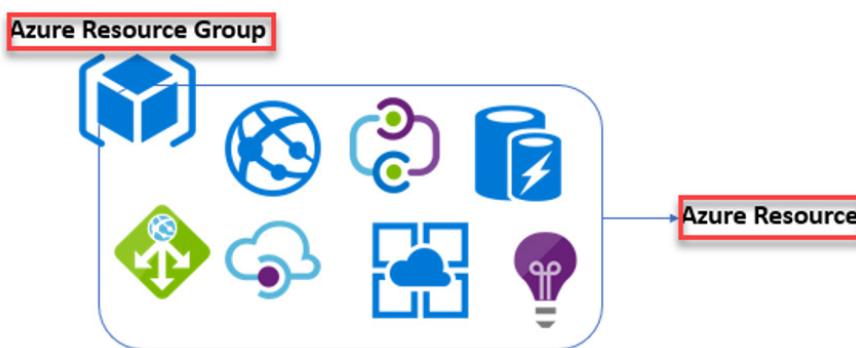
## Resources group

An Azure resource group is a logical container that contains the Azure resources in it. Resources manage the resources within the resources group together as an entity.

If you have provided the permission to a resource group, then you can also view all the resources which are available in the resource group.

You can even create or delete the resource group. If you delete the resource group, then all the resources which are present in the resource group will be deleted automatically.

For a better understanding, let us take a look *Figure 4.10*:

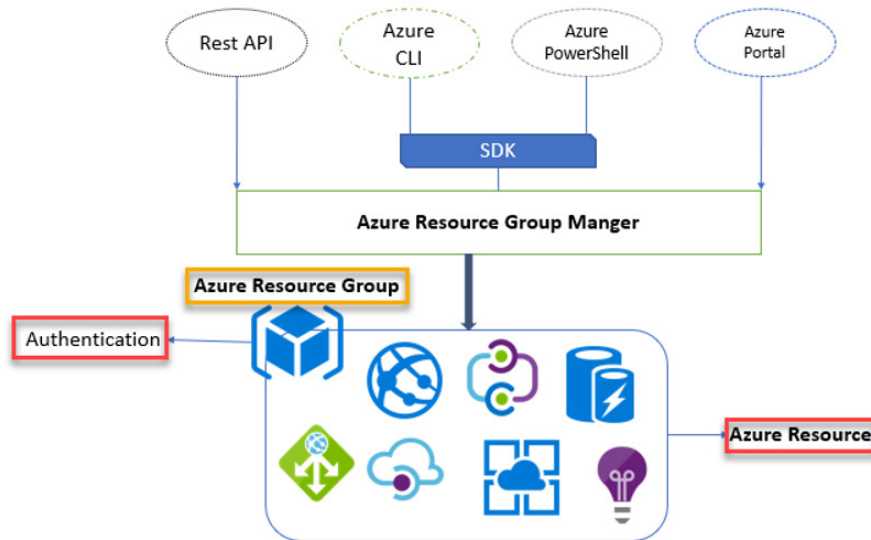


*Figure 4.10: Azure resource group*

## Azure Resource Group Manager

Azure Resource Manager is a deployment and management service for Azure. It provides management layers that will help to create, update, modify, and delete

the resources within the subscription. We can utilize the features like access control, lock, and tag. Refer to the *Figure 4.11*, for more details about Azure resource group manager:



*Figure 4.11: Resource group manager*

## Cost management

Azure Cost Management will help you to manage and control your cost. Organizations can utilize cost management to analyse and manage the cost. It gives the breakup cost of each resource and resource group. It uses advanced analytics to provide a customized cost to customers. The cost will be shown based on the consumption of each service and third-party services such as Red Hat, Oracle checkpoint firewall, and so on.

## Exploring cost management

Cost management will add all the subscriptions which are under one tenant. To get the report of each tenant separately, you need to perform the following steps:

1. Click on the **Cost Management + Billing** option from the **FAVORITES** item or search on the Azure portal.
2. Click on **Overview** that will help get all the subscription accounts under your tenant.
3. Then, you will be able to view how much you have spent every month. For a detailed analysis, use the cost management tool and follow the steps performed, as shown in *Figure 4.12*:

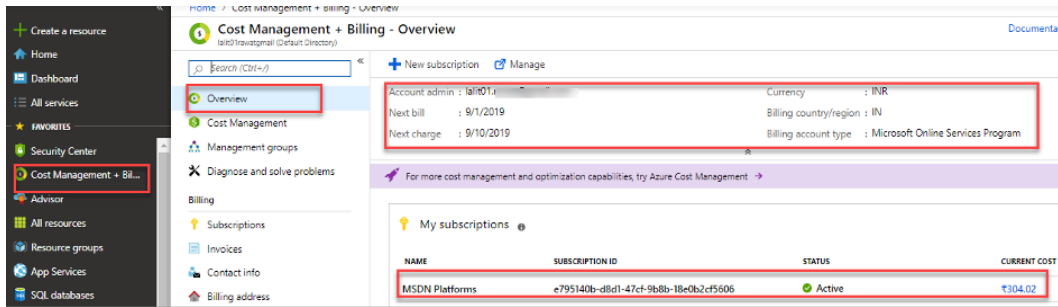


Figure 4.12: Exploring cost management

Cost management tools will help you to get more details of resource services costs, and help you set up an alert for your Azure account. Furthermore, the budget can be defined as well. Follow the given steps to configure the same:

4. Click on **Cost analysis**:
  - a. You can see the graphical view of the cost analysis.
  - b. You can see the usage of each service, and region.
  - c. If you want to go deeper, click on each resource and you will get more details.
  - d. You can export the data in CSV or Excel file for your reference or telly purpose.

Figure 4.13 displays a sample report:

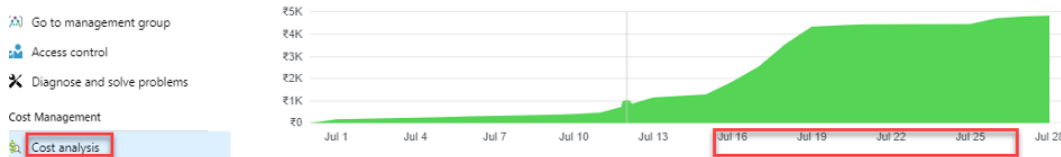


Figure 4.13: Cost management graphical view

Figure 4.14 displays a sample report which is shown in cost view models:

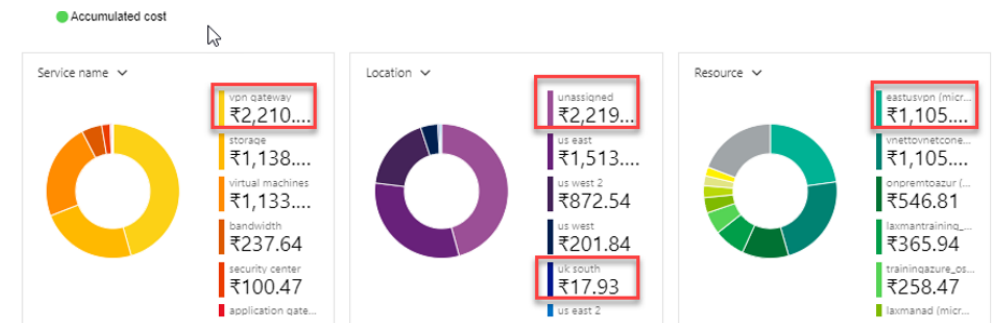


Figure 4.14: Cost management- cost separation into services

## Configuration of the budget alerts

The configuration of the budget alerts will help you get the alerts when your subscription cost gets utilized beyond the limit, and you can set an account spending limits as well. Perform the following steps to configure the budget alerts:

1. Click on the **Budgets** option in the left pane.
2. Once you click on the budget, you will get a window to provide the information.
3. Provide the alert name or budget name.
4. Reset the period month/years/weeks.
5. Provide the start date and end date of your budget.
6. Provide the number of your budget.
7. Once this is done, click on the **Next** button to create the alert.
8. Click on **Alert conditions** and set the alert % number based on your budget. Let us say your total budget is 5K. Once you have spent up to 60% (3000 INR), you will get an alert. You can change this setting as well.
9. Provide the email ID of your users or IT team to get the budget alert.
10. Click on **Create** and your alert will be created soon.
11. Perform the following steps, as shown in *Figure 4.15*:

The screenshot shows the 'Create a budget' page in the Azure portal. The left-hand navigation pane has a red box around the 'Budgets' link, labeled with a yellow circle containing the number 1. The main content area is titled '1 Create a budget' and '2 Set alerts'. It includes a 'BUDGET SCOPING' section with a 'Scope' dropdown set to 'lailit01rawatgmail (Default Directory) (root)'. Below this is the 'BUDGET DETAILS' section, which contains several fields: 'Name' (labeled 2), 'Reset period' (labeled 3 and set to 'Monthly'), 'Start date' (labeled 4, set to 2019, August, 1), and 'Expiration date' (labeled 5, set to 2021, July, 31). At the bottom is the 'BUDGET AMOUNT' section with an 'Amount' field (labeled 6) set to 0. The page also includes a search bar at the top and a list of navigation links on the left.

*Figure 4.15: Alerts creation*

12. Add the conditions as shown in *Figure 4.16*:

✓ Create a budget    ✓ Set alerts

Configure alert conditions and send email notifications based on your spend.

| Alert conditions |        |
|------------------|--------|
| % OF BUDGET      | AMOUNT |
| 60 ✓             | 3000   |
| Enter %          | -      |

1

| Alert recipients (email) |   |
|--------------------------|---|
| ALERT RECIPIENTS (EMAIL) |   |
| lrawat1@outlook.com      | ✓ |
| example@email.com        |   |

2

Previous    Create

*Figure 4.16: Alert condition*

## Azure subscription policy

The Azure subscription policy or Azure policy is used to achieve the compliance of your organization. It helps control the Azure environments as per the organization's compliance prospects.

You can create, manage, modify, and assign the policy, based on your organization standards. It will also help identify the non-compliance resources in the subscription.

- Let us assume that your organization needs to deploy a specific **Virtual Machine (VM)** instance size (VM size) in your subscription, and you want to disallow the rest of them. You can achieve this using the subscription policy.
- The second example would be probable if your company resides in Asia or the USA. Users can firstly create the resources in the specific region and then you can choose the allow location policy and allow only specific locations. All the other locations can be denied automatically. The allow location policy will help health care, financial, government services, and so on, to achieve compliance specific to the location.

## Azure policy creation, configuration, and assignment

In this section, we will learn how to implement and manage the policy. For the Azure policy configuration, follow the given steps:

1. Login to Azure portal (<https://portal.azure.com>).
2. Click on search on the left-hand side of the page in the **FAVORITES** section. Then, select the **Subscriptions** option.
3. In the **Subscriptions** section, click on the settings and select policies. Follow the steps as shown in Figure 4.17:

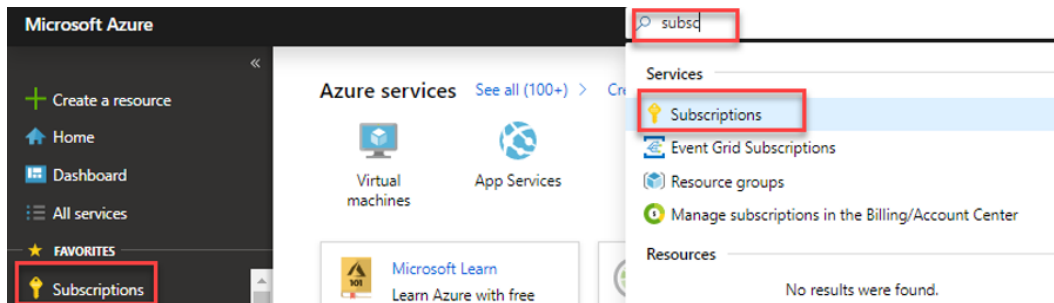


Figure 4.17: Select subscription

4. When you click on the **Policies**, you will be able to see the assigned policy in your subscription.
5. As you can see, in our example, we have applied a couple of policies in the subscription. You can also see the compliance level of the subscription. Follow the steps, as shown in Figure 4.18:

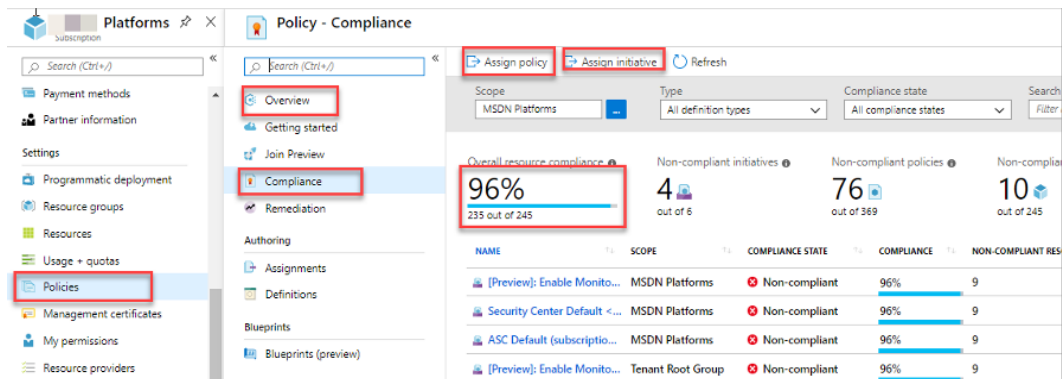


Figure 4.18: Azure policy



6. If you want to create the new policy, click on **Assigned policy**.
7. It redirects you to a new screen where new policies can be made.
8. You can provide the following values in your Azure policy. The policy will be created for a specific region:
  - a. **Scope:** Provide the subscription as shown in *Figure 4.19*:

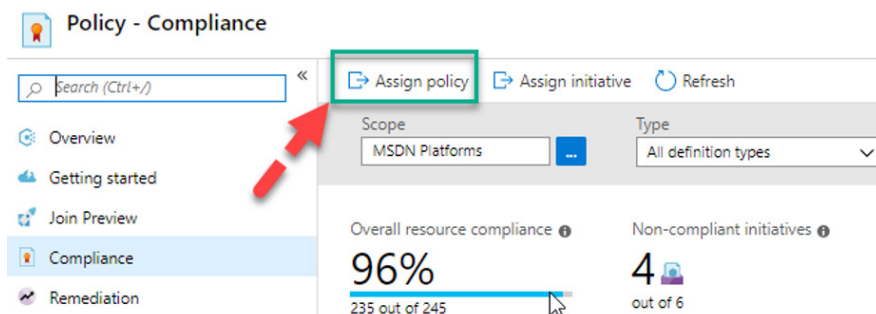


Figure 4.19: Policy compliance

- b. **Exclusions:** This option can be used if you want to exclude the resources from the policy. However, if you want to apply to the entire subscription, then do not select any resources in the exclusion policy.
- c. **Policy definition:** Policy definition will help you choose the defined policy from the policy gallery to control your resources. Follow the steps, as shown in *Figure 4.20*:

Assign policy

---

SCOPE

Scope (Learn more about setting the scope)  
MSDN Platforms

Exclusions  
Optionally select resources to exempt from the policy assignment

BASICS

\* Policy definition

\* Assignment name

Description

Assigned by  
Lalit Rawat

Figure 4.20: Policy assignments

- d. If you are planning to have the resources in a specific location, click on the **Allowed locations** policy.
- e. If you want to allow a specific **Stock Keeping Unit (SKU)**, then you can achieve this by using the Azure policy.
- f. Take a look at the following specific policy. You can search and apply the policy based on your organization's standard policy. Refer to *Figure 4.21*:

Type: All types Search: allowed

Policy Definitions (9)

**Not allowed resource types**  
Built-in  
This policy enables you to specify the resource types that your organization cannot deploy.

**Allowed storage account SKUs**  
Built-in  
This policy enables you to specify a set of storage account SKUs that your organization can deploy.

**Allowed resource types**  
Built-in  
This policy enables you to specify the resource types that your organization can deploy. Only resource types that support 'tags' and 'location' will be affected by this policy. To restrict all resources please duplicate this policy and change the 'mode' to 'All'.

**Allowed virtual machine SKUs**  
Built-in  
This policy enables you to specify a set of virtual machine SKUs that your organization can deploy.

**Allowed locations**

*Figure 4.21: Azure policy type*

9. Once you select the policy allowed location, choose the location you want to allow, such as **East US**, **Central India**, and so on.
10. Choose the **Assigned by** option.
11. Click on the **Assign** button.
12. Once done, you will be able to assign the policy successfully. Follow the instructions, as shown in *Figure 4.22*:

The screenshot shows the Azure Policy configuration page with the following sections and callouts:

- SCOPE**
  - 1. **\* Scope** (Learn more about setting the scope): MSDN Platforms
  - 2. **Exclusions**: Optionally select resources to exempt from the policy assignment
- BASICS**
  - 3. **Policy definition**: Allowed locations
  - 4. **\* Assignment name**: Allowed locations
  - 5. **Allowed locations** (dropdown menu):
    - ☐ Australia Central
    - ☐ Canada Central
    - ☐ Canada East
    - ☒ Central India
    - ☒ Central US
    - ☒ East Asia
    - ☒ East US
  - 6. **Description**: Allowed Location
  - 7. **Assigned by**: Lalit Rawat
  - 7. **\* Allowed locations**: 4 selected
- MANAGED IDENTITY**
  - Policies with effect type `deployIfNotExist` need the ability to deploy resources. To do this, a managed identity will be created to deploy the resources for you. [Learn more about Managed Identity.](#)
  - ☐ Create a Managed Identity
  - 8. **\* Managed Identity location**: East US
- Buttons**
  - Assign
  - Cancel

Figure 4.22: Azure policy configuration

Once all these steps are followed, the policy will be successfully implemented.

## Azure quota

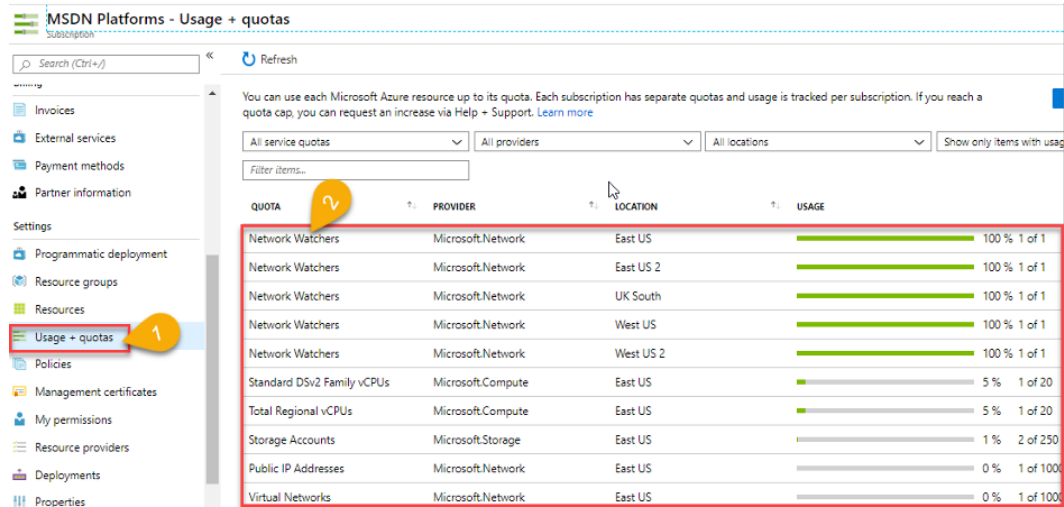
An Azure quota is nothing but the limitation of a specific subscription, of how many resources can be deployed. Generally, a quota is of two types:

- **Soft limit:** Default resources available in the subscription can be increased by raising the request with the MS team.

- **Hard limit:** Maximum resources can be deployed within the subscription, and even raising the request with the MS team cannot be increased.

If you want to see the usage limit and quota of your subscription, then click on the subscription. In the **Settings** section, click on **Usage + quotas**, and you will be able to view the available services in your subscription and see the quota as well.

You can see the details of the subscription limitation in *Figure 4.23*:



*Figure 4.23: Usage and quota limitation*

## Resource tag

We can use the Azure resource tag to add the extra fields, to identify the resources and it can be used for billing purposes. Every tag contains the following fields:

- **Name:** Production Application
- **Owner:** Lalit Rawat
- **Department:** IT
- **Bill to:** IT

**Note:** The preceding resource tags are just examples that can be changed based on your organization's policy. Based on that, you can define the tags and associate specific resources.

## Usage of the Resource Tag

Let us consider that you are a big organization that has deployed 4,000 applications. In this scenario, *how can you understand which resources group belongs to which app, and who is the owner? Who to bill the usage of services which is presented in the resources group?*

Hence, resource group tags can be used to identify the billing purpose. They are very helpful in the long term for a structured organization. Perform the following steps:

1. Click on **Resource groups**.
2. Under the **Overview** tab, click on the **Tags** option.
3. Provide the resource name, application, owner, database, and so on.
4. Then, provide the values, where values are your application name like Tomcat, Apache, SQLDB, and so on.
5. Click on **Save**, as shown in Figure 4.24:

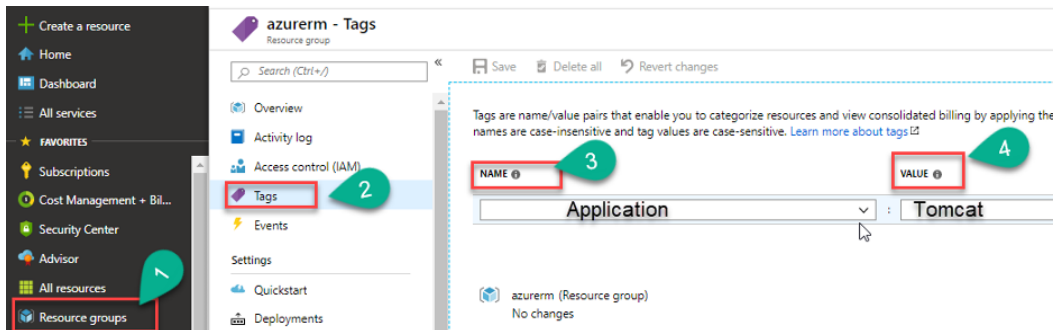


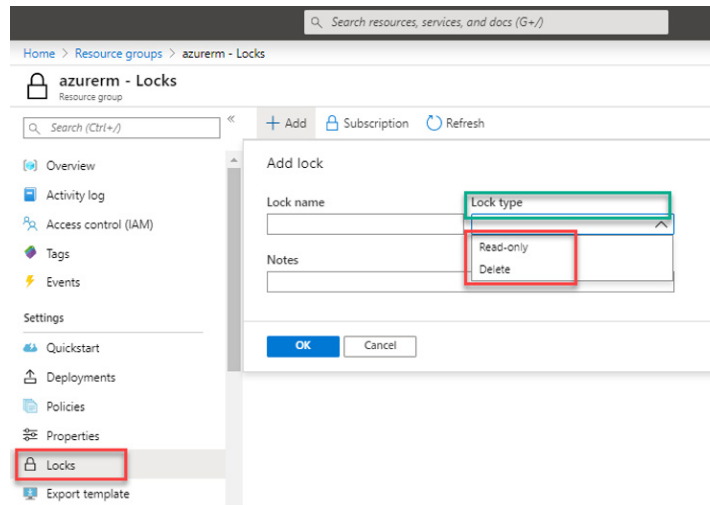
Figure 4.24: Resources tag

## Configuration of a resource lock

The resource lock helps with accidental deletion of resources. Administrators can lock the resources to prevent others from deleting the resources. In the subscription, there are two types of locks:

- **Delete:** This lock prevents users from deleting the resource. However, users can still read and modify the resource.
- **Read-only:** This lock provides access to read-only resources. In this case, users cannot modify or change the resources. However, they can still see the resources.

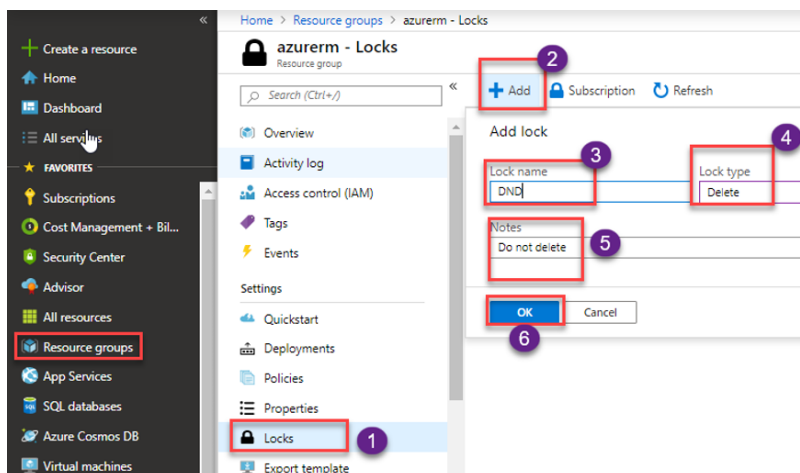
Take a look at *Figure 4.25*:



*Figure 4.25: Resources lock*

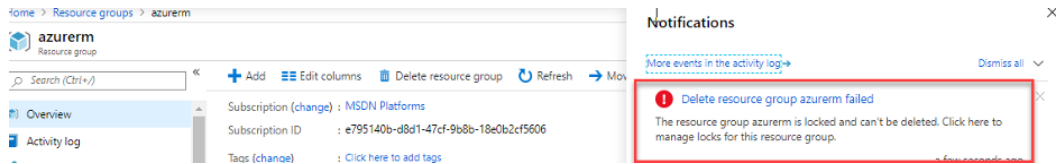
If you want to apply a lock on your resource group, follow the given steps:

1. Log in to the Azure portal by opening <https://portal.azure.com>.
2. Select **Resource groups**.
3. Under the resources group, click on **Locks**.
4. Create a lock.
5. After the lock creation, you can deploy the lock-in resource group successfully.
6. Perform the following steps, as shown in *Figure 4.26*:



*Figure 4.26: Resources lock creation*

7. If you try to delete the resources, you will get a message, as shown in *Figure 4.27*:



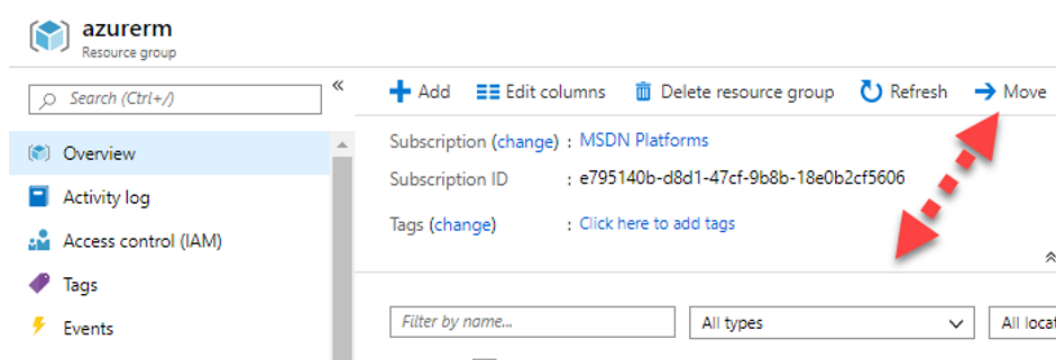
*Figure 4.27: Resources lock*

## Resources movement from one resource group to another

If you are planning to move the resource group resource (VMs and so on) to another resource group, then this can be done easily. You can also migrate the resources between subscriptions under the same tenant, and this can be done using the portal.

If you want to move the resources, perform the following steps:

1. Click on the resources group in which you want to move the resources.
2. Select the **Move** button at the top-right corner of the screen, as shown in *Figure 4.28*:



*Figure 4.28: Resources move*

3. Select the resources you want to move from one resources group to another, and click on **OK**.
4. It will take 20 to 45 minutes to complete the task, based on the size of the resource.

- Follow the given steps, as shown in *Figure 4.29*, and click on **Move** to move to the new resources group:

**Move resources**

Resources to move

☒ SELECT ALL

|                                                                                            | TYPE                                     |
|--------------------------------------------------------------------------------------------|------------------------------------------|
| <input checked="" type="checkbox"/> azuretraining_OsDisk_1_485b81129fa444c88b03a7a...      | Disk                                     |
| <input checked="" type="checkbox"/> piyushtra                                              | Disk                                     |
| <input checked="" type="checkbox"/> azuretraining                                          | Virtual machine                          |
| <input checked="" type="checkbox"/> azuretraining/AzureNetworkWatcherExtension             | microsoft.compute/virtualmachines/ext... |
| <input checked="" type="checkbox"/> azuretraining/DependencyAgentWindows                   | microsoft.compute/virtualmachines/ext... |
| <input checked="" type="checkbox"/> azuretraining/Microsoft.Insights.VMDiagnosticsSetti... | microsoft.compute/virtualmachines/ext... |
| <input checked="" type="checkbox"/> azuretraining/MicrosoftMonitoringAgent                 | microsoft.compute/virtualmachines/ext... |
| <input checked="" type="checkbox"/> shutdown-computevm-azuretrainingo                      | microsoft.deployment/scheduler           |

Move these resources to

Resource group

NetworkWatcherRG

☒ I understand that tools and scripts associated with moved resources will not work until I update them to use r

OK

*Figure 4.29: Resources selection to move*

- When you click on your resources, the resources will be migrated to a new resources group.

## Removing a resource group

A resource group can be removed by clicking on the delete resource group. This can be done through the Azure portal, CLI, PowerShell, and so on. Take a look at *Figure 4.30*:



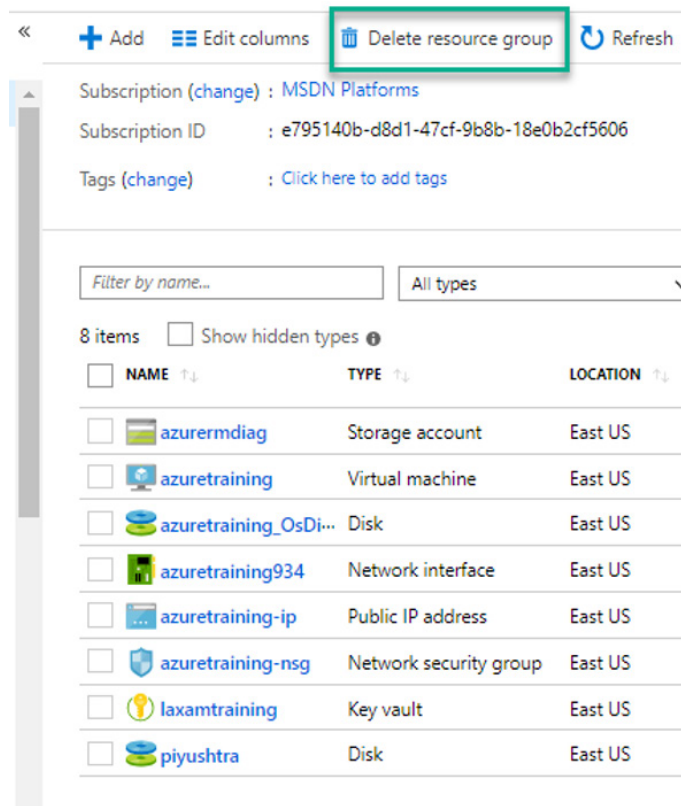


Figure 4.30: Resource group deletion

Perform the following steps:

1. Click on the delete resources group.
2. Provide the resource group name.
3. Once you provide the resources group name, click on the **Delete** button.
4. Once done, the resources will be deleted automatically.

Take a look at *Figure 4.31* for more details:

**Are you sure you want to delete "azurerm"?**

Warning! Deleting the "azurerm" resource group is irreversible. The action you're about to take can't be undone. Going further will delete this resource group and all the resources in it permanently.

TYPE THE RESOURCE GROUP NAME:  
azurerm

**AFFECTED RESOURCES**  
There are 13 resources in this resource group that will be deleted.

| NAME                                | TYPE                  | LOCATION |
|-------------------------------------|-----------------------|----------|
| azurermdiag                         | Storage account       | East US  |
| azuretraining                       | Virtual machine       | East US  |
| AzureNetworkWatcherExtension (...)  | Microsoft.Compute/... | East US  |
| DependencyAgentWindows (azur...     | Microsoft.Compute/... | East US  |
| Microsoft.Insights.VMDiagnostics... | Microsoft.Compute/... | East US  |
| MicrosoftMonitoringAgent (azure...  | Microsoft.Compute/... | East US  |
| azuretraining_OsDisk_1_485b811...   | Disk                  | East US  |
| azuretraining934                    | Network interface     | East US  |
| azuretraining-ip                    | Public IP address     | East US  |

**Delete** **Cancel**

*Figure 4.31: Resource group deletion confirmation*

## Creating and configuring management groups

The management group will help you manage multiple subscriptions in a single tenant. We can efficiently manage the access, policies, and compliance for these subscriptions.

A single policy can also be applied within the tenant group. The first management group will act as a tenant, and the policy that applies on this subscription will be inherited to other subscriptions as well.

If you want to create and configure the management group, follow the given steps:

1. Click on **All services**.

2. Type **management** in the search box.
3. Click on the **Management groups** option, as shown in Figure 4.32:

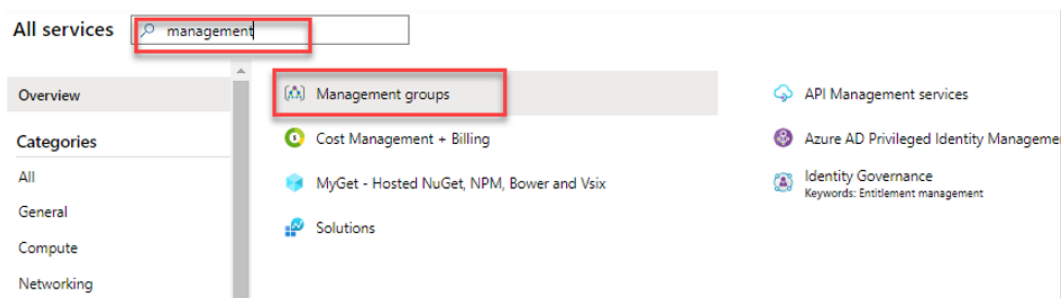


Figure 4.32: Management group

4. Once you click on the management group:
  - a. Click on **Create new**.
  - b. In **Management group ID (Cannot be updated after creation) \***, provide the name.
  - c. Provide the management group display name.
  - d. Click on **Save**, as shown in Figure 4.33:

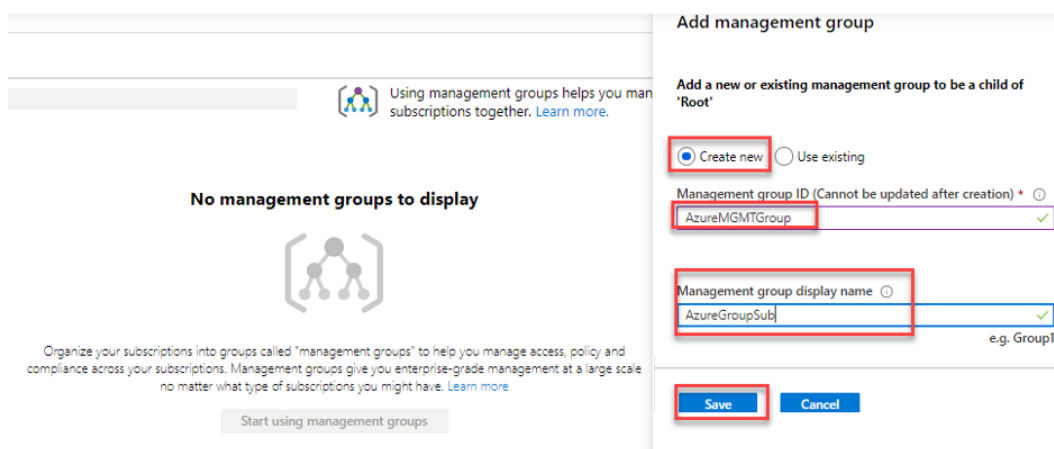
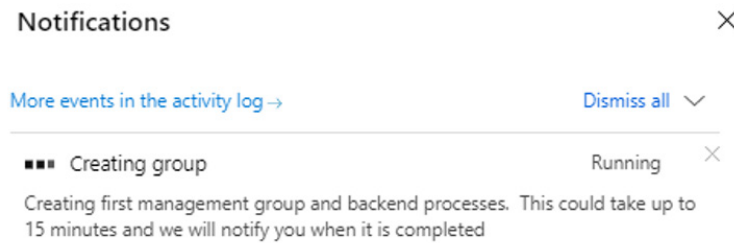


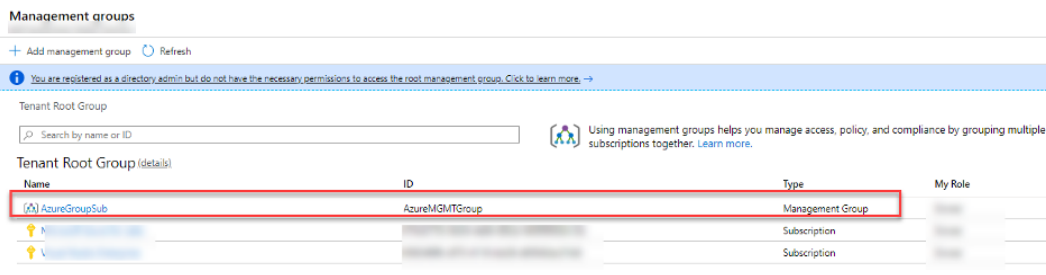
Figure 4.33: Management group creation

5. Once you click on **Save**, it will start creating the first management group, which might take up to 15 minutes. Refer to *Figure 4.34*:



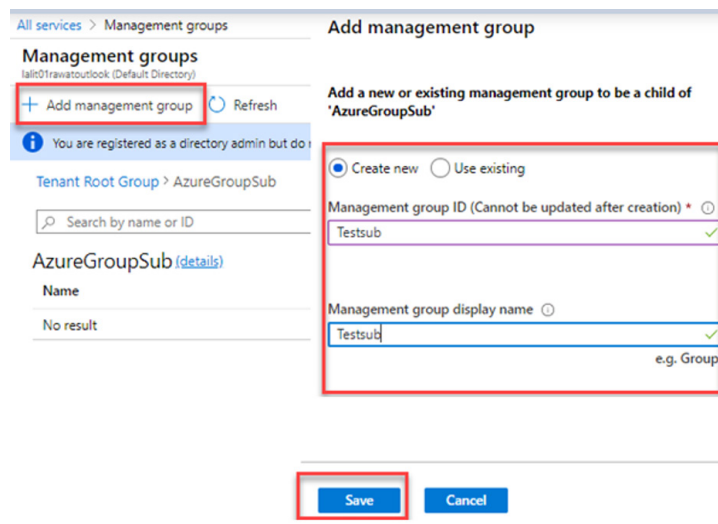
*Figure 4.34: Group creation*

6. Once the management group is created, you will see the following screen, as shown in *Figure 4.35*:



*Figure 4.35: Management group view*

7. If you want to create another management group, then click on the + **Add management group** and create another group, as shown in *Figure 4.36*:



*Figure 4.36: Add management group*

- Once the management group is created, you need to assign the subscription to the management group. This ensures that when you apply the policy, it should be inherited to the subscription associated with the management group. You can configure it, as shown in Figure 4.37.

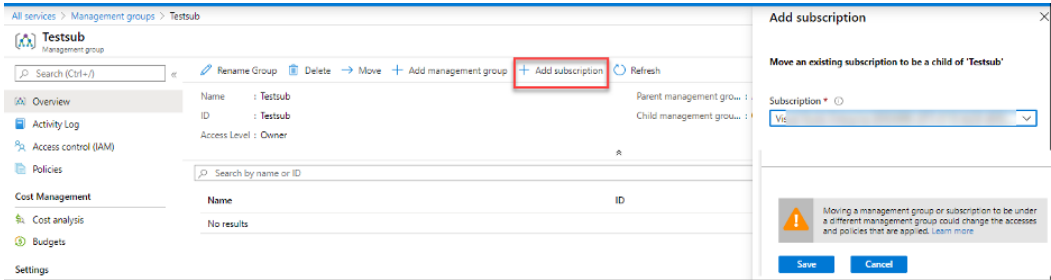


Figure 4.37: Add subscription to the management group

- We will complete this step to configure the management group and associate it with the subscription.

## Conclusion

In this chapter, we learned how to create the free Azure subscription, subscription management, and how to assign the policy. If you want to allow the resources from the Azure policy, configure the Azure resources group tags and implement the resource lock. We also covered the types of subscriptions. In the next chapter, we will cover how to monitor resources in Azure subscription.

In the next chapter, we will also learn about the management and configuration of Azure storage and its types, storage account replication, and so on.

## Points to remember

- Enterprise Agreement Subscription helps to manage your department billing and manage the hundreds of subscriptions centrally.
- Global Administrator Permission will help you manage your tenant (Azure AD).
- Cost Management will help customer to manage the cost of the subscription.
- Using Azure Subscription Policy, you can enable the security and governance within your subscription.
- Azure Quota will help to manage the available resources within your subscription, and you can raise a request for additional quota based on your resource's consumption.

- Creating and configuring management group will enable the organizational structure to manage multiple subscription.

## Multiple choice questions

- 1. The customer wants to allow only a few locations, based on his presence in the Azure subscription. How can you do that?**
  - a. Azure Policy.
  - b. Resources Group.
  - c. RBAC Access.
- 2. Your company wants to buy a subscription directly from MS. Which subscription would you choose?**
  - a. Free subscription.
  - b. Enterprise Subscription.
  - c. CSP Subscription.
- 3. What is a subscription in Microsoft Azure?**
  - a. It is the Billing Container which contains the Azure services.
  - b. It is just a Container.
  - c. It is an Azure cloud services provider.

## Answers

1. a
2. b
3. a

# CHAPTER 5

# Managing and Configuring of Azure Storage Accounts

## Introduction

In this chapter, we will cover how to manage and configure the Azure storage account. You will learn about different types of Azure storage accounts, the use of storage accounts, and creation and configuration of Azure storage accounts, which will further help you understand how the storage accounts work in Azure. We will explain how to secure your storage account using the Azure firewall configuration and integrate it with a virtual network. We will cover more about replication, how this replication will work, and how your data can be synced to a different region.

## Structure

The following topics will be covered in this chapter:

- Azure storage account
  - Types of Azure storage accounts
  - Azure storage account creation and configuration
- Implementing Azure Storage replication
- Generating and managing the shared access signature
- Managing storage account access key

- Configuring network access to the storage account
- Installation and configuration of the Storage Explorer

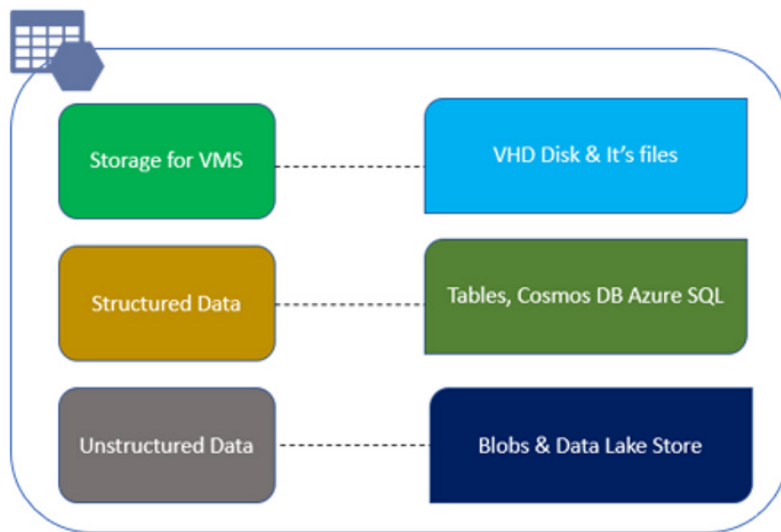
## Objectives

In this chapter, you will learn how to configure the storage account and how to store data in Azure. We will provide you with step-by-step instructions to create and configure the Azure storage account, connect to the Azure storage account using the Azure storage explorer, and to use the Azure storage key.

## Azure storage account

An Azure storage account is a cloud-based solution for storing structural and un-structural data.

It is also used to store the data disk of **virtual machines (VMs)**, files, and so on. It is available, durable, and secure. It can be accessed by HTTP/HTTPS from anywhere. You can take a look at *Figure 5.1* to understand about the storage account data structure:



*Figure 5.1: Azure storage account data*

- **Storage for VMs data:** This kind of data will be stored in a blob storage account under the page blob, which stores the Virtual Hard Disk (VHD) file of VMs.
- **Structured data:** It is a commonly used cosmos **database (DB)** tables, and so on, where the data will be stored structurally and can give the results easily.



- **Unstructured data:** Unstructured data can be used to store the data log file, image, movie or archival data, and so on, which are used to dump the data. This does give results faster, as this is not stored in a formatted or structural way.

## Types of Azure storage accounts

Azure storage accounts are of the following three types:

1. **Blob storage account:** Blob storage accounts are used for unstructured data, such as backup, JPEG, AVI files, and so on. A blob storage account offers three kinds of accounts: cool storage, hot storage, and **archive**.
  - **Access tiers:** Access tiers have the functionality to determine how frequently data can be accessed. It is based on these tiers that the storage account bill is charged:
    - o **Hot storage:** This type of storage account can be used when you need to access the data frequently, such as day-to-day operations.
    - o **Cool storage:** This type of storage account can be used for data that is infrequently accessed and stored for a minimum of 30 days. For example, if have an older backup or file you want to store to a storage account, you need to access it monthly once or twice.
    - o **Archive storage:** This type of storage account is used to store the data which has been accessed rarely and stored for at least 180 days, such as an older backup with more than 5 or 10-year compliance data.

Please refer to *Figure 5.2* for more details:

Account kind  BlobStorage 

Replication 

Access tier (default)  ☐ Cool ☒ Hot

The account Access Tier is the default tier that is inferred by any blob without an explicitly set tier. The **Hot Access Tier** is ideal for frequently accessed data, and the **Cool Access Tier** is ideal for infrequently accessed data. The **Archive Access Tier** can only be set at the blob level and not on the account. [Learn more about access tiers](#) 

*Figure 5.2: Azure blob storage account tier*

1. **General purpose V1:** GPv1 storage accounts are legacy accounts and they have been used for blobs (also referred to as a container), files queues, and tables. They are commonly used and support replications like LRS, GRS, and RA-GRS. Take a look at *Figure 5.3*:

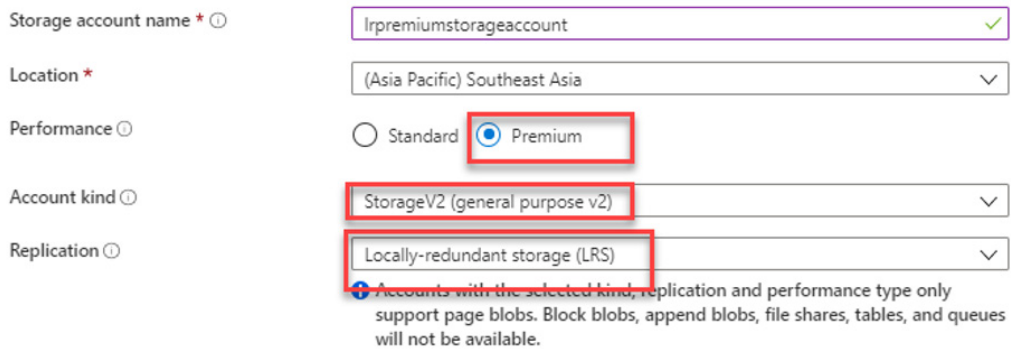
*Figure 5.3: Azure GPv1 account*

2. **General Purpose V2:** GPv2 storage accounts are recommended to be used, as they are the upgraded versions. They are used for blobs (or container), files queues, and tables. They support replication like LRS, GRS, RA-GRS, and ZRS. They also have the feature for cold/hot storage account, which you can get only in the blob storage account.

Recently, MS Azure has released new replications such as **GZRS-zone** redundant storage and **read-access geo-zone-redundant storage (RA-GZRS)**. They are in the preview feature. Refer to *Figure 5.4*:

*Figure 5.4: GPv2*

3. **Premium storage accounts:** Premium storage accounts use the SSD disk and provide high performance with low latency disk support. The premium storage account is mainly used for mission-critical applications or production environments. 1 TB disk provides the 7500 IOPS and 250 MB throughput for the disk. Take a look at *Figure 5.5*:



Storage account name \* ⓘ  ✓

Location \*  ▼

Performance ⓘ ☐ Standard ☒ Premium

Account kind ⓘ  ▼

Replication ⓘ  ▼

Accounts with the selected kind, replication and performance type only support page blobs. Block blobs, append blobs, file shares, tables, and queues will not be available.

Figure 5.5: Premium storage account

## Azure storage account creation and configuration

To create a storage account, follow these steps:

1. Please click on **Create a resource**.
2. Search for **Storage account**.
3. Click on the **Create** button to create a storage account, as shown in Figure 5.6:

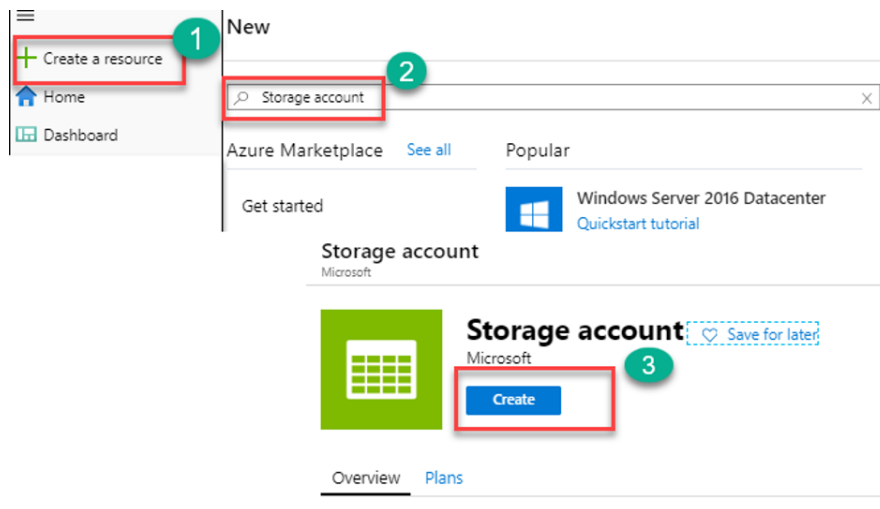


Figure 5.6: Storage account creation

4. Select the subscription for which you want to create the Azure storage account.

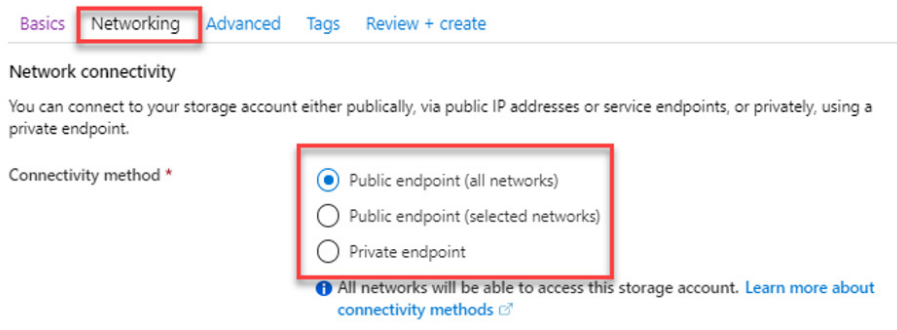
5. Create the new resources group or use an existing resources group from the drop-down menu.
6. Provide the Azure storage account name. This name should only be in lowercase and in numbers.
7. Select the region you want to deploy the storage account.
8. The performance type can be either Standard or Premium, as per customer requirements.
9. For the account kind, you can select: GPv1, GPv2, or blob storage account. In our case, we have selected GPv2, since it is the latest version.
10. For replication, you can select the default RA-GRS option, but based on the requirements, you can also choose from GRS, LRS, or ZRS (if available in your region).
11. Select the access tier: **Hot** or **Cool**. In our case, we have selected **Hot**.
12. Click on **Next: Networking** > for further configuration, as shown in *Figure 5.7*:

The screenshot shows the 'Basics' tab of the Azure Storage account configuration page. The page is divided into sections: 'Project details' and 'Instance details'. In the 'Project details' section, the 'Subscription' dropdown is set to 'Azure' (callout 1) and the 'Resource group' dropdown is set to '(New) azure4you' (callout 2), with a 'Create new' link below it. In the 'Instance details' section, the 'Storage account name' is 'lailitstorageaccount' (callout 3), the 'Location' is '(US) West US 2' (callout 4), the 'Performance' is 'Standard' (callout 4), the 'Account kind' is 'StorageV2 (general purpose v2)' (callout 5), the 'Replication' is 'Read-access geo-redundant storage (RA-GRS)' (callout 5), and the 'Access tier' is 'Hot' (callout 6). At the bottom, the 'Next: Networking >' button is highlighted with a green box and callout 7.

*Figure 5.7: Storage account configuration details*

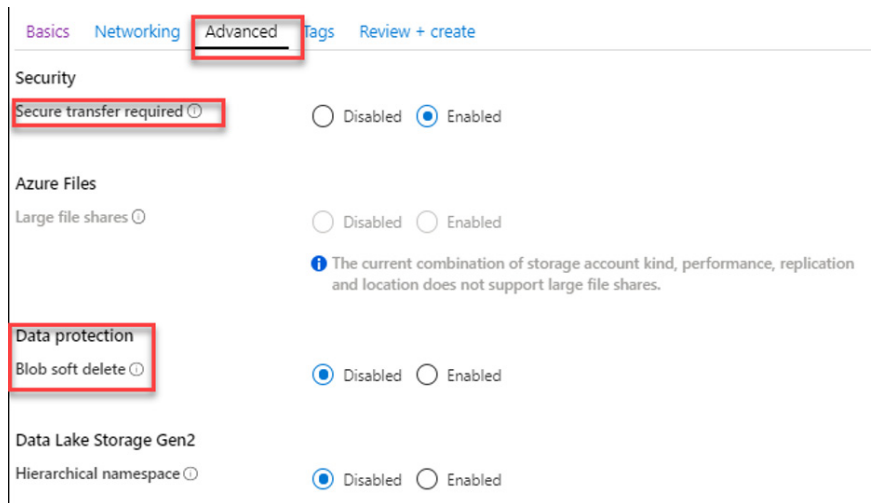
13. Based on the requirements, you can enable the following endpoints:

- **Public Endpoint (all networks):** Open to all networks.
- **Public Endpoint (selected networks):** For a selected network(s).
- **Private Endpoint:** Integrate the VNet and make it available for your network only, as shown in *Figure 5.8*:



*Figure 5.8: Storage account networking configuration*

- Click on the **Advanced** tab, and here, you can set the security options, such as **Secure transfer required** and **Data protection** settings, and so on. For more details, take a look at *Figure 5.9*.
- Also click on **Tags** and assign the tags for billing purposes.



*Figure 5.9: Storage account advance settings*

14. Once the validation is complete, you will see the green mark.

15. Please verify the details one more time and click on **Create** to create the account.
16. After that, the deployment will start and your storage account will be created within 5 to 10 minutes. Refer to *Figure 5.10*:

Validation passed

Basics Networking Advanced Tags Review + create

**Basics**

|                       |                                            |
|-----------------------|--------------------------------------------|
| Subscription          | Azure Pass - Sponsorship                   |
| Resource group        | (New) azure4you                            |
| Location              | (US) West US 2                             |
| Storage account name  | lalltstorageaccount                        |
| Deployment model      | Resource manager                           |
| Account kind          | StorageV2 (general purpose v2)             |
| Replication           | Read-access geo-redundant storage (RA-GRS) |
| Performance           | Standard                                   |
| Access tier (default) | Hot                                        |

**Networking**

|                     |                                |
|---------------------|--------------------------------|
| Connectivity method | Public endpoint (all networks) |
|---------------------|--------------------------------|

**Advanced**

|                          |          |
|--------------------------|----------|
| Secure transfer required | Enabled  |
| Hierarchical namespace   | Disabled |
| Blob soft delete         | Disabled |

Create < Previous Next >

*Figure 5.10: Storage account verification and creation*

In this session, we have understood the Azure storage account data type and its usage. We also studied how to create the storage account, and so on. Now, the reader will be able to understand and create the storage account.

## Implementing Azure storage replication

In Azure storage replication, we have replication policies as part of the storage account replication. It helps us to maintain the compliance part and secure the data.

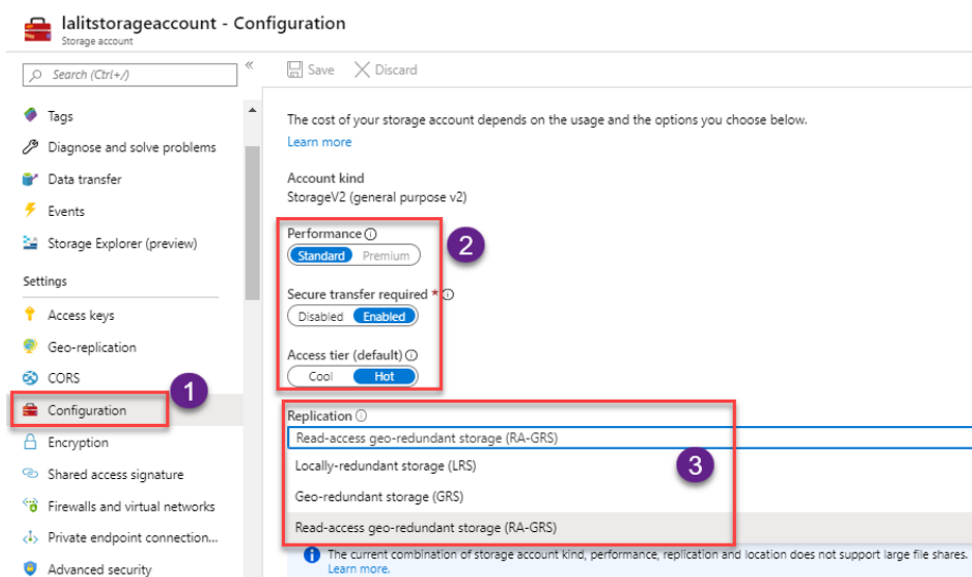
- **Locally Redundant Storage (LRS) account:** It maintains three copies of your data within a single datacenter in a single region. Its usage data can be

reconstructed, and it helps in your data compliance for regional governance requirements.

- **Zone Redundant Storage (ZRS):** It maintains three copies of your data within 2 or 3 datacenters in a single region or across the region. Data will be replicated across the three-storage clusters in a single region.
- **Geo Redundant Storage (GRS) account:** It maintains six copies of the data and data that has been replicated three times within the primary region and three times in the secondary region, 100 miles away from the primary region. Data will be available as read-only during a failure.
- **Read-only Geo-Redundant Storage (GRS) account:** It maintains six copies of the data and works in the same way as your GRS, but it provides the read access to your secondary region even without the failover.

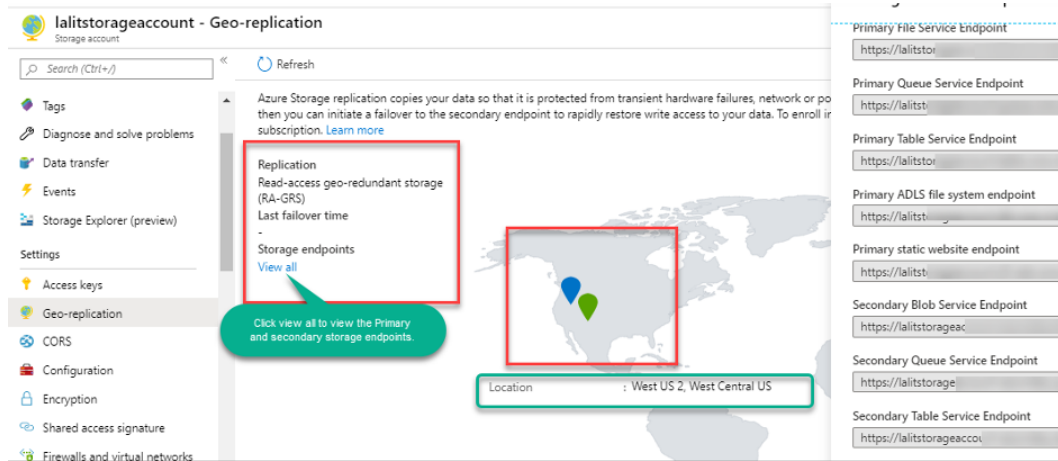
To implement or change the replication, follow these steps:

1. Select the Azure storage account.
2. Go to **Configuration**.
3. Select the appropriate replication from the **Replication** drop-down menu.
4. Click on **Change**. If you click on change, the changes might be applicable based on the replication you select.
5. Click on **Save**, as shown in *Figure 5.11*:



*Figure 5.11: Storage account replication*

6. Once you change the replication, click on **Geo-replication**.
7. In this section, you will be able to see the primary and secondary regions where your data has been copied. This can be seen in *Figure 5.12*:



*Figure 5.12: Storage account replication with a secondary endpoint*

## Generating and managing the shared access signature

A shared access signature will allow you to provide the restricted access to the storage account, if anyone requests to gain access to the storage account. You can provide access with time limitation, and after the set duration, the access will get expired. You can generate the **Statistical Analysis System (SAS)** access using your primary storage account key or secondary storage account key.

If you need to generate the SAS key, select the **Shared access signature** tab under **Settings** and follow these steps:

1. Please select the allowed services like **Blob, File, Table, or Queue**.
2. Select the allowed resource types like **Service, Container, or Object**.
3. Allow permission like **Read, Write**, and so on, based on the requirements.
4. You can select the specific IP and click allow protocol https.
5. Select the HTTP or HTTPS selection.
6. Click on the **Generate SAS and connection string** button.
7. After a few seconds, keys will be generated, and the user can access the key.



Refer to Figure 5.13:

Storage Explorer (preview)

Settings

- Access keys
- Geo-replication
- CORS
- Configuration
- Encryption
- Shared access signature**
- Firewalls and virtual networks
- Private endpoint connection...
- Advanced security
- Static website
- Properties
- Locks
- Export template

Blob service

- Containers
- Custom domain
- Soft delete

Learn more

Allowed services

☒ Blob ☒ File ☒ Queue ☒ Table

Allowed resource types

☒ Service ☒ Container ☒ Object

Allowed permissions

☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☒ Update ☒ Process

Start and expiry date/time

Start

12/09/2019 1:52:34 AM

End

12/20/2019 9:52:34 AM

(UTC+05:30) --- Current Time Zone ---

Allowed IP addresses

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols

☒ HTTPS only ☐ HTTPS and HTTP

Signing key

key1

Generate SAS and connection string

Figure 5.13: Generating shared access signature

## Managing storage account access key

The Azure storage account key is used to access the storage account from the storage explorer, or to access it publicly. It is just like a storage account password, which you can change any time by clicking on the **Refresh** button. Some features of it are as follows:

- You will have a primary and secondary key.
- While clicking on the **Refresh** button, you can generate the new key which is marked in a red circle, as shown in Figure 5.14:

- You can use the connection string to connect to the storage account.

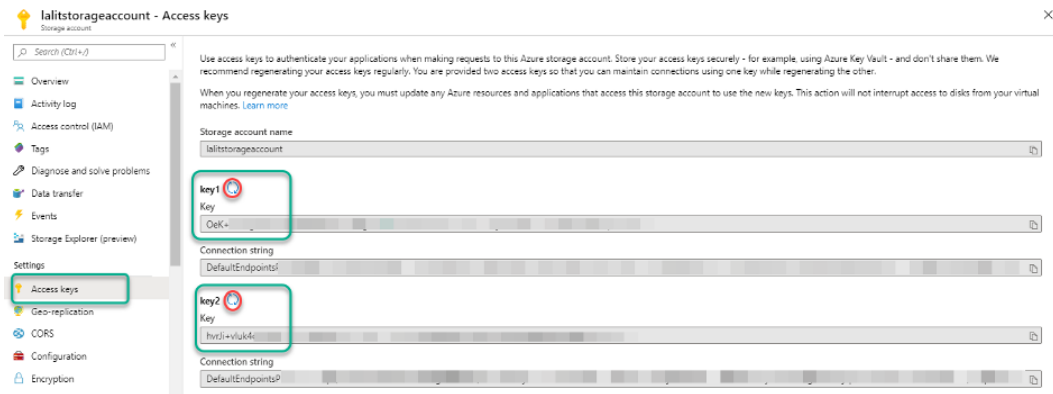


Figure 5.14: Managing the Azure storage account key

## Configuring network access to the storage account

Enabling the VNet access, the Azure storage account will provide an additional layer of security to your storage account that has your critical data. After integration, the storage account can be accessed within VNet, but not publicly, until the public endpoint or public IP is added.

1. Please select the storage account for which you want to enable the VNet.
2. Select **Firewalls and virtual networks** under **Settings**.
3. Select the network and click on the **Add new virtual network** option. You can also add the existing network, as shown in Figure 5.15:

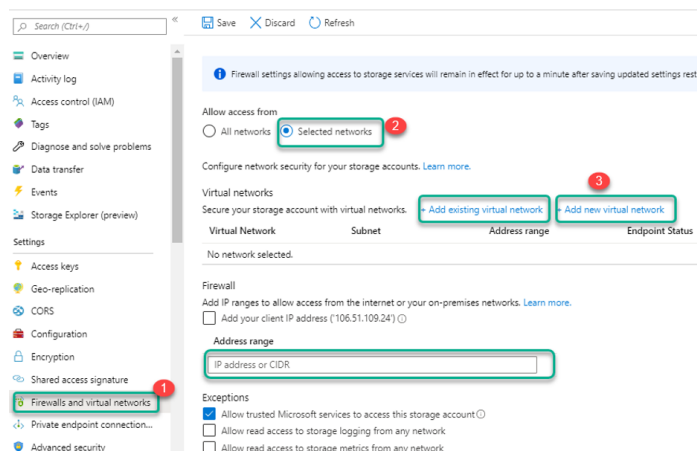


Figure 5.15: Azure Storage account network configuration

4. Select the existing Vnet or create a new Vnet.
5. Please provide the VNet name and range of IP.
6. Provide the resources group and region.
7. Provide the subnet name and range of IP.
8. Provide the location and click on **Create**. Please check out the details, as shown in *Figure 5.16*:

**Create virtual network** ✕

**Name \***  
BPBnetwork ✓

**Address space \*** ⓘ  
10.1.0.0/16  
10.1.0.0 - 10.1.255.255 (65536 addresses)

**Subscription \***  
Azure f ▼

**Resource group \***  
azure4you ▼  
[Create new](#)

**Location \***  
(US) West US 2 ▼

**Subnet**  
**Name \***  
default

**Address range \*** ⓘ  
10.1.0.0/24 ✓  
10.1.0.0 - 10.1.0.255 (256 addresses)

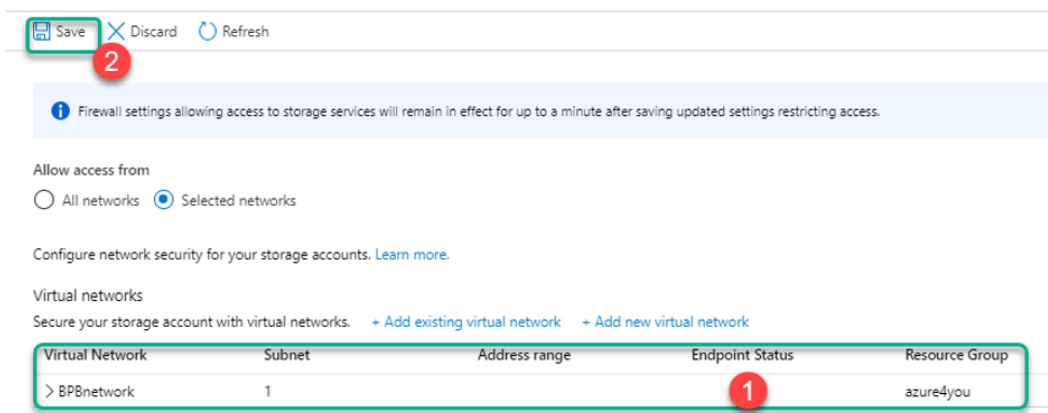
**DDoS protection** ⓘ  
☒ Basic ☐ Standard

**Service endpoint** ⓘ  
Microsoft.Storage

**Firewall** ⓘ  
☒ Disabled ☐ Enabled

*Figure 5.16: Azure storage account-VNet creation*

Once the Vnet is associated with a storage account, click on the **Save** button to save the configuration. Once this is done, you will be able to successfully configure the network with a storage account. Refer to *Figure 5.17*:



*Figure 5.17: Azure storage account VNet association*

## Installation and configuration of the storage explorer

The Azure storage explorer is an application that will help you to connect to storage accounts and move the data from an on-premises system to the Azure blob, file, queue, and table storage account.

You can easily upload, download, and manage Azure blobs, files, queues, tables storage account, Azure Cosmos DB, and Azure Data Lake Storage data. It is easy to manage and access from your system. You can access virtual machine disks from the ARM or classic storage accounts.

If you want to install the Azure storage explorer, then follow the given steps:

1. Go to <https://Azure.microsoft.com/en-in/features/storage-explorer/> to download the Azure storage explorer.
2. Select the OS (**Windows/Linux** or **MAC**) from the drop-down menu based on the requirements. Take a look at *Figure 5.18*:

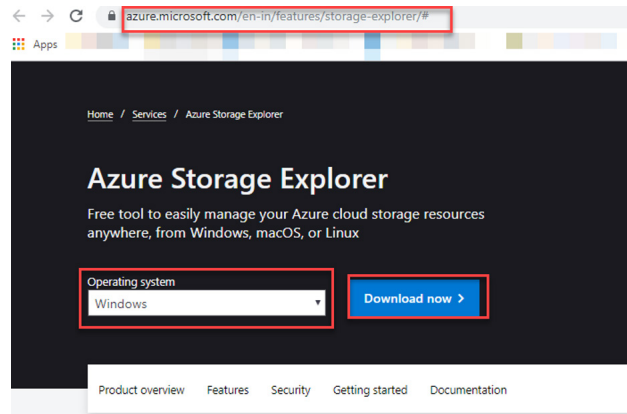


Figure 5.18: Azure storage explorer

3. Once you download the storage account file, double click on it and follow the instructions.
4. Once done, you will be able to successfully install the storage explorer.
5. Open the Azure Storage Explorer.
6. Click on the **User** icon.
7. Click on **Add an account...** as shown in Figure 5.19.
8. Log in with the Azure account, connection string or SAS URI, or any other option available.
9. Click on **Next**.

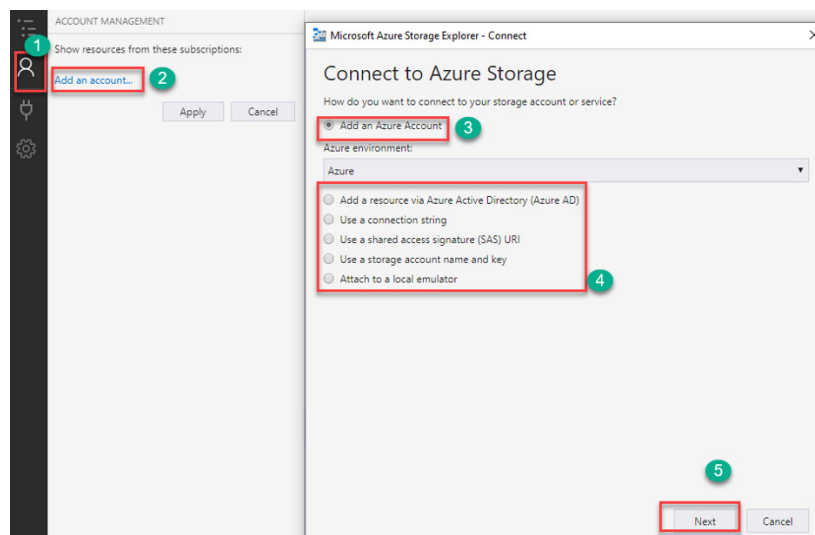
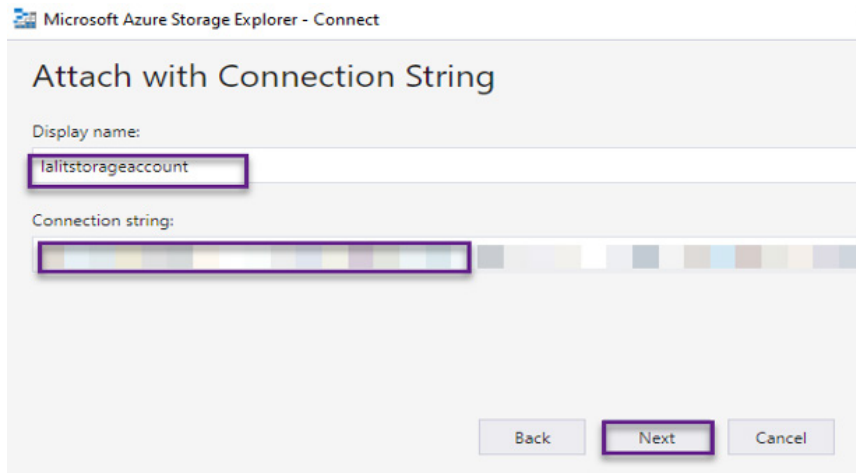


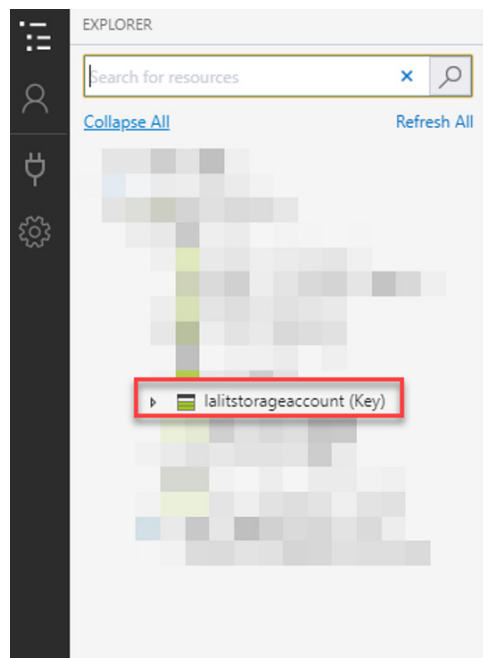
Figure 5.19: Azure storage explorer sign in

10. You can copy and paste the storage account strings, as shown in *Figure 5.20*.
11. For **Connection string**, please check the topic managed access key.
12. Once done, you will be able to log in successfully to the storage account.



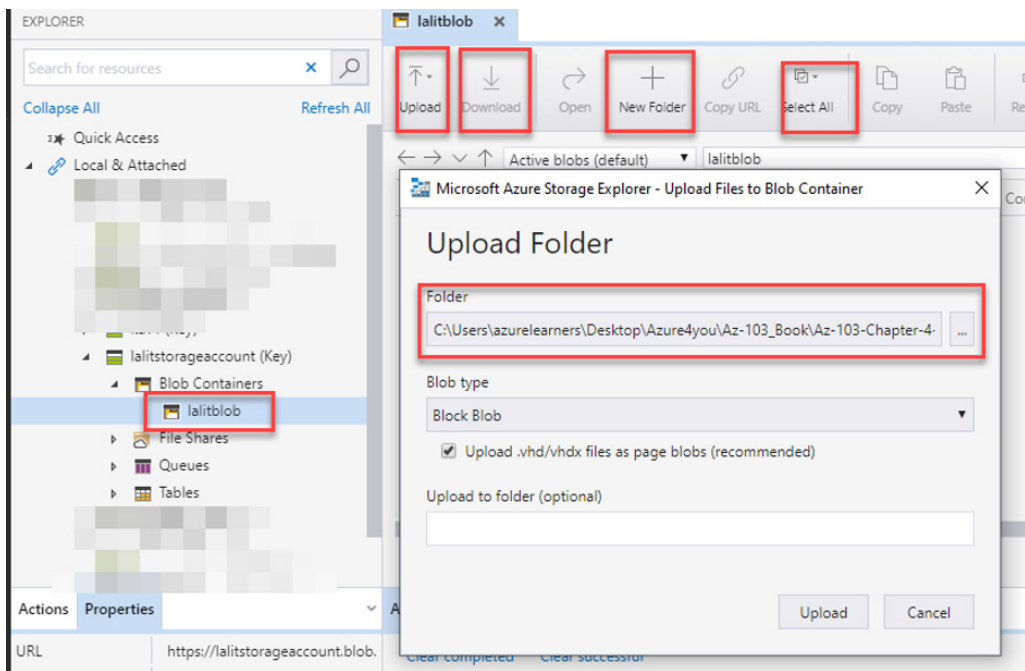
*Figure 5.20: Azure storage explorer login method*

Now, you will successfully be able to log in to the Azure storage explorer as shown in *Figure 5.21*:



*Figure 5.21: Azure storage in explorer*

13. You can upload the data to the Azure blob storage accounts, and also create a container.
14. You can upload the data using the **Upload** option.
15. You can download the data by clicking on the **Download** option.
16. Create a new folder if required.
17. You can select all the documents and update the necessary changes.
18. The same storage account can work for your file storage, and you can create the queue and table as well. For more details, refer to *Figure 5.22*:



*Figure 5.22: Azure storage in explorer usage*

## Conclusion

In this chapter, we covered the different types of storage accounts and how to use those storage accounts. We explained the replication policy and learned how it can help you in your compliance with the data or to replicate the data. We learned how to create the storage account and what are the GPv1 and GPv2 storage accounts. We covered the premium storage account and its usage.

In the next chapter, we will discuss how to import and export data and how to move the data using the Azure AzCopy command-line utility.

## Points to remember

- Storage account can be created as standard or premium storage account.
- Premium storage accounts have more performance than standard storage account.
- We can secure the access using the SAS key based authentication. It can allow specific IP addresses to access the storage account services.
- Using network and security section, we can enable vent integration and can configure the private endpoint.
- Azure storage explorer tool is used to uplod and download the files and folders to blob, azure files, and so on.
- Storage replication will replicate the data from primary region to secounday region. Storage account replication will change, based on the replication type LRS, GRS, RA-GRS, Z-GRS, and so on.

## Multiple choice questions

1. **Which storage account type will you create if client needs more IOPS and performance?**
  - a. Standard Storage account.
  - b. Premium Storage account.
  - c. File Storage account.
2. **How to configure the network access for storage account?**
  - a. Go to Setting and configure the network access.
  - b. Upgrade the storage account.
  - c. Go to network setting and click on Security and networking.
3. **How to generate the SAS access key ?**
  - a. Under the security settings, click on access key.
  - b. It is just a Container.
  - c. Under the security settings, click on Shared access signature.

## Answers

1. b
2. c
3. c



# CHAPTER 6

# Manage Data in Azure Storage

## Introduction

In this chapter, we will discuss how to migrate large data to the Azure storage account using the Azure import and export services. We will also discuss the Azure Data Box and configuration of Azure AD authentication, for the storage account usage. We will cover how to use the **Azcopy** command, which will help you move the data from on-premises to the Azure storage account. You can also learn how to configure the blob object replication in a step by step manner. We have covered all of those steps in details.

## Structure

The following topics will be covered in this chapter:

- Import and export jobs in Azure
  - Configuring Azure Blob Storage
  - Creating import and export jobs in Azure Storage
- Azure Data Box
  - Configuring Azure AD Authentication for a Storage Account
  - Copy data using **Azcopy**

- Configure Blob Object Replication

## Objectives

The objectives of this chapter are to explain how to migrate the petabytes of the data, using the Azure export/import utility and Azure Data Box solutions, and how to transfer the data to a blob storage account using the **AzCopy** command-line utility.

## Import and export jobs in Azure

We can create the import and export jobs using the Azure storage account, which requires a blob storage account. The blob storage account is where we can keep the data. Import and export jobs can be used to send large data to Azure Blobs; for example, terabytes or petabytes of data.

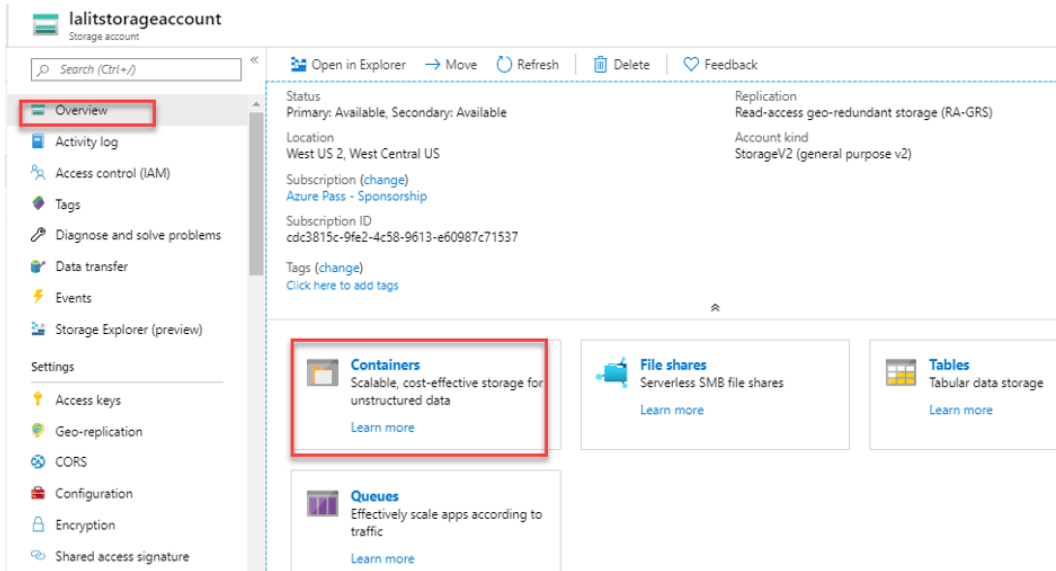
If you require a data disk to copy the data and configure the services, then the data will need to be shipped to Microsoft. Microsoft will copy the data to Azure Blob as per the customer's request. The data will then be encrypted end to end using BitLocker, during the configuration of import and export jobs.

## Configuring Azure Blob Storage

In *Chapter 5, Managing and Configuration of Storage Accounts*, we explained about the blob and its usage. If you want to create the blob (container) under the storage account, follow these steps and refer to *Figure 6.1*:

1. Log in to the portal.
2. Select the storage account for which you want to create the blob storage (container).
3. Click on **Containers**.

**Note:** The blob storage name has been changed recently to container due to new modifications made by Microsoft Azure. However, the usage is the same.



*Figure 6.1: Blob creation in the storage account*

4. Click on the **Container** button.
5. Provide the name of the container.
6. For **Public access level**, select any one of the following options, based on the requirements:
  - **Private (no anonymous access)**
  - **Blob (anonymous read access for blobs only)**
  - **Container (anonymous read access for containers and blobs)**

Figure 6.2 shows the container creation:

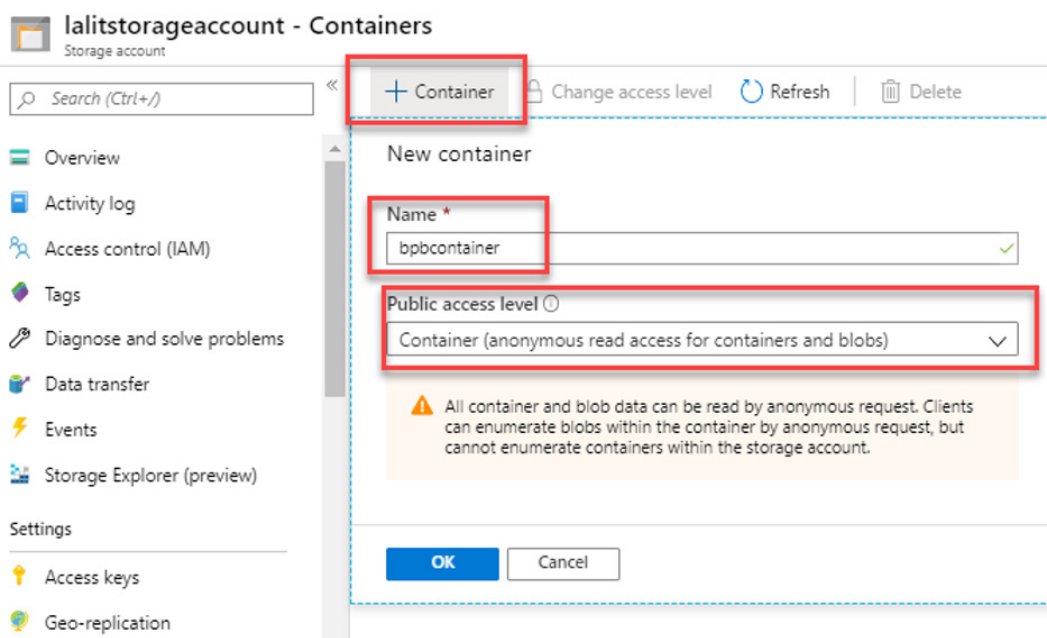


Figure 6.2: Container creation

- Once your container is created, you will be ready to configure the import and export jobs. You can also upload the data directly. Take a look at the container configuration as shown in Figure 6.3:

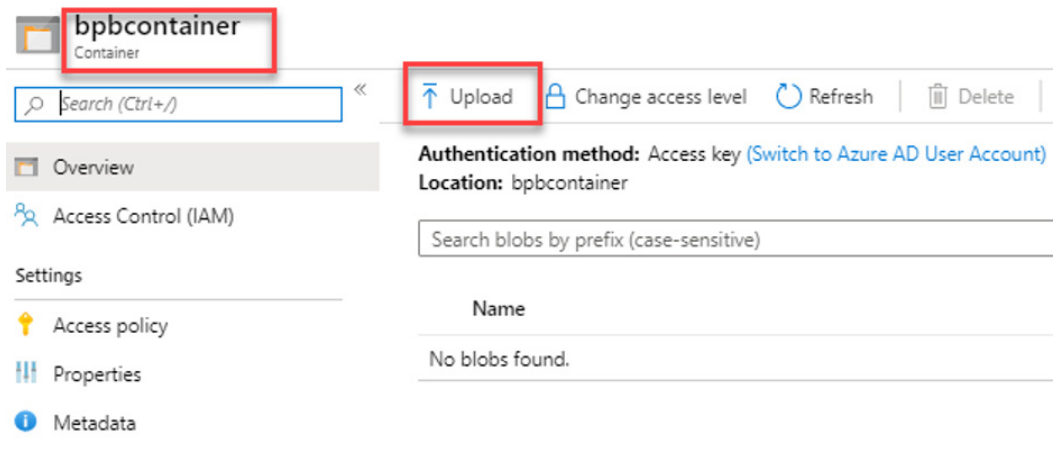


Figure 6.3: Container configuration

## Creating import and export job in Azure Storage

If you want to create an import job, follow the given steps:

1. Login to subscription.
2. Go to **All services** and search for **Import/export jobs**.

Refer to Figure 6.4:

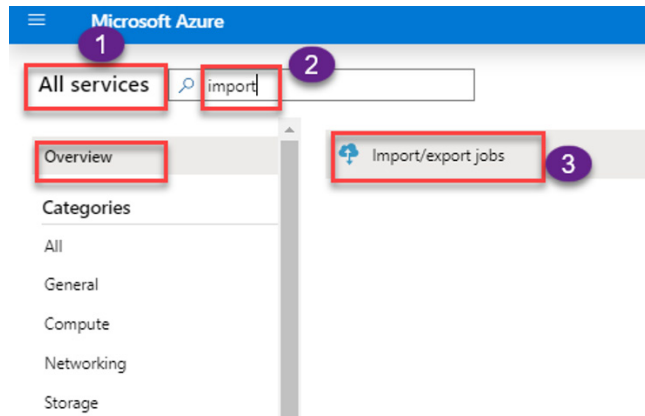


Figure 6.4: Import and export search

3. Once this is done, you can provide the basic configuration setting.
4. Select the **Import into Azure** option.
5. Provide the subscription and resource group name, as shown in Figure 6.5:

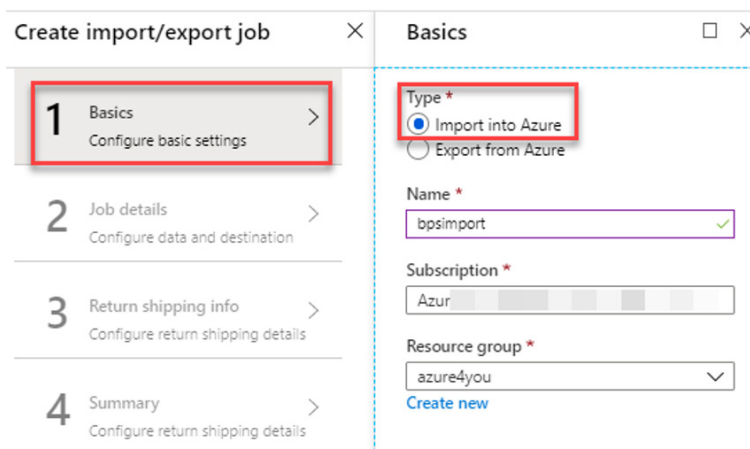


Figure 6.5: Import basic configuration

6. Click on **Job details**.
7. Download and install the **WAImportExport** tool to generate the **.jrn** file.
8. Now, you can upload the JRN or XML file.
9. Once it is uploaded, select the storage account. The location will be the default.
10. Click on the **OK** button and provide the return shipping information and configure the return shipping details.
11. Click on **OK** and your import jobs will be created.

Take a look at *Figure 6.6*:

The screenshot displays the 'Create import/export job' wizard, specifically the 'Job details' step. The sidebar on the left shows four steps: 1. Basics (Configure basic settings), 2. Job details (Configure data and destination), 3. Return shipping info (Configure return shipping details), and 4. Summary (Configure return shipping details). The main panel contains the following elements:

- Step 1:** Basics (Configure basic settings) - marked with a green checkmark.
- Step 2:** Job details (Configure data and destination) - highlighted with a red box and a purple circle 1.
- Warning:** Download the latest WAImportExport tool to generate the .jrn file - marked with a purple circle 2.
- Data source:** Upload journal files - marked with a purple circle 3. The input field contains "bpbjrn.xml".
- Drive ID:** Journal file - No files uploaded.
- Import destination:** Storage account - marked with a purple circle 4. The dropdown shows "lalitstorageaccount".
- Drop-off location:** - marked with a purple circle 5. The dropdown shows "West US 2".
- Checkbox:** Save verbose log in the 'waimportexport' blob container - marked with a purple circle 5.
- OK button:** - marked with a purple circle 6.

*Figure 6.6: Import jobs details*

After creating the import job, we will focus on creating an export job in Azure.

You need to follow the same steps you followed in the import job. In the configuration however, you have to export the job rather than import it:

1. After you create the job, you can provide the basic configuration setting.
2. Select the **Export from Azure** option.
3. Provide the subscription and the resource group name.

Take a look at the *Figure 6.7*:

**Create import/export job** ×

**Basics** □ >

**1 Basics** >  
Configure basic settings

**2 Job details** >  
Configure data and destination

**3 Return shipping info** >  
Configure return shipping details

**4 Summary** >  
Configure return shipping details

Type \*

☐ Import into Azure

☒ Export from Azure

Name \*

bpsimport ✓

Subscription \*

Azure

Resource group \*

azure4you ▾

Create new

OK

*Figure 6.7: Export basic configuration*

4. Select the data source and select the storage account.
5. Click on **Export all**, **Selected containers and blobs**, or **Export from the blob list file (XML format)** based on the requirements.

Take a look at *Figure 6.8*:

**Create import/export job** ×

**Job details** □ ×

**1 Basics** ✓  
Configure basic settings

**2 Job details** > 1  
Configure data and destination

**3 Return shipping info** >  
Configure return shipping details

**4 Summary** >  
Configure return shipping details

Data source 2

\*Storage account

lalitstorageaccount >

Drop-off location \*

West US 2 ▾

Blobs to export 3

☒ Export all

☐ Selected containers and blobs

☐ Export from blob list file (XML format)

☒ Save verbose log in the 'waimportexport' blob container 4

*Figure 6.8: Export job details*

6. Provide the courier's name such as Blue Dart, DHL, FedEx, and so on.
7. Then, add the name, address, phone number, and other details as shown in *Figure 6.9*:

The screenshot shows the 'Create import/export job' interface. On the left, a sidebar lists four steps: 1 Basics, 2 Job details, 3 Return shipping info (highlighted with a red box), and 4 Summary. The main area displays the 'Return shipping info' form. The 'Return carrier' dropdown is highlighted with a red box, showing 'Blue Dart' selected. Other fields include 'Carrier account number' (45678734), 'Return address' (Lalit), 'Contact name' (Lalit), 'Phone' (954524234424), 'Email' (lraxyz@outlook.com), 'Street address 1' (16th cross), and 'Street address 2' (optional).

*Figure 6.9: Export job shipping details*

Once you follow these steps, you will be able to successfully create the export job. The courier guys will pick up the courier and send it to the data centre to recover the data. You can securely transfer the data using the data box. Each data box has the storage capacity of 80 TB data.

## Azure Data Box

Azure Data Box will help us migrate the terabytes of data to Azure quickly. The Data Box is a less expensive and reliable solution and is a hardware device that needs to be set up and configured. It is used for different scenarios such as:

- **One-time migration:** If you have a large amount of on-premises data and you want to move to Azure:
  - You can move the media library from your on-premises and backup tapes.
  - It will help if you want to migrate your VM, SQL Server, and applications to Azure.
  - If you want to move historical data from on-premises to Azure for in-depth analysis, and so on.



- **Initial bulk transfer:** Initial bulk transfer is done using Data Box (seed), and it provides incremental transfers over the network.
- **Periodic uploads:** If your organization generates a large amount of data periodically and if it needs to be moved to Azure, then the Data Box will help us do this.

The Data Box supports a large amount of data to migrate to Azure. It is a Microsoft device that can be configured in your on-premises data center and is connected to the Azure Data Box solution.

## Configuring Azure AD authentication for a storage account

In this section, we will discuss how to configure the authentication of Azure AD users for a storage account. It helps to manage a single identity to access the blob storage account and provide access to it, so that the user does not have to depend on the storage account key and instead, only provide the granular access using Azure AD authentication. Follow the given steps:

1. Go to the storage account and then click on **Containers**.
2. Select the container and click on the **containers**, as shown in Figure 6.10:

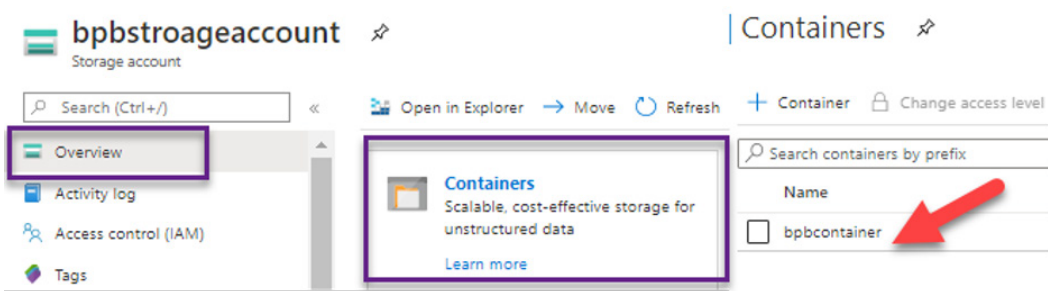
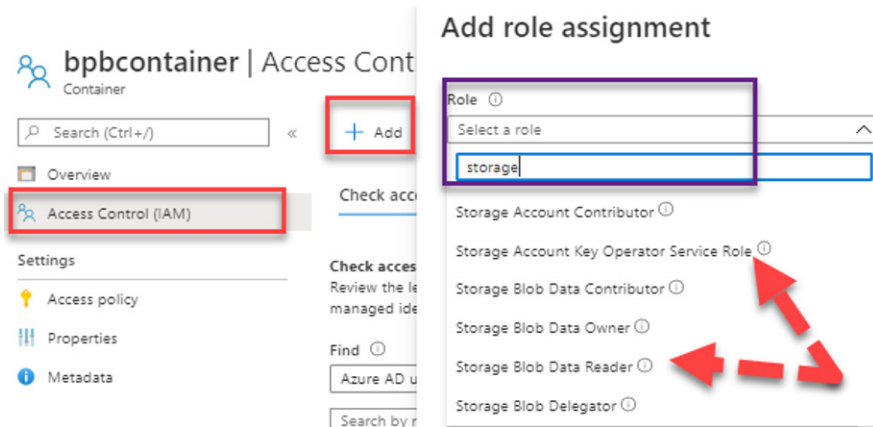


Figure 6.10: Azure AD authentication to the storage account

3. Once you get an insight into the Azure storage container, click on the Access control (IAM), as shown in Figure 6.11. Select an appropriate role from the available options. This can also be done from the storage account IAM as well:
  - **Storage Blob Data Owner:** It is used to set ownership and manage access control for **Azure Data Lake Storage Gen2** and the storage account.
  - **Storage Blob Data Contributor:** It is used to grant read/write/delete permissions to blob storage resources.

- **Storage Blob Data Reader:** It is used to grant read-only permissions to blob storage resources.
  - **Storage Queue Data Contributor:** It is used to provide the read/write/delete permissions to Azure queues.
  - **Storage Queue Data Reader:** It is used to provide read-only permissions to Azure queues.
  - **Storage Queue Data Message Processor:** It is used to grant peek, retrieve, and delete permissions to messages in Azure storage queues.
  - **Storage Queue Data Message Sender:** It is used to provide the permissions to messages in Azure storage queues.
4. Once you select the roles to assign, click on **OK** to provide the access, as shown in *Figure 6.11*:



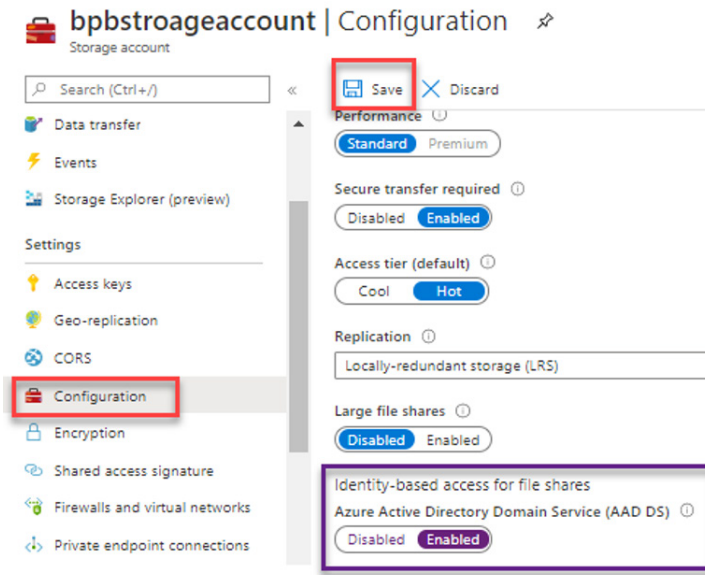
*Figure 6.11: Azure AD authentication role*

Once you provide the permission, the user will have a specific role and will be able to access the data or storage account as per the associate role.

Let us now learn how to enable the **Active Directory Domain Services (ADDS)** in the Azure storage account to access an Azure file share. Follow these steps:

1. Click on **Storage account**.
2. In the storage account, click on **Configuration**.
3. Select **Identity-based access for file shares**.

- Click on **Enabled** and save the settings, as shown in *Figure 6.12*:



*Figure 6.12: Identity-based access for a file share*

## Copying data using AzCopy

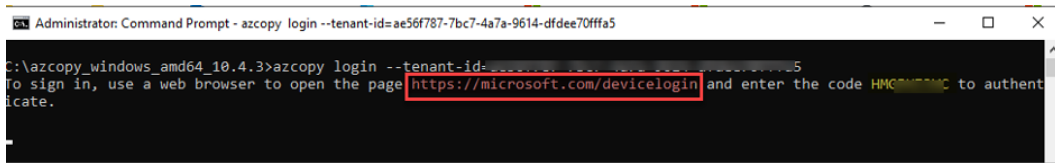
**AzCopy** is a command-line utility that is designed to copy the data from the Azure Blob, file, and table storage account. It uses the Azure AD or SAS-based authentication to connect to the Azure storage account.

We can use the utility in Windows, Mac, or Linux OS. It can also be used if you want to move or copy your blob storage account, from one storage account to another.

Let us now see how we can run these command-line utilities, to make sure we copy the data from the blob storage or upload the data in the blob storage. We can download the utility from <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>. Follow these steps:

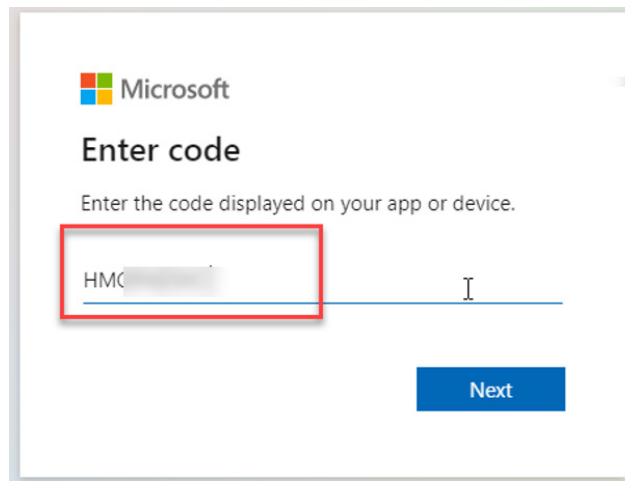
- Use the following command to log in to your Azure AD tenant:  
**azCopy login --tenant-id=aeXXXX-XXXX-XXX**
- Then, click on *Enter*.

3. Once the URL comes up in the command line, select and press *Enter* to copy the URL (<https://microsoft.com/devicelogin>). Go to the URL and browse it and provide the code which comes with the URL. Refer to *Figure 6.13*:



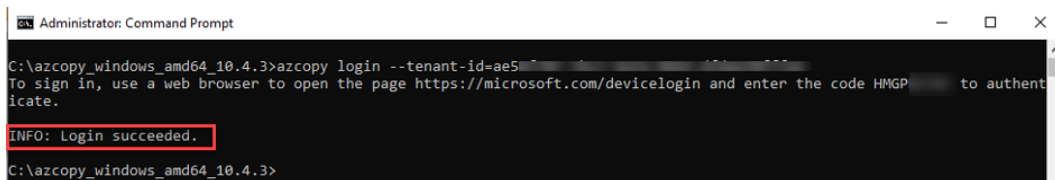
*Figure 6.13: AzCopy login*

4. Provide the authentication code, as shown in *Figure 6.14*:



*Figure 6.14: AzCopy login auth-code*

5. Once you enter the auth-code, you will be able to log in to the Azcopy console, as shown in *Figure 6.15*:



*Figure 6.15: AzCopy login successful*

6. Use the following command to copy the data to the blob storage account:

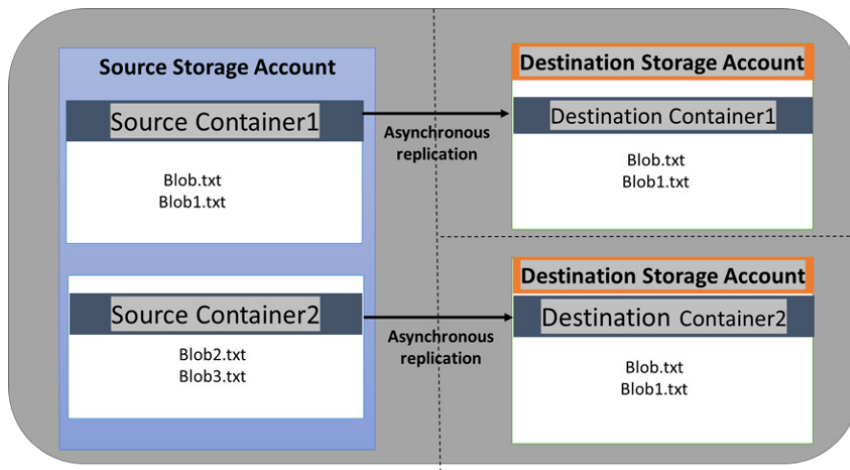
```
azCopy copy 'C:\bpbfolder\bpbTextFile.txt' 'https://bobstorage.blob.core.windows.net/bpb/bpbTextFile.txt'
```

7. Once you click on *Enter*, you will be able to copy the data. Make sure to use the correct blob storage account and destination to copy the data.

## Configure Blob object replication

Object replication asynchronously copies the data between source storage account and destination storage account. This helps to minimize the latency, increase the efficiency for compute workloads, optimizing data distribution and optimize the cost.

Refer to *Figure 6.16* for an illustration of object replication:



*Figure 6.16: Object Replication*

## Prerequisites

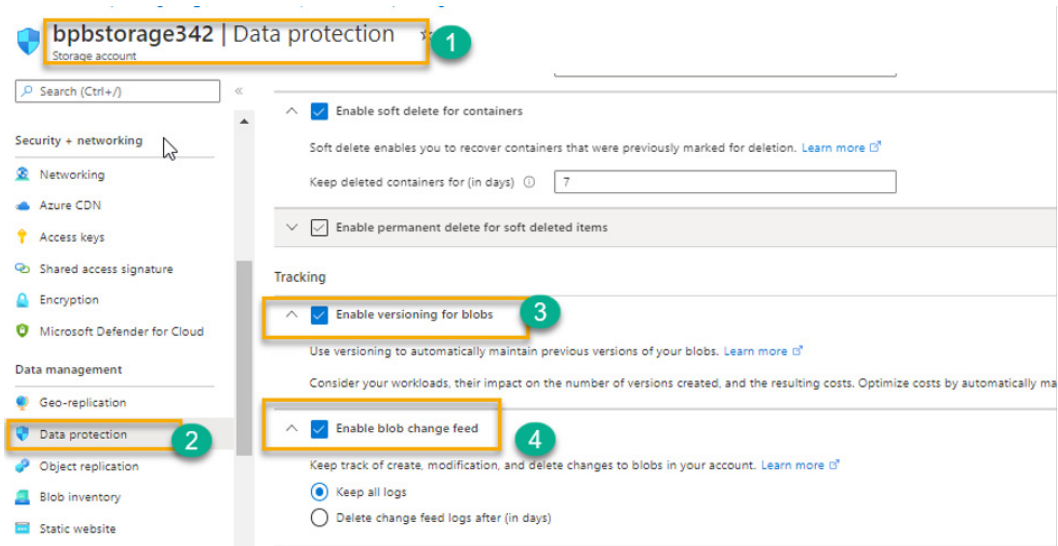
- You will have to enable the change feed for storage accounts.
- Blob versioning must be enabled for both the source and destination storage account.
- Object replication will provide support for accounts that have been encrypted using the customer managed key.
- Object replication will not be supported for customer provided key.

## Configure object replication for block blobs

Follow these steps to enable the change feed and blob versioning:

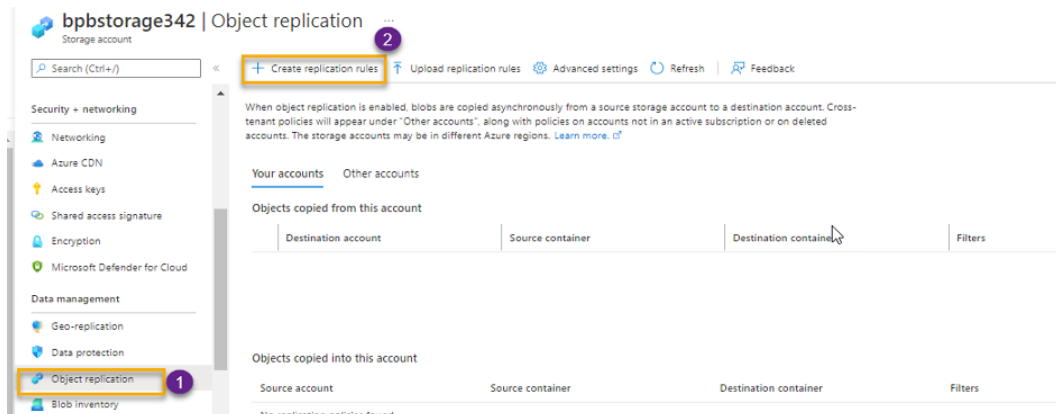
1. Select the storage account you want to enable the blob object replication for.

2. Go to **Data Project** tab under **Data management**.
3. Enable the change feed and Blob versioning, as per *Figure 6.17*:



*Figure 6.17: Enable Versioning for blob and blob change feed*

4. Go to data management and click on the **object replication**.
5. Once you will select the object replication, click on **Create replication rules**, as per *Figure 6.18*:



*Figure 6.18: Object replication*

6. Select the destination subscription and provide the details.
7. Chose the destination storage account from the drop-down menu.

8. Select the source and destination blob storage account.
9. You can also add the filter, based on the client's requirements.
10. Click on **Create**.

Refer to *Figure 6.19*:

**Create replication rules** ...

1 When you create object replication rules, blob change feed and blob versioning are automatically enabled for the source and destination storage accounts. Enabling these features may increase costs. →

**Destination details**

To begin replicating objects, specify the source storage account and the destination storage account.  
[Learn more about copying objects in object replication](#)

Destination subscription \* AzureLabs 3

Destination storage account \* lathamstorage 3

Don't see your account? [↗](#)

**Container pair details**

A container pair consists of a container in the source account and a container in the destination account. Objects in the source container are copied over to the destination container according to the replication rule. You can optionally filter which objects are copied by specifying a prefix match and by copying objects created only after a specified date and time.

| Source container          | Destination container          | Filters | Copy over                 |
|---------------------------|--------------------------------|---------|---------------------------|
| bbp                       | backup                         | 0 (add) | Only new objects (change) |
| bbp1                      | insights-logs-coreazurebackup  | 0 (add) | Only new objects (change) |
| Select a source container | Select a destination container |         |                           |

4

5 To configure more than 10 container pairs (up to 1000), see [Configure object replication using a JSON file](#)

Create Cancel 5

*Figure 6.19: Object replication creation*

After these steps are completed, the object replication policy will be created successfully, as shown in *Figure 6.20*:

**bbp1.txt** ...

Blob

Upload Change access level ...

**Authentication method:** Access key ([Switch to Azure AD User Account](#))

**Location:** bpb

Search blobs by prefix (case-...)

☒ Show deleted blobs

[Add filter](#)

**Name**

☐ bpb1.txt ...

Save Discard Download Refresh Delete Change tier Acquire lease Break lease

CONTENT-LANGUAGE

CONTENT-DISPOSITION

LEASE STATUS Unlocked

LEASE STATE Available

LEASE DURATION -

COPY STATUS -

COPY COMPLETION TIME -

**Undelete**

**Object replication**

| Policy ID                        | Rule ID                           | Status   |
|----------------------------------|-----------------------------------|----------|
| f9eb5974-d557-4d8a-a714-c2635... | e331b1a8-8e13-4102-8f9f-f6289e... | Complete |

*Figure 6.20: Object replication validation*

## Conclusion

In this chapter, we discussed the use of the import and export services and how to migrate the petabytes of data to Azure. We also discussed the Azure AD authentication which will help define the fine-grained access to the Azure storage account. Using the Azure **AzCopy** command utility, you can transfer the data from one blob storage account to another, and also transfer from on-premises systems. We have also covered the blob object replication and now the reader can replicate the data between 2 different storage accounts.

In the next chapter, we will discuss the Azure file configuration, and see how to access the Azure file share. We will learn about the Azure file sync as well and the details of usage and configuration in the next chapter.

## Points to remember

- Azure data box will help to migrate the 100 TB data Azure.
- AzCopy will help to migrate up to 10 TB data to Azure.
- Configure blob object replication for blob versioning and change feed.

## Multiple choice questions

1. The customer wants to migrate the 2 PB data from on-premises to Azure. Which solution will you choose?
  - a) AzCopy
  - b) Azure file sync
  - c) Azure data box
2. Blob object replication is used for:
  - a) Blob versioning
  - b) Changing feed
  - c) Both

## Answers

1. c
2. c



# CHAPTER 7

# The Azure File Share

## Introduction

In this chapter, we will discuss the Azure file share, creating the Azure File share and mapping a network drive. We will use the Azure File sync services and see how to troubleshoot them. We will also discuss the different types of Azure File sync groups and how to setup and configure the blob lifecycle management for storage cost optimization.

## Structure

The following topics will be covered in this chapter:

- Azure file share
  - Creating and configuring the Azure file share
  - Configuring the Azure File Sync
  - Azure File Sync group
- Azure File Sync troubleshooting
- Configure blob life cycle management

## Objectives

By the end of this chapter, we will understand the Azure File share and how to create the Azure File share. The Azure File share can be used as a network drive, and we will learn how to map it to our servers and sync the on-premises files to Azure. We will also learn about the Azure File sync and how Azure File Sync helps customers transfer the on-premises files to Azure. It provides flexibility, performance, and compatibility.

## Azure File share

The Azure File share can be used for network sharing just like the map network drives. It works on SMB port and 445 port, and it can be used to keep the data with regards to **Virtual Hard Disk (VHD)**, backup, and sharing the data. You can keep a maximum of 5 TB data per file share. If you want to keep more data in it, then you must create more file share storage account to keep the data.

There is a limitation in the Azure File share, but not in Azure storage account. In just one storage account, you can create multiple file shares and keep the data and apply different kinds of security policies.

The Azure File share helps us provide the storage space without adding any additional storage on-premises.

## Creating and configuring the Azure File share

In *Chapter 5, Managing and Configuration of Storage Accounts*, we learned how to create a storage account, its type, and its usage. If you want to create the file share in the storage account, follow the given steps:

1. Log in to the portal.
2. Select the storage account for which you want to create the Azure File share.
3. Click on the **File Share** option.

Take a look at the Azure File share created in the storage account, as shown in *Figure 7.1*:

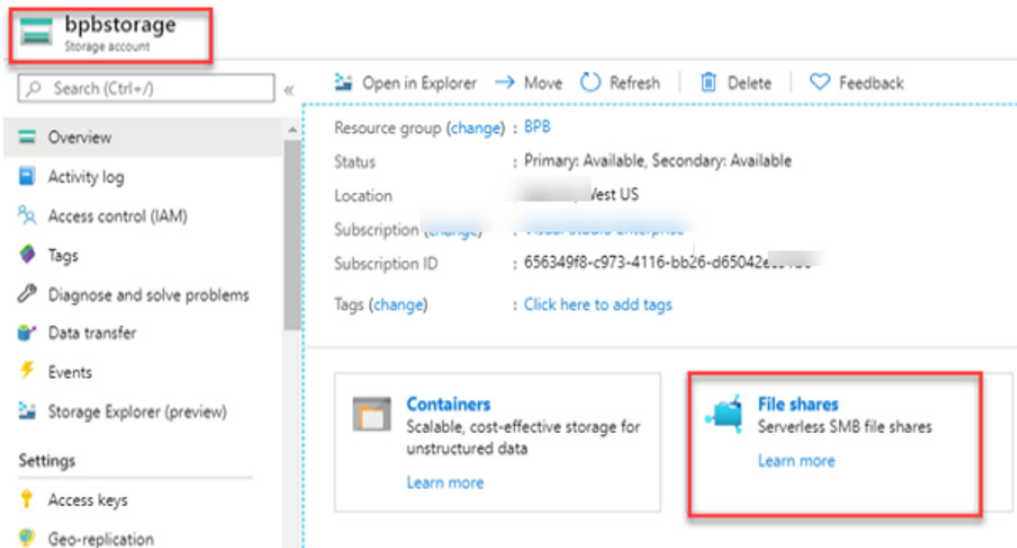


Figure 7.1: Azure File share creation in a storage account

4. Click on the **File share** button.
5. Provide the name, as shown in Figure 7.2.
6. Set the quota limit as per the customer's requirements.
7. Click on the **Create** button.

Let us take a look at Figure 7.2:

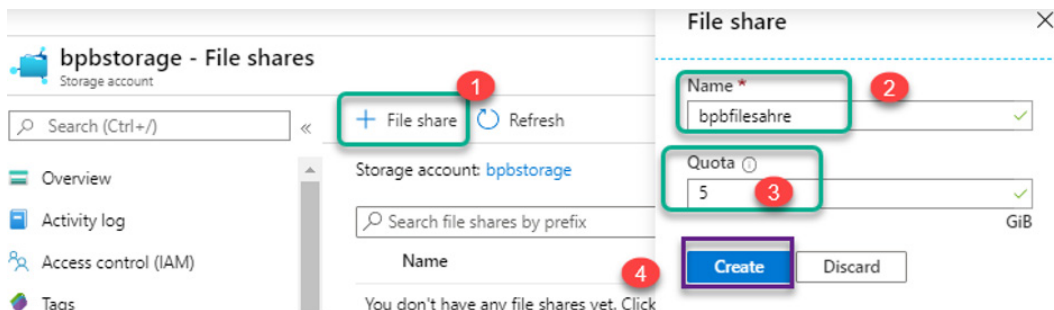
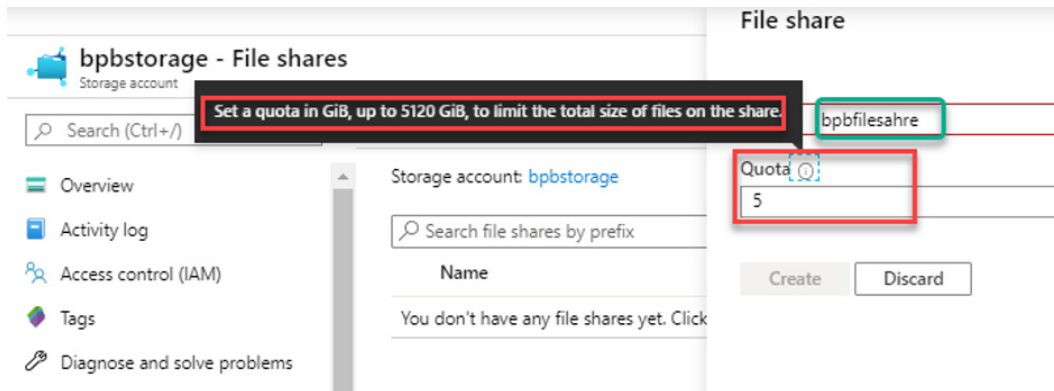


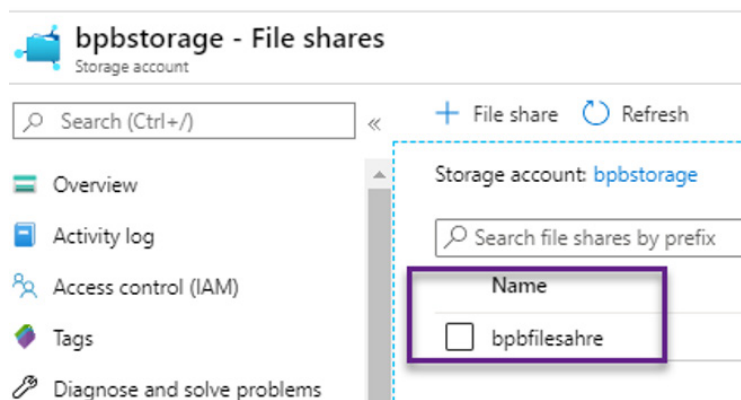
Figure 7.2: File share creation

8. You can create the file share up to 5 TB each, and this is a limitation from MS Azure end. Let us take a look at *Figure 7.3*:



*Figure 7.3: Azure File share limitation*

9. Once the file share is created, it will look like *Figure 7.4*:

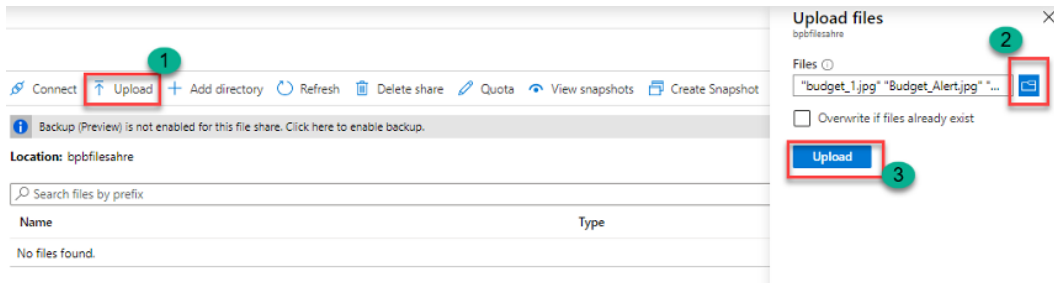


*Figure 7.4: Azure File share*

10. Once you click on the folder, you will get the option to upload the data.
11. Click on the **Upload** tab.
12. Select the file and browse the folder to upload the documents from.
13. Once done, click on the **Upload** button to upload the documents:
  - **Add directory**: Used for folder creation or to add folder in the file share.
  - **Refresh**: If the data is not reflecting, you can refresh the button.

- **Delete share:** This can be used to delete the complete share folder.
- **Quota:** This will help increase or decrease the quota limit.
- **View snapshots:** This can be used to see a snapshot of your file share.
- **Create snapshot:** This can be used to create the backup of your file share or create the snapshot within a storage account.

Refer to *Figure 7.5*:

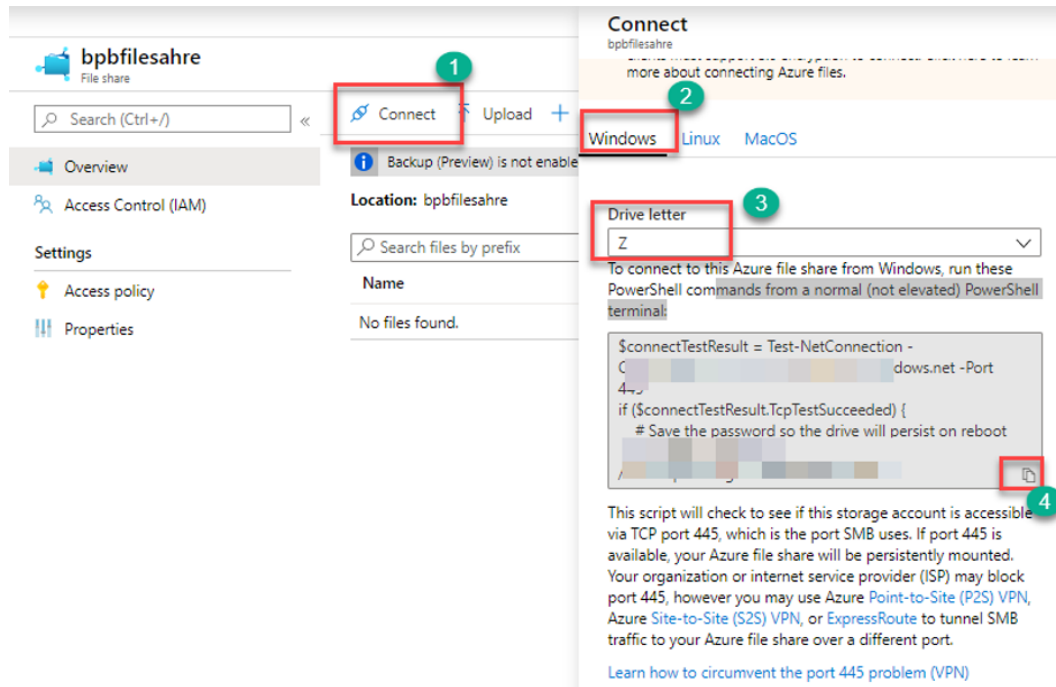


*Figure 7.5: Azure File share file upload*

Now, let us learn how to connect the file share with your on-premise machine or local desktop PC:

1. Click on the **Connect** option.
2. Once done, it will ask you to copy the path and run it in PowerShell.
3. The Azure File share supports Windows, Linux, and Mac OS to connect to the file share.
4. Based on the OS, you can copy the command line and follow the instructions to connect.
5. Make sure you allow 445 port from your Firewall and NSG to connect to the file share.

Let us take a look at *Figure 7.6*:



*Figure 7.6: Azure File share connect*

Now, you can connect the Azure File share and upload the data which will automatically sync to an Azure File share.

## Configuration of Azure File Sync

Azure File sync will help you manage the documents centralized just like your network share. It provides flexibility and high performance with your on-premises file server. It supports protocols like SMB, NFS, and FTPS to access your data locally and provides the cache to the Azure File share.

**Note:** For now, it supports only Windows Server and no other platform as per the MS documentation. Please take a look at the documentation for more clarification on Azure File sync support and features.

If you want to create the Azure File share, follow the given steps to create the Azure File sync:

1. Go to **Marketplace** and search for **Azure File Sync**.
2. Select the services.

3. Provide the name of the file sync services.
4. Click on create **Azure File sync**.
5. Select the resources group.
6. Click on **Review + Create**.
7. Once done, you will be able to create file sync services.

Let us take a look at *Figure 7.7*:

Basics \*   Tags   Review + create

Azure File Sync in combination with Azure file shares allows you to centralize your organization's file shares in Azure, while keeping the flexibility, performance, and compatibility of an on-premises file server. [Learn more](#)

**Storage Sync Service**  
Microsoft

Deploying this storage sync service resource will allow you to transform your Windows Server into a quick cache for Azure file shares with optional cloud tiering and multi-server sync functionality. Keep in mind that servers registered to different storage sync service resources cannot exchange data with each other. It's best to register all servers to the same storage sync service if they will ever have a need to sync the same Azure file share.

Subscription \*

Resource group \*  [Create new](#)

Storage sync service name \*

Region \*

**Review + Create**   Previous   Next: Tags >

*Figure 7.7: Azure File sync creation*

8. Now, you can create the Azure File Sync.

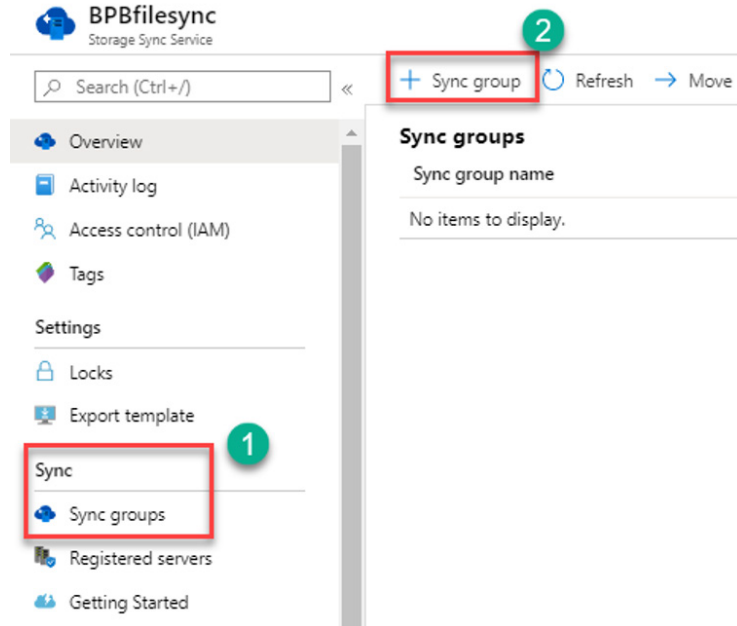
Next, we will create the Azure File Sync group.

## Azure File Sync group

Azure File Sync provides a set of sync topology to a set of files, to keep the data syncing through the endpoint, which has been created during the Azure File Sync group creation. The sync group helps to sync files from multiple endpoints, to continue syncing. To create the sync group, follow the given steps:

1. Select the **Azure File Sync**.
2. Go to the **Sync** tab and click on the **Sync group** option.

Let us take a look at *Figure 7.8*:



*Figure 7.8: Sync group creation*

3. Provide the sync group name.
4. Select the subscription.
5. Click on the storage account and select the Azure storage account. Then select the Data Box as well for the same solution.
6. Select the **Azure File Share** from the drop-down menu.
7. Click on **Create**. Once done, your sync group will be created.



Take a look at *Figure 7.9*:

Start by specifying an Azure file share to sync with - this is the sync group's first cloud endpoint.

You can specify a folder on your servers you want to sync later.

[Learn more](#)

Sync group name: BPBsyncgroup

1st Cloud endpoint: Subscription

Storage account: Select storage account

/subscriptions/

**Choose storage account**

These are the storage accounts i

bpbstorage BPB

storage4311 NetworkWatcherRG

**Azure File Share**

bpbfilesahre

Create Cancel

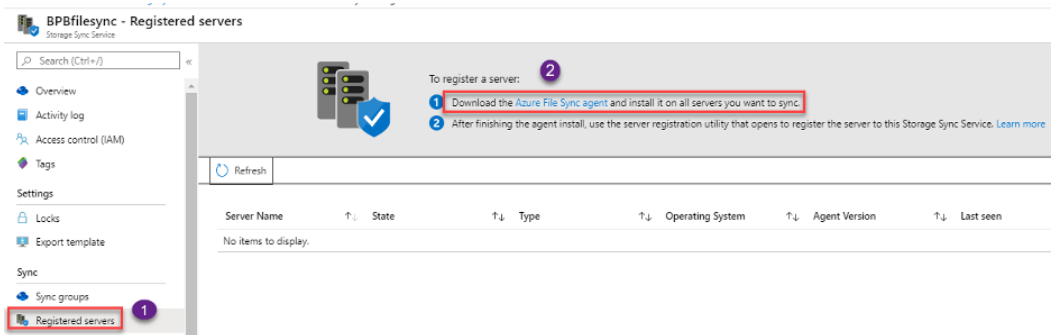
**Figure 7.9: Sync group creation steps**

*Figure 7.9: Sync group creation steps*

Now, you can create the Azure sync group. Once the sync group is created, please register the servers you want to transfer the data to:

1. Click on the **Sync** tab.
2. Click on **Registered servers**.
3. Click on the **Download Azure File Sync agent and install it on all servers you want to sync** option.
4. Once the agent is installed, your servers will be shown to register servers.
5. You will be able to transfer the files and folders automatically.

Take a look at *Figure 7.10*:



*Figure 7.10: Registered servers*

## Azure File Sync troubleshooting

Azure File Sync troubleshooting will help you figure out the common issues you face, to connect to the Azure File share. You might have a problem deleting the files from the Azure File share or agent installation. You might have an issue with registered servers' addition or removal process.

You might sometimes face an issue of the server being already added, which leads you to troubleshoot and fix the issue. Sometimes, you might also face the issue of the sync group not working or **MgmtServerJobFailed**.

For all these issues, Microsoft Azure has written a wonderful documentation (<https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-troubleshoot?tabs=portal%2Cazure-portal>). Follow this documentation to fix the issue.

## Configure blob life cycle management

Blob life cycle management enables blob data to move to another tier while expiring.

For example, let us assume you have 1 TB data which you are using as hot store, but after a few months or a year, when the data is expired or no longer needed, you can easily move to archive or cool tier using life cycle management policy without putting any manual efforts.

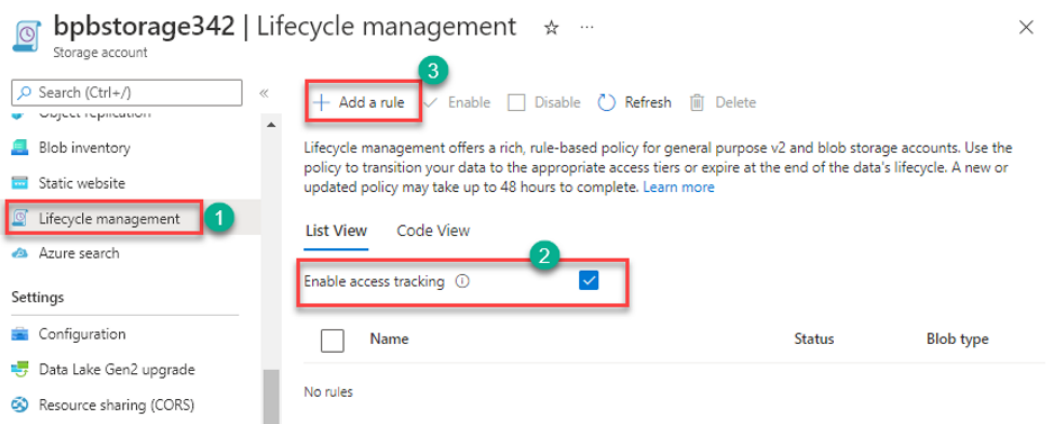
Life cycle management policy is a combination of one or more rules, that define the set of action to take, based on conditions you configured in policy.

For example, it has been a number of days since the last blob has been modified. Based on that, you create a rule and put forth that condition that data will move to cool or archive tier, after that many days have passed. This will help to optimize the storage cost as well.

To configure the blob life cycle management, follow these steps:

1. Select the storage account you want to configure the lifecycle management of.
2. Enable the access tracking while clicking on the check box.
3. Click on **Add a rule** to configure the lifecycle management access policy.

Let us refer to *Figure 7.11*:



*Figure 7.11: Life cycle management*

4. Once we will click on the add rule, it will ask you to provide the details, as shown in *Figure 7.12*:
  - a. **Rule Name:** Based on the organization standard.
  - b. **Rule Scope:** You can specify the rule if you want to apply on whole blob storage account or with limit blobs with filters.
  - c. Click on the **Blob type**, select the **Block blob** and **Append blobs**.
  - d. You can also select the blob subtype, such as **Base blob**, **Snapshots**, and **Version** also.

Let us take a look at *Figure 7.12*:

**Add a rule** ...

**1 Details** **2 Base blobs**

A rule is made up of one or more conditions and actions that apply to the entire storage account. Optionally, specify that rules will apply to particular blobs by limiting with filters.

Rule name \* **4**  
 Enable the cool and Archive tier

Rule scope \* **5**  
☒ Apply rule to all blobs in your storage account  
☐ Limit blobs with filters

Blob type \* **6**  
☒ Block blobs  
☐ Append blobs

Blob subtype \* **6**  
☒ Base blobs  
☐ Snapshots  
☐ Versions

**7**  
 Previous **Next**

*Figure 7.12: Life cycle Management Add rule*

5. You can select the condition based on if and then, as shown in *Figure 7.13*.
6. Supposing you want to move the data in the base blob, which has not been accessed in the last 30 days. In that case, set the first condition that this will be moved to a cool storage.
7. The second condition that we have put forth, for the sake of this example is, if base blob has not been accessed from the last 60 days, then it will be moved to archive storage or we can put the condition to delete those data if it is no longer needed. It is purely based on your organization policy and how you want to setup.
8. Once you done with your condition, click on **Add** and your lifecycle management rule will be successfully created.

Let us refer to *Figure 7.13*:

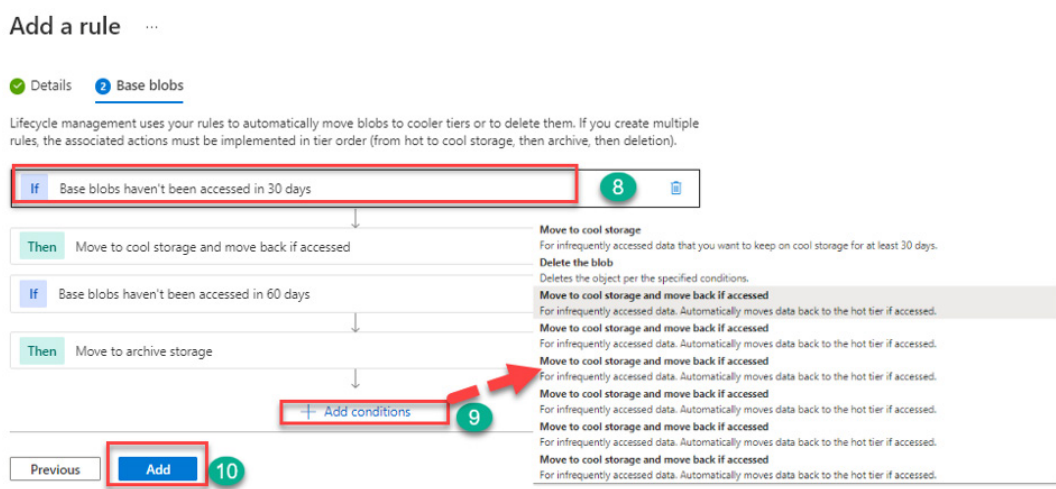


Figure 7.13: Life cycle Management rule conditions

9. Once your rules have been added, you can enable or disable based on your organizations need, as shown in *Figure 7.14*:

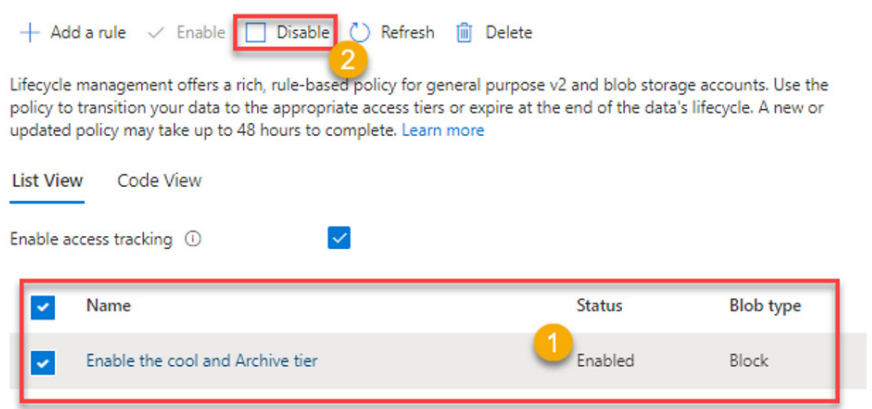


Figure 7.14: Life cycle Management rule enable/disable

# Conclusion

In this chapter, we explained the usage of the Azure File share and how to connect and transfer the files in the Azure File share. We also explained the limitation of the Azure File share. We discussed the Azure File Sync configuration and explained the components as well. In Azure File Sync, we discussed the sync group and how to register the servers. If you get stuck on some issues, then you can use the Azure File Sync troubleshooting steps, to fix the issue. We have also covered the blob lifecycle

management and provided the steps to configure the same. It will also help to manage the data in blob storage, as well as in regards to storage cost optimization.

In the next chapter, we will discuss the implementation of the Azure virtual machine and how to create and configure the Azure virtual machine.

We will discuss the high Azure availability and disk encryption and how to redeploy the Azure VM and its usage.

## Points to remember

- Azure File share will work with your network drive connect, which will help to share the files over the network. It can also map to your system.
- Azure File Sync will have to move the data to Azure, and it can do so using continuous sync.
- Configure Blob Life Cycle Management will help to manage the complete blob life cycle end to end.

## Multiple choice questions

1. **Which OS is supported by Azure file share?**
  - a. Windows & Linux
  - b. Mac
  - c. Linux
2. **What is the limit of Azure file share?**
  - a. 2 TB
  - b. 5 TB
  - c. 4 GB
3. **What is the use of Azure file sync?**
  - a. Centralized management for your files and folder.
  - b. Used to sync docs Azure to Azure.
  - c. Used for file sharing which is in the cloud.

## Answers

1. **Both a and b**
2. **b**
3. **a**

# CHAPTER 8

# Creating and Configuring of Azure VMs

## Introduction

In this chapter, we will be discussing the use of Azure VMs, how to configure the high availability, to monitor the Azure VMs usage of the Azure Storage and the kinds of disks required while creating the VMs. We will be discussing about the Azure scale set as well as to scale-in the Azure environments using Azure scale set. Lastly, we will be discussing how to choose the Azure VM size, and so on.

## Structure

The following topics will be covered in this chapter:

- Azure Virtual Machine
  - Virtual Machine Components
  - Creating a Windows Virtual Machine
  - Creating Linux VMs
- Azure Virtual Machine Scale Set Creation
- Configure Azure Disk Encryption
- Redeploying a VM

## Objectives

By the end of this chapter, the reader will be able to create the Azure Windows and Linux VM in Azure subscription, which can be used for tests, development, and production environments. Configuring the high availability will help reduce the downtime of the Azure VMs. The reader will also be able to set up the monitoring, storage, VM size, and configure the disk encryption in Azure VM, which will help to encrypt the disk and secure the disk data.

## Azure Virtual Machine

The **Azure Virtual Machine (AVM)** provides flexibility in virtual environments without buying on-premise hardware or software licenses. It provides high availability, and we can use it as on-premise servers. You can even perform tasks like software installation patching and other such tasks, as per the customer's requirements.

Azure VMs are mainly used for application testing, development work, or hybrid cloud scenarios. If you need to extend your on-premises environments to Azure, you can do that as well. Microsoft Azure supports Windows, Linux, and another custom OS version as per marketplace standards. Microsoft Azure supports various types of VM sizes as well, so that customers can deploy the VMs, based on their required configuration. It also supports high level of VM sizes for SAP and SAP HANA (**H**igh-**p**erformance **A**Nalytic **A**ppliance) as well.

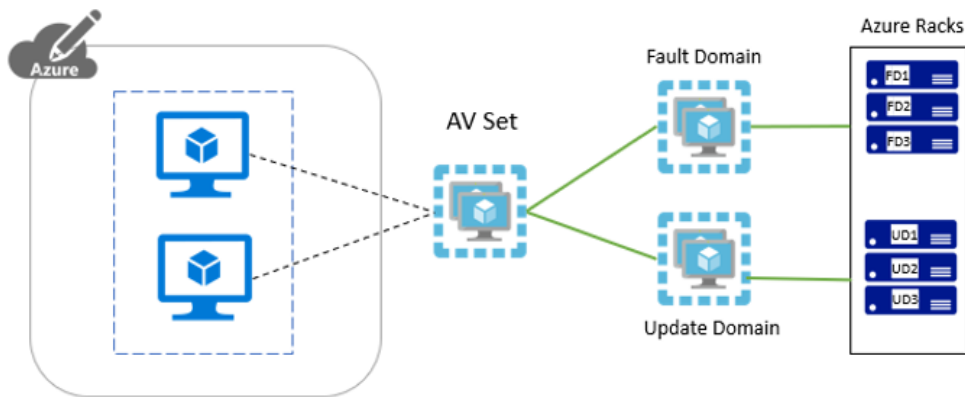
## Virtual Machine Components

If you are planning to create a VM, then you need to follow the given steps and complete a few pre-requisites. Once we understand the components, it will be easy to create the VMs:

- **Subscription:** You need to select the correct subscription where you want to deploy the VMs.
- **Resource group:** Please select the correct resources group for which you want to deploy the VMs. For more details, refer to *Chapter 4, Resource Group Management*.
- **Virtual machine name:** Follow your organization naming convention or get the details from your customer/project. Provide the machine name.
- **Region:** The region is equal to your Azure data center location. If your customer is from the US, you can choose a location like **East US**, **East US2**, **West US**, or **Central US**. Based on the customer location, you can choose the region which will help to reduce the latency.



- **Availability set:** The availability set is a logical grouping of your Azure VMs which provides high availability of your VMs in case of unexpected hardware failure, unplanned hardware or software maintenance, and if there is any planned maintenance from Microsoft Azure.
  - **Fault domain:** Fault domain shares the common power sources and physical network switch. This means that if anything happens in the hardware or network layer, then it will help your VMs to keep alive.
  - **Update domain:** Update domain will help you in case of any planned or unplanned software maintenance from Microsoft Azure. It ensures your application VMs reboot at the time within the availability set. Take a look at *Figure 8.1*:



*Figure 8.1: Azure availability set*

- **Availability zone:** The availability zone is another option that provides high availability in case of data center failure within the zone. The zone has been designed with one more data center, which provides the resiliency and availability of your data and application services. Refer to *Figure 8.2*:



*Figure 8.2: Azure availability zone*

- **Image:** Images are nothing but the operating system that you can choose while creating the VMs. Images can have Windows, Linux, Ubuntu, and other such customized images, that are available in the Azure marketplace. Refer to *Figure 8.3*:

**Marketplace**

My Saved List

Recently created

Service Providers

**Categories**

Get Started

AI + Machine Learning

Analytics

Blockchain

Compute

Containers

Search the Marketplace

Pricing : All

Operating System :

Showing All Results

| Name                                                                                                                                                                          | Publisher | Category  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------|
| >  SQL Server 2014 SP2 on Windows Server 2012 R2                                             | Microsoft | Compute   |
| >  SQL Server 2016 SP1 on Windows Server 2016                                                | Microsoft | Compute   |
|  Data Science Virtual Machine for Linux (CentOS)                                             | Microsoft | Analytics |
| >  SQL Server 2012 SP4 on Windows Server 2012 R2                                             | Microsoft | Compute   |
|  Windows Server 2016 Remote Desktop Session Host 2016                                        | Microsoft | Compute   |
| Name                                                                                                                                                                          | Publisher | Category  |
|  Data Science Virtual Machine for Linux (CentOS)                                             | Microsoft | Analytics |
|  Data Science Virtual Machine for Linux (Ubuntu)                                             | Microsoft |           |
|  SQL Server 2017 Web on Red Hat Enterprise Linux 7.4 (RHEL)                                 | Microsoft | Databases |
| >  SQL Server 2017 on Red Hat Enterprise Linux 7.4                                         | Microsoft | Compute   |
|  Free SQL Server License: SQL Server 2017 Express on Red Hat Enterprise Linux 7.4 (RHEL)   | Microsoft | Databases |
|  Free SQL Server License: SQL Server 2017 Developer on Red Hat Enterprise Linux 7.4 (RHEL) | Microsoft | Databases |
|  SQL Server 2017 Standard on Red Hat Enterprise Linux 7.4 (RHEL)                           | Microsoft | Databases |
|  Microsoft Machine Learning Server 9.3.0 on CentOS Linux 7.2                               | Microsoft | Compute   |

*Figure 8.3: Azure image options*

- **Administrator accounts:** The administrator account is used to log in locally in the VMs. You can use the VM credentials that will help you to connect the VMs to the **Remote Desktop Protocol (RDP)** or **Secure Shell (SSH)**.
- **Disk type:** The disk type is where your data and OS are stored. It consists of the following types:
  - **HDD:** Hard disk drive is backed by a magnetic disk, and it provides *500 IOPS/1TB*. It is used for any workload based on the customer's requirements.

- **SSD:** It is also called a premium disk which is backed by the solid-state drive and provides 7500 IOPS/1TB. It is mainly used for production workload.
- **Standard SSD:** It is a combination of SSD and HDD disk, which provides faster performance and provides 500 IOPS/1TB. It can be used for development and UAT environments.
- **Azure VMs size:** Azure VMs size is a collection of the capacity (memory, disk, IOPS, and so on) and features supported by your Azure VMs instance, such as, 2 GB RAM with 120 GB disk space as your on-premises hardware. You can make choices based on the requirements. It supports large instance sizes which can be used for GPU-based systems or SAP VMs. Refer to *Figure 8.4*:

Select a VM size

Browse available virtual machine sizes and their features

Search by VM size... Clear all filters

Size: Small (0-6) Generation: 2 selected Family: General purpose Premium disk: Supported Add filter

Showing 13 of 258 VM sizes. | Subscription: Visual Studio Enterprise | Region: East US | Current size: Standard\_DS1\_v2

| VM Size | Offering | Family          | vCPUs | RAM | Data disks | Max IOPS | Temporary storage | Premium disk support | Cost/month |
|---------|----------|-----------------|-------|-----|------------|----------|-------------------|----------------------|------------|
| B1ls    | Standard | General purpose | 1     | 0.5 | 2          | 160      | 4                 | Yes                  | ₹255.71    |
| B1ms    | Standard | General purpose | 1     | 2   | 2          | 640      | 4                 | Yes                  | ₹1,017.94  |
| B1s     | Standard | General purpose | 1     | 1   | 2          | 320      | 4                 | Yes                  | ₹511.43    |
| B2ms    | Standard | General purpose | 2     | 8   | 4          | 1920     | 16                | Yes                  | ₹4,091.41  |
| B2s     | Standard | General purpose | 2     | 4   | 4          | 1280     | 8                 | Yes                  | ₹2,045.71  |
| B4ms    | Standard | General purpose | 4     | 16  | 8          | 2880     | 32                | Yes                  | ₹8,163.15  |
| D2s_v3  | Standard | General purpose | 2     | 8   | 4          | 3200     | 16                | Yes                  | ₹4,720.86  |
| D4s_v3  | Standard | General purpose | 4     | 16  | 8          | 6400     | 32                | Yes                  | ₹9,441.72  |

Figure 8.4: Azure instance size

- **Network component:** Azure network components are mainly used to connect your VMs/services to your network. For example, while creating VMs, you need to select the virtual network and subnet which define the network boundary of your VMs.
- **Public IP:** A public IP address is used if you want to connect your VMs to the internet, or access and connect applications publicly.
- **NSG (inbound and outbound port):** The network security group defines the rules for ports that need to be allowed or denied, and based on the requirements, you can allow the ports. Ports are of two types:
  - **Inbound port:** The traffic which you want to allow from the internet to your VMs.

- **Outbound port:** The traffic which you want to allow from your VMs to the internet.
- **Boot diagnostics:** It is used to capture the console output and help you provide the figures of the VM running on a host, in case of occurrence of an issue.
- **OS guest diagnostics:** It helps to collect the metrics of your virtual machine. Thus, you can use and create alerts to update your teams.
- **Diagnostic accounts:** The diagnostics account is nothing but your storage account, where you want to store the diagnostics logs for further troubleshooting.
- **Auto shutdown configuration:** It helps to shut down the VMs after your business hours automatically. It is recommended that you do not use this option for your production environments.
- **Dedicated host:** It is a new feature that was launched by Microsoft Azure. It allows a dedicated host in the Azure data center, to provision the VMs within a dedicated host. It provides isolated environments and helps in any maintenance initiated by Microsoft Azure. However, it is not necessary to choose the same.
- **Proximity placement group:** It allows users to group Azure resources physically closer together within the same region.
- **Resource group tag:** It is used for billing purposes and you can tag your resources based on your requirements, such as a cost center, application name, product team, and so on.
- **Review and create:** Finally, you will see all the required details in this tab, and you can review and create the VMs.

Now let us understand and create the Azure VMs.

## Creating a Windows Virtual Machine

To create the Windows VM, perform the following steps:

1. Provide the following required details:
  - **Subscription:** Provide the subscription name.
  - **Resource group:** Provide the resources group name based on the organization standards.
  - **Virtual machine name:** Provide the VM name.

- **Region:** Provide the location you want to deploy the VM to.
- **Availability set:** Provide the availability set based on the requirements.
- **Availability zone:** Provide the availability zones based on the requirements.
- **Image:** Select the image Windows, Linux, or custom image.

Refer to the following *Figure 8.5*:

**Create a virtual machine**

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? [Create VM from Azure Marketplace](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ [Subscription] 1

Resource group \* ⓘ BPB 2 [Create new](#)

**Instance details**

Virtual machine name \* ⓘ BPBvm 3 ✓

Region \* ⓘ (US) East US 4

Availability options ⓘ Availability set 5

Availability set \* ⓘ (new) bpbvm 6 [Create new](#)

Image \* ⓘ Windows Server 2016 Datacenter 7 [Browse all public and private images](#)

*Figure 8.5: Azure VM details*

2. Then, add the following details:

- **Administrator account:** Provide the admin account username and password.
- **Size:** Provide the size of the VMs based on the requirements.

Take a look at following Figure 8.6:

The screenshot shows the 'Size' and 'Administrator account' sections of the Azure VM configuration page. The 'Size' section is highlighted with a green box and contains a yellow circle with the number 8. It shows 'Standard DS1 v2' with '1 vcpu, 3.5 GiB memory (₹3,589.82/month)' and a 'Change size' link. The 'Administrator account' section is highlighted with a red box and contains a yellow circle with the number 9. It has fields for 'Username' (bpbadmin), 'Password' (masked with dots), and 'Confirm password' (masked with dots), each with a green checkmark. Below this is the 'Inbound port rules' section, which is highlighted with a red box and contains a yellow circle with the number 10. It shows 'Public inbound ports' set to 'Allow selected ports' and 'Select inbound ports' set to 'RDP (3389)'. A warning message at the bottom states: 'This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.'

Figure 8.6: Azure VMs credentials

3. Specify the disk based on the requirements, such as **Premium SSD**, **Standard HDD**, or **Standard SSD**.
4. You can add an additional disk using advance options. Take a look at Figure 8.7:

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

**Disk options**

OS disk type \* ⓘ

Enable Ultra Disk compatibility ⓘ

**Data disks**

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

| LUN                                                                                  | Name | Size (GiB) | Disk type | Host caching |
|--------------------------------------------------------------------------------------|------|------------|-----------|--------------|
| <a href="#">Create and attach a new disk</a> <a href="#">Attach an existing disk</a> |      |            |           |              |

The screenshot shows the 'Disk options' and 'Data disks' sections of the Azure VM configuration page. The 'OS disk type' dropdown menu is highlighted with a red box and contains a yellow circle with the number 1. It shows 'Premium SSD' selected, with other options 'Standard HDD', 'Standard SSD', and 'Premium SSD' visible. The 'Data disks' section is highlighted with a red box and contains a yellow circle with the number 2. It shows a table with columns 'LUN', 'Name', 'Size (GiB)', 'Disk type', and 'Host caching'. Below the table are two links: 'Create and attach a new disk' and 'Attach an existing disk'.

Figure 8.7: Azure VMs disk specification

5. Select the virtual network name and subnet.
6. If you need **Public IP**, then click on **Create new** and provide the name.
7. Select the ports you want to allow to connect to VMs, such as 3389 or 22, and so on.

Take a look at *Figure 8.8*:

**Network interface**

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ NetworkWatcherRG-vnet ▼  
[Create new](#)

Subnet \* ⓘ default (10.0.0.0/24) ▼  
[Manage subnet configuration](#)

Public IP ⓘ None ▼  
[Create new](#)

NIC network security group ⓘ ☐ None ☒ Basic ☐ Advanced

Public inbound ports \* ⓘ ☐ None ☒ Allow selected ports

Select inbound ports \* RDP (3389) ▼

**⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.**

Accelerated networking ⓘ ☐ On ☒ Off

The selected VM size does not support accelerated networking.

*Figure 8.8: Azure VMs network configuration*

8. Provide the boot and OS diagnostics accounts.
9. Select the **Diagnostic storage account** from the drop-down menu.
10. Enable the auto-shutdown option for VMs that are not production VMs.

### 11. Provide the email ID and time zone, and so on. Refer to *Figure 8.9*:

Configure monitoring and management options for your VM.

#### Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.  
[Learn more](#)

✓ Your subscription is protected by Azure Security Center standard plan.

#### Monitoring

Boot diagnostics ⓘ ☒ On ☐ Off

OS guest diagnostics ⓘ ☐ On ☒ Off

Diagnostics storage account \* ⓘ

[Create new](#)

#### Identity

System assigned managed identity ⓘ ☐ On ☒ Off

#### Auto-shutdown

Enable auto-shutdown ⓘ ☒ On ☐ Off

Shutdown time ⓘ

Time zone ⓘ

Notification before shutdown ⓘ ☒ On ☐ Off

Email \* ⓘ

#### Backup

Enable backup ⓘ ☐ On ☒ Off

*Figure 8.9: Azure VMs diagnostics configuration*

### 12. Select the **Advanced** tab and click on **Next**, to select the **Tags** option, as shown in *Figure 8.10*:



Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

| Name ⓘ  | Value ⓘ | Resource      |
|---------|---------|---------------|
| Project | : ITS   | All resources |

Figure 8.10: Azure VMs resources tag

13. Verify **Review + create** the VMs. It will take 8 to 10 minutes to create the VMs. Now, the VM creation process is complete. Refer to Figure 8.11:

Basics Disks Networking Management Advanced Tags Review + create

**PRODUCT DETAILS**

Standard B1ls  
by Microsoft  
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ  
**0.3437 INR/hr**  
[Pricing for other VM sizes](#)

**TERMS**

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

⚠ You have set RDP ports open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

**Basics**

Subscription

Resource group B0B

Virtual machine name B0BVM

Region (US) East US

Availability options Availability set

Availability set (new) bpbav

Username lsit

Public inbound ports RDP

Already have a Windows Server license? No

Azure Spot No

**Disks**

OS disk type Standard SSD

Use managed disks Yes

Use ephemeral OS disk No

**Networking**

Virtual network (new) B0B-vnet

Subnet (new) default (10.1.0.0/24)

Public IP (new) B0BVM-ip

Accelerated networking Off

Place this virtual machine behind an existing load balancing solution? No

**Management**

Boot diagnostics On

OS guest diagnostics Off

Azure Security Center Standard

Diagnostics storage account bpbstorage

System assigned managed identity Off

Auto-shutdown On

Backup Disabled

**Advanced**

Extensions None

Cloud init No

Proximity placement group None

**Tags**

Project ITS (Auto-shutdown schedule)

**Create**

Figure 8.11: Azure VMs creation review

Now, you will be able to create the Windows VM. Let us now learn to create Linux VMs.

## Creating Linux VMs

If you need to create the Linux VMs, please change the image name to *Linux, Red Hat Enterprise*, and so on, followed by the preceding steps as provided for the Windows virtual VM creation. Refer to *Figure 8.12*:

The screenshot shows the 'Create VM' wizard in the Azure portal. The tabs at the top are Basics, Disks, Networking, Management, Advanced, Tags, and Review + create. The 'Image' dropdown is highlighted with a red box, showing 'Red Hat Enterprise Linux 7.7' and a link to 'Browse all public and private images'. The 'Virtual machine name' is 'BPEVM', 'Region' is '(US) East US', 'Availability set' is '(new) bpbav', and 'Image' is 'Red Hat Enterprise Linux 7.7'.

Figure 8.12: Azure Linux VMs

Once you complete all the steps, click on **Create** and your Linux VM will be created. You can refer to the VM creation section to get more details.

## Azure virtual machine scale set creation

The Azure scale set helps you to create a group of VMs and manage them. It is automatically managed to increase or decrease the VMs, based on the CPU usage or other rules, which you have to define in a scale set. It provides high availability of your application while auto-scaling the VM, based on the required configuration. It provides redundancy and improves the performance of your applications which is distributed across multiple instances.

It is easy to create a scale set and high availability and application resiliency. You can scale the instance based on application demands. Follow these steps to create a VM scale set:

1. Let us configure and deploy the scale set and follow the given steps:
  - **Virtual machine scale set name:** BPBScaleset
  - **Operating system disk image:** Windows Server 2016 Datacenter
  - **Subscription:** Select a subscription.
  - **Resource group:** BPB
  - **Location:** (US) East US
  - **Availability zone:** Select if required or leave it to default.
  - **Username:** BPBuser
  - **Password:** Provide the password.

Take a look at *Figure 8.13*:

**Create virtual machine scale set**

 [Preview the new create experience →](#)

---

**BASICS**

Virtual machine scale set name \*  ✓

Operating system disk image \* ⓘ  ▼  
[Browse all public and private images](#)

Subscription \*  ▼

Resource group \*  ▼  
[Create new](#)

Location \*  ▼

Availability zone ⓘ  ▼

Username \* ⓘ  ✓

Password \*  ✓

Confirm password \*  ✓

*Figure 8.13: Azure scale set configuration*

- **Instance count:** The default value is 2 and based on the requirement, you can increase the count.
- **Instance size:** **Standard B1S**

- **Use managed disks:** Select **Yes**, if it is required.
- Enable the scale set while creating or you can select after creating it as well.

Take a look at *Figure 8.14*:

The screenshot displays the Azure portal configuration for a scale set. The 'INSTANCES' section is expanded, showing the following settings:

- Instance count \***: 2
- Instance size \***: Standard B1ls (1 vcpu, 0.5 GiB memory). A 'Change size' link is visible.
- Deploy as low priority (preview)**: No (selected), Yes
- Use managed disks**: No, Yes (selected)
- Use ephemeral OS disk**: No (selected), Yes

Below the instance settings, a message states: 'Low priority is not available for the selected instance size.' and 'Ephemeral OS disks are currently not supported for the selected instance size.'

The '+ Show advanced settings' link is visible. The 'AUTOSCALE' section is also expanded, showing the following settings:

- Autoscale**: Disabled, Enabled (selected)
- Minimum number of VMs \***: 1
- Maximum number of VMs \***: 10
- Scale out**:
  - CPU threshold (%) \***: 75
  - Number of VMs to increase by \***: 1
- Scale in**:
  - CPU threshold (%) \***: 25
  - Number of VMs to decrease by \***: 1

*Figure 8.14: Azure scale set auto-scale configuration*

2. If you want to select the application gateway, select the same.
3. Select the virtual network.
4. Select Public IP, if required.

5. Public inbound ports are required.
6. Enable the boot diagnostics.
7. Click on the **Create** button.

Take a look at *Figure 8.15*:

**NETWORKING**

Microsoft Azure Application Gateway is a dedicated virtual appliance providing application delivery controller (ADC) as a service. Azure Load Balancer allows you to scale your applications and create high availability for your services.  
[Learn more about load balancer differences](#)

| Resources           | Optimal for          | Supported Protocols | SSL offloading | RDP to instance |
|---------------------|----------------------|---------------------|----------------|-----------------|
| Application Gateway | Web-based traffic    | HTTP/HTTPS/WebSo... | Supported      | Not supported   |
| Load balancer       | Stream-based traffic | Any                 | Not supported  | Supported       |

Choose Load balancing options ☒ Application Gateway ☐ Load balancer ☐ None

Application Gateway \* ⓘ No available application gateways in the selected subscription and location ▼

Virtual network

Subnet ⓘ No application gateway selected ▼

Public IP address per instance ⓘ ☐ On ☒ Off

Accelerated networking ⓘ ☐ On ☒ Off

**i** The selected VM size does not support accelerated networking.

NIC network security group ⓘ ☐ None ☒ Basic ☐ Advanced

Public inbound ports \* ⓘ ☒ None ☐ Allow selected ports

Select inbound ports Select one or more ports ▼

**i** All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

**MANAGEMENT**

Boot diagnostics ⓘ ☐ On ☒ Off

System assigned managed identity ⓘ ☐ On ☒ Off

**Create**

*Figure 8.15: Azure scale set network configuration*

# Configure Azure Disk Encryption

The Azure disk encryption will use a BitLocker feature to enable the full disk encryption of the Windows OS and data disk. We can configure the Azure disk encryption, using the Azure portal, PowerShell, and Azure CLI. The Azure key vault is integrated with Azure encryption, to help you to manage the access and control the encrypted disk.

For Linux, the Azure VM uses a DM encrypt feature to provide the volume encryption to the OS and data disk of the Linux VM. The Azure key vault is integrated with the Azure encryption, to help you to manage the access and control the keys and secrets. It supports the following OSes:

- Windows 8 and later OS version
- Servers 2008 R2 and later OS version
- Red Hat, Ubuntu, and so on as per Linux OS disk encryption supported

Let us see how to configure the disk encryption:

1. Go to the VM to which you want to enable the disk encryption.
2. Under **Settings**, click on the **Disks** option.
3. On the right-hand side of the tab, click on **Encryption**, as shown in *Figure 8.16*:

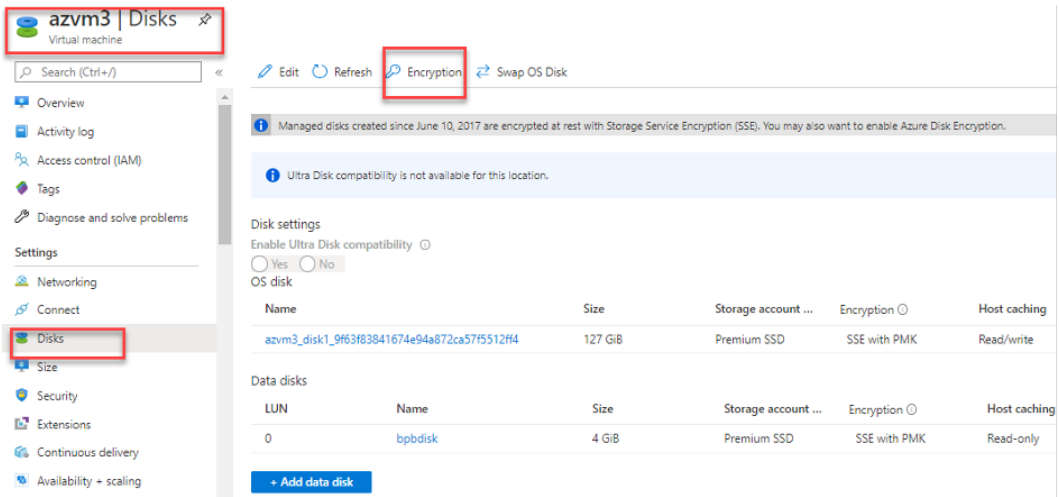


Figure 8.16: Azure disk encryption

4. Once you click on **Encryption**, it will open another tab to provide the details to encrypt the disk. Follow the given details:

- a. Select the following disk option from the drop-down menu:
  - i. None
  - ii. OS disk
  - iii. OS and data disks
- b. Once you select this option, you need to select the key vault, key, and key version, as shown in Figure 8.17:

**Encryption**  
azvm3

Save Discard

Azure Disk Encryption (ADE) provides volume encryption for the OS and data disks. [Learn more about Azure Disk Encryption.](#)

⚠ Data disks must be mounted by the guest operating system before they can be encrypted.

Disks to encrypt ⓘ  
OS and data disks

None  
OS disk  
OS and data disks

Encryption settings  
Azure Disk Encryption is integrated with Azure Key Vault to help manage encryption keys. As a prerequisite, you need to have an existing key vault with encryption permissions set. For additional security, you can create or choose an optional key encryption key to protect the secret.

Select a key vault and key for encryption

Key vault \* ⓘ  
/subscriptions/.../resourceGroups/BPB/providers/Microsoft.KeyVault/vaults/bpb... ✓

Key ⓘ  
diskecryption

Version ⓘ  
f8dabbf6c4524221ab71eaaa71151da0

Figure 8.17: Azure disk encryption settings

5. Once you fill all the parameters, click on **Save** at the top, to encrypt the disk. It will pop up the message that the VM might reboot, and you need to reboot the VM.
6. Click on **Yes** and your disk will start encrypting, as shown in Figure 8.18:

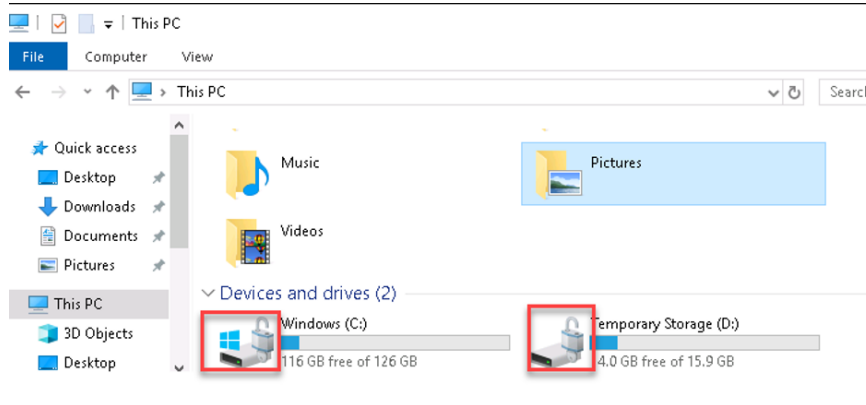
Save Discard

Enabling Azure Disk Encryption will cause the VM to reboot.  
Do you want to encrypt and restart virtual machine 'azvm3'?

Yes No

Figure 8.18: Azure disk encryption save

7. Once you log in to your system, you will observe that you have enabled the disk encryption. Then, you will see that the disk has a lock sign, which is a BitLocker encryption symbol. Hence, your disk has been encrypted, as shown in *Figure 8.19*:



*Figure 8.19: Azure disk encryption verification*

Now, we have successfully verified that the Azure disk encryption is done and understands the whole process.

## Redeploying a VM

Azure VM redeploy can be used if you are facing an RDP connection troubleshooting issue or application connectivity issue in the Azure VM. Azure redeploy will help you to move them to a new node, and in this process, the VM will shut down, as well as the entire configuration, including your data disk. However, the temporary disk data will be deleted. Let us see how to process with the Azure virtual machine redeploy VM option.

1. Go to the VM for which you want to perform the Azure VM redeploy option.
2. Go to **Support + troubleshooting**.



3. Then, click on the **Redeploy** option, as shown in Figure 8.20:

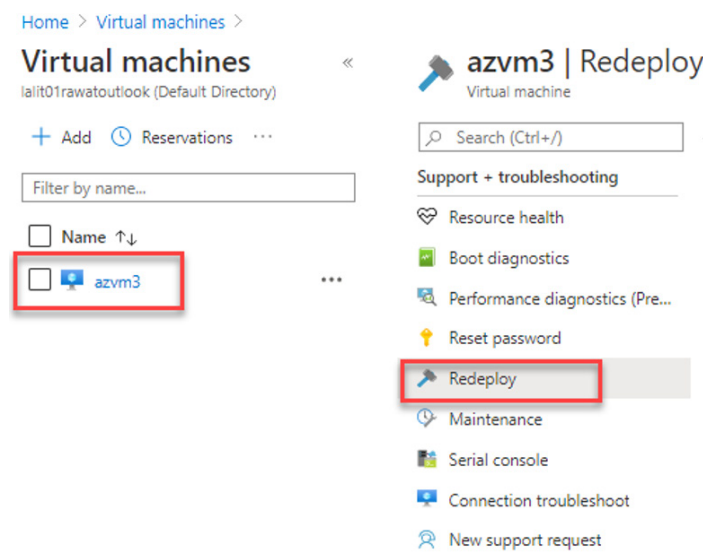


Figure 8.20: Azure VM redeploy

4. Once you click on the **Redeploy** option, click on the **Redeploy** button and the process will start. Then you can go through the instruction, as shown in Figure 8.21:

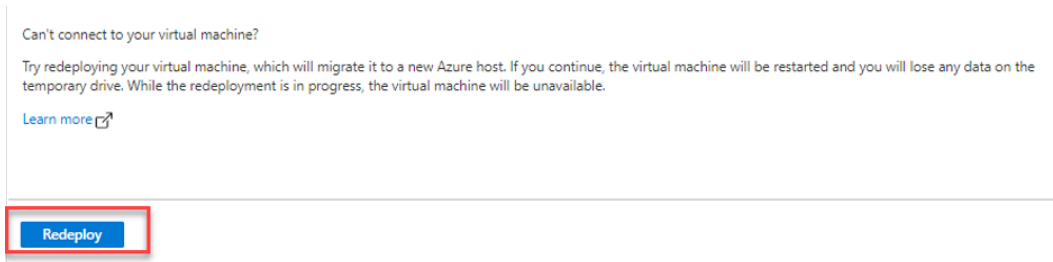


Figure 8.21: Azure VM redeploy instruction

It will take up to 15 to 20 minutes to complete the process. Once this is complete, you can see your VM up and running fine. You can then connect to apps or VMs.

## Conclusion

In this chapter, we discussed the Azure virtual machine and its usage. We described the Azure virtual machine and scale set components in detail. We also discussed how to implement the Azure disk encryption and encrypt your disk, and how to troubleshoot the issue using the Azure VM redeploy option.

In the next chapter, we will discuss how to deploy the Azure virtual machine automatically using the Azure template. We will also discuss how to use the ARM template and modify the same.

## Points to remember

- Azure VM will be created using Azure portal or using automation such as PowerShell, terraform, Biceps, and so on.
- Azure Virtual Machine Scale Set will help to manage the autoscaling of virtual machines and can reduce the dependencies during peak hours.
- Configure Azure Disk Encryption will help to encrypt the disk and will protect the data.
- Redeploying a VM will be done when your virtual machine is not working. In that case, you can redeploy the azure virtual machines.

## Multiple choice questions

1. **How many types of data disk can you add in azure VMs?**
  - a. Standard HDD
  - b. Premium SSD
  - c. Standard SSD
  - d. All of the above
2. **While redeploying, which data drive data will be erased?**
  - a. D drive -Temp drive
  - b. C drive
  - c. Data Disk
3. **If you want to move resources to another resource group, what option will you choose?**
  - a. Under resources group, choose Move
  - b. Resources group
  - c. None

## Answers

1. d                      2. a                      3. a

# CHAPTER 9

# Automating Deployment of VMs

## Introduction

In this chapter, we will discuss the automation of Azure VMs, how to deploy the VMs using the ARM template, how to configure the location of VMs and the ARM template, and how to save the template and deploy the VMs.

## Structure

The following topics will be covered in this chapter:

- Azure ARM template
- Modifying the ARM template
- Template deployments

## Objectives

By the end of this chapter, you will be informed about the ARM template and how to create the Azure VM using the template. We will also learn how to generate and deploy the ARM template in an Azure subscription.

## Azure ARM template

The Azure ARM template defines an automated way to deploy the Azure infrastructure, just like the Azure virtual machine storage account, and so on. This is managed by the API, called the **ARM API** or resource manager, and is used to deploy the infrastructure code. You can use the Azure portal, PowerShell or CLI, by calling the API directly and by creating ARM templates.

We can create the ARM template in the JSON format, and we can use it for the repeated deployment of your resources. It can also be used to deploy resources across the subscription environments.

**Note:** Many templates are available in the GitHub and Microsoft documentation, which can be used and modified for your deployment. Refer to the ARM GitHub at <https://github.com/Azure/azure-quickstart-templates>.

## Modifying the ARM template

In this section, we will deploy an Azure virtual machine and you will see how to use the ARM template deployment from the template. You will also understand how to generate and modify the Azure template.

To create the template, follow the given steps:

1. Log in to the portal.
2. Select the virtual machine and provide the parameters.
3. Select the subscription.
4. Select the Resources group name:
  - a. VM name
  - b. Azure disk
  - c. VNet
  - d. Subnet
5. Once the process is complete, download the template, as shown in *Figure 9.1*:

## Create a virtual machine

✓ Validation passed

[Basics](#)
[Disks](#)
[Networking](#)
[Management](#)
[Advanced](#)
[Tags](#)
[Review + create](#)

### PRODUCT DETAILS

Standard DS1 v2  
by Microsoft

[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ

**4.8250 INR/hr**

[Pricing for other VM sizes](#)

### TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

⚠

**You have set RDP port(s) open to the internet.** This is only recommended for testing. If you want to change this setting, go back to Basics tab.

### Basics

Create

< Previous

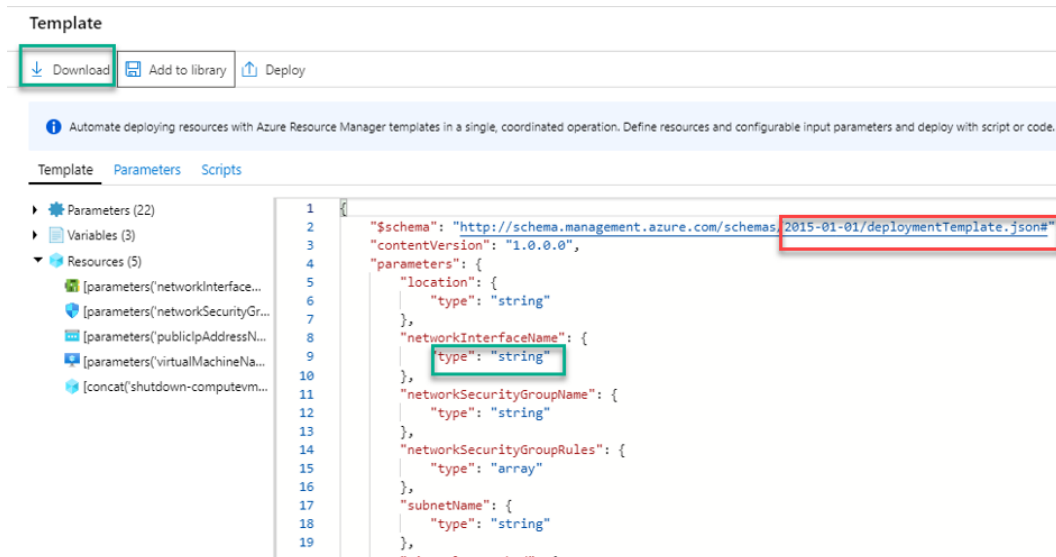
Next >

Download a template for automation

Figure 9.1: Resources template Create

6. Once you click on **Download a template for automation**, you will get multiple options such as:
  - a. Download the template
  - b. Add to ARM library
  - c. Deploy using the same template
7. You can see that the template has been created in the JSON format. It has strings and values in the template.
8. If you need to edit the template, then you will have certain edit parameters such as \$schema, contentVersion, Parameters, Variables, Resources, and Output. Once you set all these parameters, your template is ready for deployment.

Let us take a look at *Figure 9.2*:



*Figure 9.2: Resources template download*

The template will be downloaded in the ZIP folder, and you can open it in the ARM editor software.

9. Now, you can see the template parameters, and you can even set the value that could be required for further template deployment, and so on. The following values can be seen:
  - a. Location
  - b. RDP
  - c. Ports

Let us take a look at *Figure 9.3*:

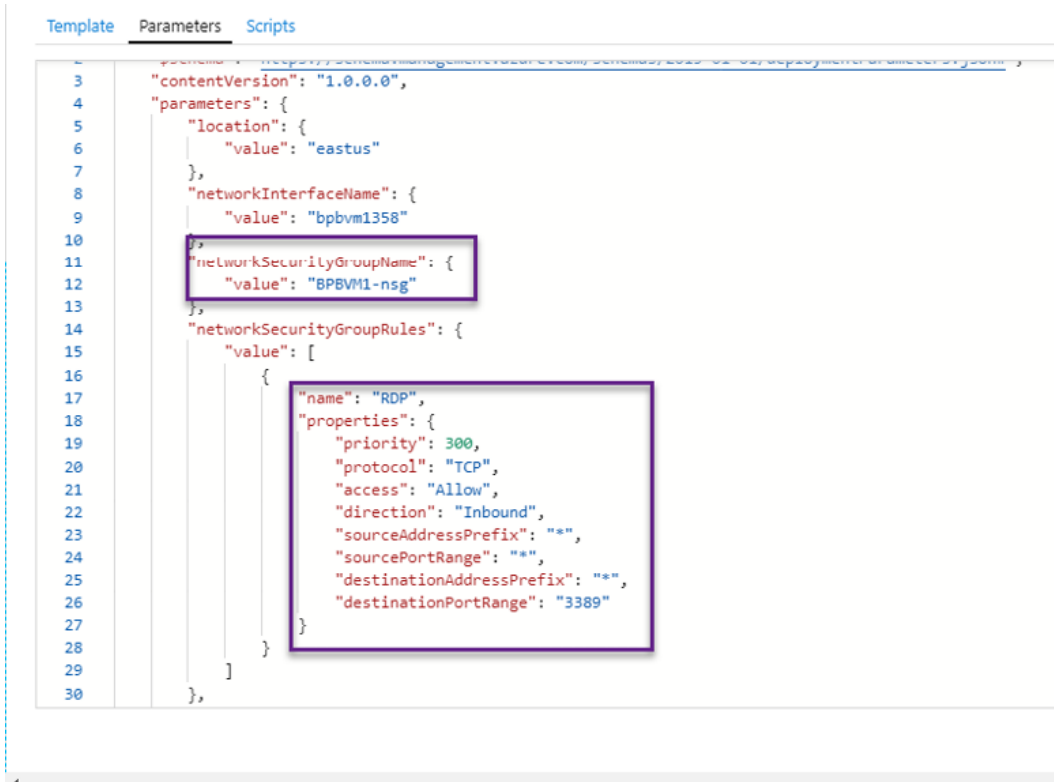


Figure 9.3: Resources template parameter

10. Search for the deployments and select the **Deploy a custom template** option, as shown in Figure 9.4:

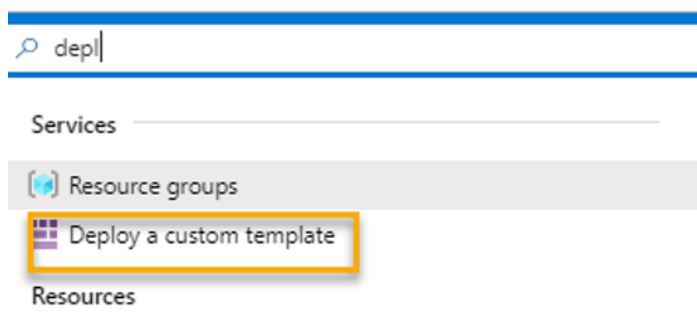


Figure 9.4: Resources template custom deployment

11. Once you select the template, you will get an option to edit the template. You can choose the template from the GitHub directly and click on edit. Refer to Figure 9.5:

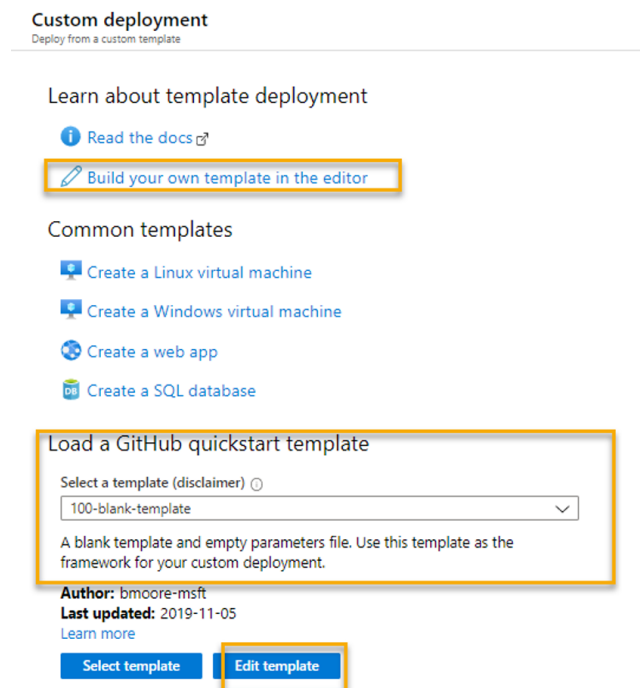


Figure 9.5: Template editor deployment

12. Once you click on **Edit template**, you will be directed to the next section. Then, select the **Load file** option and try and upload the file, as shown in Figure 9.6:

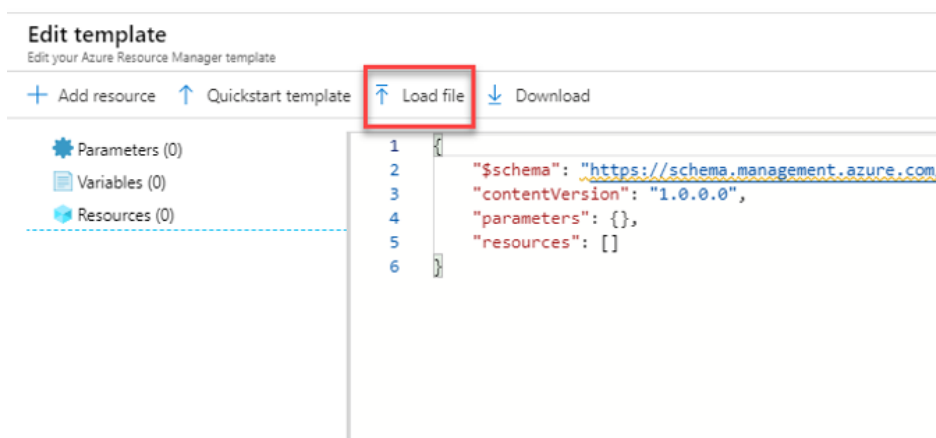


Figure 9.6: ARM template load file



13. Once you add the template, it will add your parameters, and you need to verify the parameters. Then, click on **Save**, as shown in Figure 9.7:

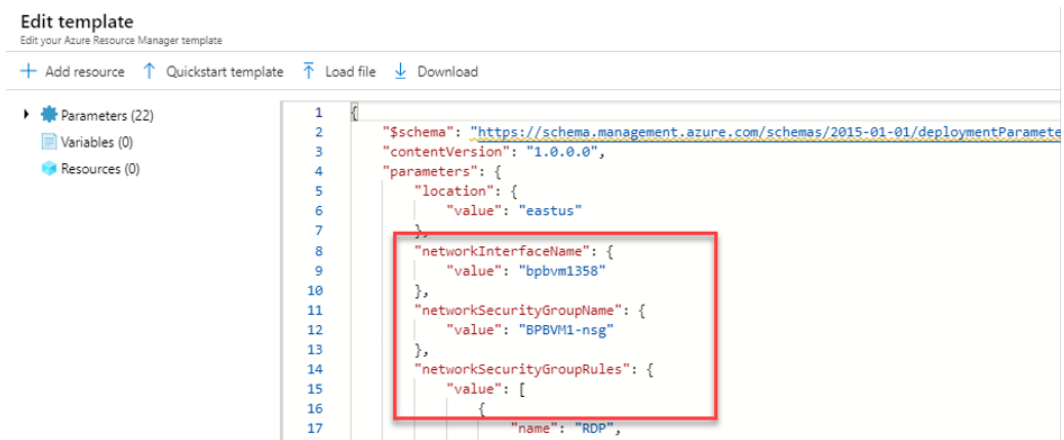


Figure 9.7: ARM template edits

## Template deployments

To deploy the template, perform the following steps:

1. Once you click on **Save**, it will automatically go to the deployment screen.
2. Provide all the parameters as per your requirements.
3. Once you are done with the parameters, click on **Purchase** and you will be able to deploy the VMs.

It will take 10 to 15 minutes to deploy the VMs. After this, your deployment will be completed. Refer to *Figure 9.8*:

**Custom deployment**  
Deploy from a custom template

---

**BASICS**

Subscription \*

Resource group \*   
[Create new](#)

Location \*

---

**SETTINGS**

**Location \***

Network Interface Name \*

**Network Security Group Name \***

Network Security Group Rules \*

**Subnet Name \***

Virtual Network Id \*

Public Ip Address Name \*

*Figure 9.8: ARM template deployment*

## Conclusion

In this chapter, we discussed how to deploy the Azure virtual machine using the ARM automation, which will help you to deploy your big infrastructure quickly and save your time.

In the next chapter, we will discuss how to create and configure the Azure containers and use of the Kubernetes services. We will give you step-by-step instructions on how to deploy the Kubernetes and container services in an Azure subscription.

## Points to remember

- ARM template use configures and deploys the Azure resources like compute, network, and so on.
- We can modify the Azure ARM template based on customer needs.

- Template deployment can be done using the VS code, portal or PowerShell.

## Multiple choice questions

1. **In which format should ARM template save?**
  - a. JSON
  - b. PowerShell
  - c. CLI
2. **What are ways of deploying the ARM template?**
  - a. PowerShell
  - b. CLI
  - c. All of the above
3. **How to deploy the ARM template from portal?**
  - a. Using Custom template
  - b. PowerShell
  - c. None

## Answers

1. **a**
2. **c**
3. **a**



# CHAPTER 10

# Creating and Configuring Container

## Introduction

In this chapter, we will learn about the Azure Container and Kubernetes services, and how to create these services as well as their usages. We can also learn about Kubernetes network configuration, upgrading AKS services or scaling with AKS. We will also discuss about Azure Container, container creation, configuration of sizing and scaling.

## Structure

The following topics will be covered in this chapter:

- Azure Container
  - Use of an Azure Container
  - Creating a Container
  - Configure scaling and sizing for Container services
    - App container creation
- Azure Kubernetes
  - Creating Azure Kubernetes

- Configuring Scaling for AKS
- Upgrade the AKS Cluster
- Configure Network Connecting for AKS

## Objectives

The objective of this chapter is to help create and configure **Azure Container Instances (ACI)** and **Azure Kubernetes Service (AKS)**.

## Azure Container

An Azure Container is a standard package of software which helps you to package the code, dependencies, and configuration of a particular application. Containers help to split the monolithic applications into individual services, which make up the solution.

## Use of an Azure Container

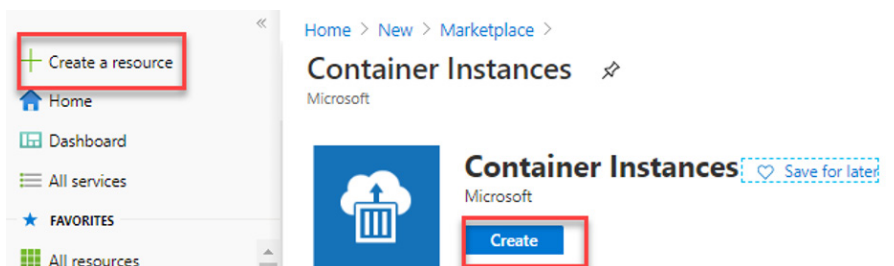
The uses of an Azure Container are as follows:

- It is used to scale up the application.
- It provides lightweight and immutable infrastructure for packaging the application and deployment.
- It provides better performance and removes the OS, versions, and dependencies.

## Creating a Container

Let us see how to create the container services using the following steps:

1. Click on **Create a resource**.
2. Search for **Container Instances**.
3. Click on **Create** for creating the container instance, as shown in *Figure 10.1*:



*Figure 10.1: Container instance create*

4. Provide the following details:
  - a. The subscription and the resources group name.
  - b. The region for which you want to create the container.
  - c. Select the image sources from any of the following options:
    - i. QuickStart images
    - ii. Azure Container Registry
    - iii. Docker Hub or another registry
  - d. Select the size of the container instance.
5. Click on the **Next: Networking** > button, as shown in *Figure 10.2*:

## Create container instance

Basics Networking Advanced Tags Review + create

Azure Container Instances (ACI) allows you to quickly and easily run containers on Azure without managing servers or having to learn new tools. ACI offers per-second billing to minimize the cost of running containers on the cloud.  
[Learn more about Azure Container Instances](#)

**Project details**  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

**Container details**

Container name \* ⓘ  ✓

Region \* ⓘ

Image source \* ⓘ ☒ Quickstart images ☐ Azure Container Registry ☐ Docker Hub or other registry

Image \* ⓘ

Size \* ⓘ  [Change size](#)

[Review + create](#) < Previous Next : Networking >

*Figure 10.2: Container instance details*

6. In the **Networking** tab, provide the following details:
  - a. Select the networking type from the following options:
    - i. **Public**: It will create a public IP address and assign it to the container for public access.
    - ii. **Private**: If you want to integrate a VNet with the container, select this option.
  - b. Provide the DNS custom name.
  - c. Verify the port number.
7. Once done, click on the **Next: Advanced** > button, as shown in *Figure 10.3*:

Basics **Networking** Advanced Tags Review + create

Choose between three networking options for your container instance:

- **'Public'** will create a public IP address for your container instance.
- **'Private'** will allow you to choose a new or existing virtual network for your container instance. This is not yet available for Windows containers.
- **'None'** will not create either a public IP or virtual network. You will still be able to access your container logs using the command line.

Networking type ☒ Public ☐ Private ☐ None

DNS name label ⓘ  .eastus.azurecontainer.io

Ports ⓘ

| Ports                | Ports protocol       |
|----------------------|----------------------|
| 80                   | TCP                  |
| <input type="text"/> | <input type="text"/> |

[Review + create](#) [< Previous](#) [Next : Advanced >](#)

*Figure 10.3: Container networking*

8. In the **Networking** tab, follow the given steps:
  - a. Click on any one option of the restart policy:
    - i. On failure
    - ii. Always
    - iii. Never



- b. Set up the environment variable if you want to set up the container.
- c. You can set a command line to override if required.

Let us take a look at *Figure 10.4*:

Basics Networking **Advanced** Tags Review + create

Configure additional container properties and variables.

Restart policy ⓘ On failure ▼

Environment variables

| Key                  | Value                |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |

Command override ⓘ  Example: [ "/bin/bash", "-c", "echo hello; sleep 100000" ]

Review + create < Previous Next : Tags >

*Figure 10.4: Container advance settings*

9. Click on **Create** after the validation of the container services, as shown in *Figure 10.5*:

### Create container instance

✓ Validation passed

Basics Networking Advanced Tags **Review + create**

**Basics**

|                     |                                 |
|---------------------|---------------------------------|
| Subscription        | Visual Studio Enterprise        |
| Resource group      | BPB                             |
| Region              | East US                         |
| Container name      | bpbcontainer                    |
| Image type          | Public                          |
| Image               | microsoft/aci-helloworld:latest |
| OS type             | Linux                           |
| Memory (GiB)        | 1.5                             |
| Number of CPU cores | 1                               |
| GPU type (Preview)  | None                            |
| GPU count           | 0                               |

**Networking**

Create < Previous Next > [Download a template for automation](#)

*Figure 10.5: Container instance creation*

Once these steps are completed, the container will be created.

## Configure scaling and sizing for Container services

If you want to configure the sizing and scaling for container services, you need to create the App Container services from the portal or using the ARM/PowerShell template. Azure Container instance does not support scaling and sizing configuration.

### App Container creation

To create the App Container instance, follow these steps:

1. Click on the **All services**.
2. Then search for container and select the **Container Apps**, as shown in *Figure 10.6*:



*Figure 10.6: Container App instance creation*

3. Select the appropriate subscription where you want to create the app container instance.
4. Choose the existing resources group or create a new resources group for the same.
5. Provide the container app name.
6. Select the region based on the client requirements or based on your company policy.
7. Then click on **Next**.

Refer to *Figure 10.7*:

## Create Container App ...

Basics App settings Tags Review + create

Azure Container Apps are containerized apps that scale on demand without requiring you to manage cloud infrastructure. You'll need a container and an environment for your first app. Select existing resources, or create them now. [Learn more](#)

### Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*  [Create new](#)

Container app name \*

### Container Apps Environment

The environment is a secure boundary around one or more container apps that can communicate with each other and share a virtual network, logging, and Dapr. [Container Apps Pricing](#)

Region \*

Container Apps Environment \*

[Review + create](#) [< Previous](#) [Next : App settings >](#)

*Figure 10.7: Container App instance details*

8. Select the quick image check box or uncheck if you want to create customize container. You can change the CPU and memory allocation, and so on.
9. You can verify container resource allocation in terms of CPU and memory.
10. Check the application ingress settings.
11. Provide the tag name and click **Review and Create**.
12. Once you will click on **Review and Create**, the creation process will start, and it will take a few minutes to create the instance.

Refer to *Figure 10.8*:

## Create Container App ...

Basics App settings Tags Review + create

Select a quickstart image for your container, or deselect quickstart image to use an existing container.

Use quickstart image ☒

### Container details

You can change these settings after creating the Container App.

Quickstart image \*

### Container resource allocation

|                     |      |
|---------------------|------|
| Number of CPU cores | 0.25 |
| Memory size (Gi)    | 0.5  |

### Application ingress settings

Enable ingress for applications that need an HTTP endpoint.

|                 |                                 |
|-----------------|---------------------------------|
| HTTP Ingress ⓘ  | Enabled                         |
| Ingress traffic | Accepting traffic from anywhere |
| Target port ⓘ   | 80                              |

*Figure 10.8: Container App settings*

## Scaling for Container App Instance

If you want to configure the scaling for container app instance, follow these steps:

1. Search for App container instance and select the app instance.
2. Under the **Application** tab with container property, select **Scale**.
3. Then click on **Edit and deploy**.

Refer to Figure 10.9:

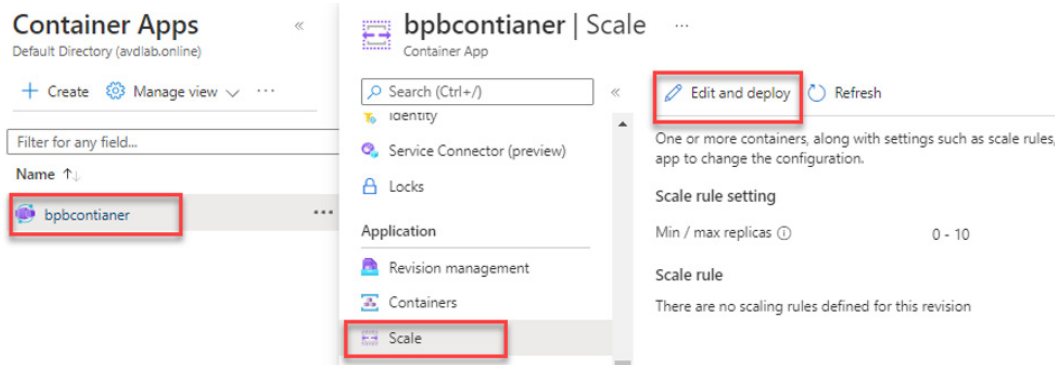


Figure 10.9: Container App instance Scale

4. Once you will click on **Edit** and deploy, it will ask Name / Prefix for container.
5. If you want to add another instance, click on **Add** and add the new instance.
6. Next, click on **Scale**, as shown in Figure 10.10:

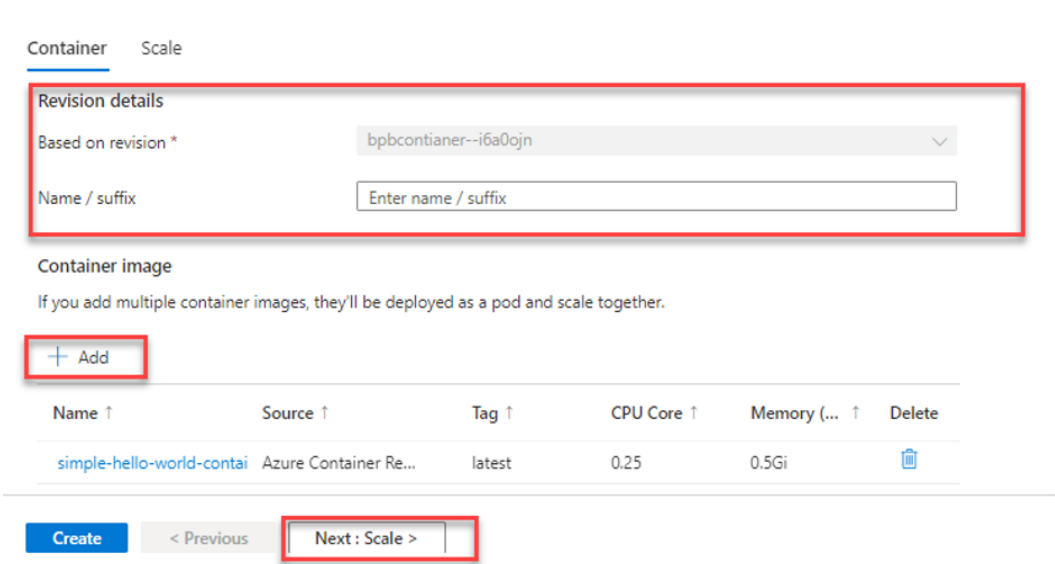


Figure 10.10: Add a new Container App instance

7. Drag and drop for minimum and maximum scaling instance.

- Click on **Add** to add the new scale rule, as shown in Figure 10.11:

Container Scale

**Scale rule setting**

Control automatic scaling by setting the range of application replicas that'll be deployed in response to a trigger event. Use scale rules to determine the type of events that trigger scaling.

Min / max replicas \* ⓘ

**Scale rule**

**+ Add**

**Create** **< Previous : Container** **Next >**

Figure 10.11: Container App instance scale rule

- Provide the scaling rule name.
- Select the type of scaling, HTTP scaling, Query scaling, and custom scaling.
- Provide the concurrent request and click on **Add**, as shown in Figure 10.12:

**Add scale rule** ×

**Scale rule details**

Rule name \*

Type \* ⓘ  ▼

Concurrent requests

**Add** **Cancel**

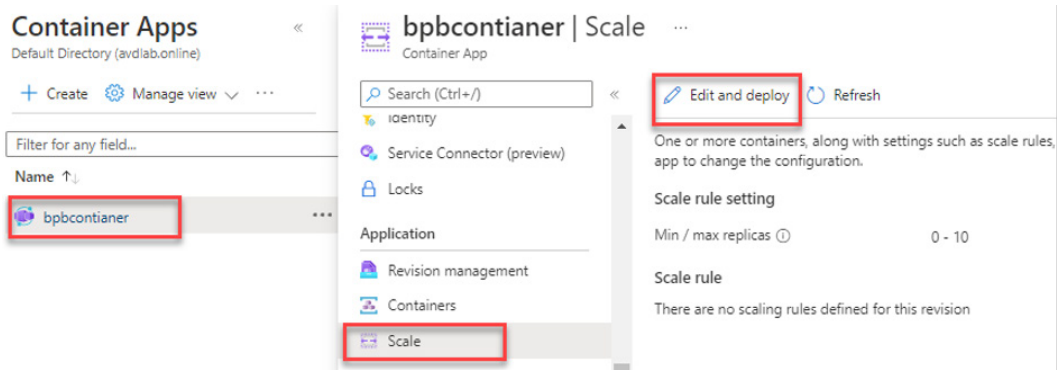
Figure 10.12: Container App instance scale rule setting

## Sizing Container App instance

If you want to configure the Container Sizing for container app instance, follow these steps:

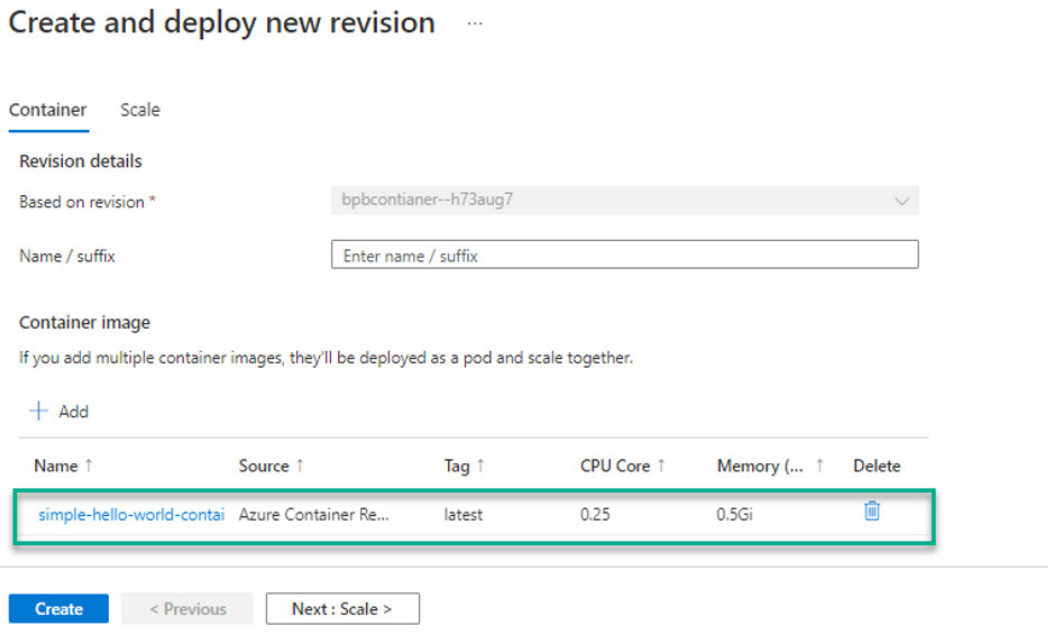
- Search for App container instance and select the app instance.

2. Under the **Application** tab with container property, select the **Scale**.
3. Then click on the **Edit and deploy**, as shown in *Figure 10.13*:



*Figure 10.13: Container App instance Sizing*

4. Click on the **Container Apps**, as shown in *Figure 10.14*:



*Figure 10.14: Container App instance select*

5. Once you will click on the **Container**, the container edit windows will open and you will be able to see all the edited properties of container instance.
6. Go to the **Container resources allocation** tab, as shown in *Figure 10.15* and increase the instance size.

7. Once you change the CPU and RAM, click on the **Save** button to update the changes.
8. You can also change the image source and image type as well.

Refer to *Figure 10.15*:

**Edit a container** [X]

Basics Health probes

**Container details**

You can change these settings after creating the Container App.

Name \* simple-hello-world-container

Image source ☐ Azure Container Registry ☒ Docker Hub or other registries

Image type ☒ Public ☐ Private

Registry login server \* ⓘ mcr.microsoft.com

Image and tag \* azuredocs/containerapps-helloworld:latest

OS type Linux

Command override ⓘ Example: /bin/bash, -c, echo hello; sleep 10...

**Container resource allocation**

CPU Core \* ⓘ 0.25 0.25 - 2 cores

Memory (Gi) \* ⓘ 0.5 Gi 0.1 - 4 Gi

**Environment variables**

+ Add

| Name | Source | Value | Delete |
|------|--------|-------|--------|
|------|--------|-------|--------|

*Figure 10.15: Container App instance Sizing change*

By following the above-mentioned steps, we can configure the scaling of container instance and sizing of container instance.



# Azure Kubernetes

Kubernetes is an open-source portable platform for automatic deployment, scaling, and management of containerized workload. It is managed and orchestrated by the container in difference compute environments. This orchestration platform provides the ease of use and flexibility with PaaS and IaaS environments.

## Creating Azure Kubernetes

To create Azure Kubernetes, follow these steps:

1. Click on **Create a resource**.
2. Search for Kubernetes Service.
3. Select the service and click on **Create**, as shown in *Figure 10.16*:



*Figure 10.16: Kubernetes services*

4. Once you click on create the Kubernetes services, it will ask you to fill the following details:
  - a. Subscription
  - b. Resource group
  - c. Provide the cluster details as follows:
    - i. **Kubernetes cluster name:** Set of node machines called Kubernetes, for running containerized applications.
    - ii. **Region:** The place you want to deploy the services.
    - iii. The version of Kubernetes services you want to deploy.
  - d. **Node:** A node is a physical or virtual machine that depends on the cluster configuration. Provide the node size and node count.
  - e. Check if you might want to add an additional Kubernetes cluster.

Refer to Figure 10.17:

## Create Kubernetes cluster

Basics Node pools Authentication Networking Integrations Tags Review + create

Azure Kubernetes Service (AKS) manages your hosted Kubernetes environment, making it quick and easy to deploy and manage containerized applications without container orchestration expertise. It also eliminates the burden of ongoing operations and maintenance by provisioning, upgrading, and scaling resources on demand, without taking your applications offline. [Learn more about Azure Kubernetes Service](#)

### Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ   
 Resource group \* ⓘ

BPB   
 [Create new](#)

### Cluster details

Kubernetes cluster name \* ⓘ   
 Region \* ⓘ   
 Kubernetes version \* ⓘ

bpbkubernetes   
 (Europe) North Europe   
 1.15.11 (default)

### Primary node pool

The number and size of nodes in the primary node pool in your cluster. For production workloads, at least 3 nodes are recommended for resiliency. For development or test workloads, only one node is required. You will not be able to change the node size after cluster creation, but you will be able to change the number of nodes in your cluster after creation. If you would like additional node pools, you will need to enable the "X" feature on the "Scale" tab which will allow you to add more node pools after creating the cluster. [Learn more about node pools in Azure Kubernetes Service](#)

Node size \* ⓘ   
 Node count \* ⓘ

Standard DS2 v2   
 [Change size](#)

3

[Review + create](#) < Previous Next : Node pools >

Figure 10.17: Kubernetes services details

5. Once you are done with the preceding configuration, go to the **Node pools** section and provide the following details:
  - a. Add the node pool and its instance size with the OS.
  - b. Select the virtual node to be enabled or disabled.

- c. Select the VM scale set to be enabled.
6. Go to the Authentication tab, as shown in *Figure 10.18*:

Basics **Node pools** Authentication Networking Integrations Tags Review + create

**Node pools**

In addition to the required primary node pool configured on the Basics tab, you can also add optional node pools to handle a variety of workloads. [Learn more about multiple node pools](#)

+ Add node pool ...

| Name                                         | OS type | Node count | Node size       |
|----------------------------------------------|---------|------------|-----------------|
| <input type="checkbox"/> agentpool (primary) | Linux   | 3          | Standard_DS2_v2 |

**Virtual nodes**

Virtual nodes allow burstable scaling backed by serverless Azure Container Instances. [Learn more about virtual nodes](#)

Virtual nodes ☐ Disabled ☒ Enabled

**VM scale sets**

Enabling VM scale sets will create a cluster that uses VM scale sets instead of individual virtual machines for the cluster nodes. VM scale sets are required for scenarios including autoscaling, multiple node pools, and Windows support. [Learn more about VM scale sets in AKS](#)

VM scale sets ☐ Disabled ☒ Enabled

**VM scale sets are required for multiple node pools**

[Review + create](#) [< Previous](#) [Next : Authentication >](#)

*Figure 10.18: Kubernetes services node pool*

7. In the **Authentication** tab, select the following details:
  - a. **Select the authentication method:** Service Principal or system-assigned managed identity.
  - b. In Kubernetes authentication and authorization, enable the RBAC role.
  - c. Select the encryption type as default.

8. Click on the **Networking** tab, as shown in *Figure 10.19*:

Basics Node pools **Authentication** Networking Integrations Tags Review + create

**Cluster infrastructure**  
The cluster infrastructure authentication specified is used by Azure Kubernetes Service to manage cloud resources attached to the cluster. This can be either a [service principal](#) or a [system-assigned managed identity](#).

**Authentication method** ☒ Service principal ☐ System-assigned managed identity

**Service principal \***   
[Configure service principal](#)

**Kubernetes authentication and authorization**  
Authentication and authorization are used by the Kubernetes cluster to control user access to the cluster as well as what the user may do once authenticated. [Learn more about Kubernetes authentication](#)

**Role-based access control (RBAC)** ☒ Enabled ☐ Disabled

**Node pool OS disk encryption**  
By default, all disks in AKS are encrypted at rest with Microsoft-managed keys. For additional control over encryption, you can supply your own keys using a disk encryption set backed by an Azure Key Vault. The disk encryption set will be used to encrypt the OS disks for all node pools in the cluster. [Learn more](#)

**Encryption type**

[Review + create](#) [< Previous](#) [Next : Networking >](#)

*Figure 10.19: Kubernetes services authentication*

9. Once you click on the **Networking** tab, provide the following details:

- a. **Select the network configuration:** Basic or Advanced
- b. DNS name prefix
- c. Load balancer
- d. **Private cluster:** Enabled or Disabled
- e. Network policy
- f. **HTTP application routing:** Yes or No

10. Go to the next tab, as shown in *Figure 10.20*:

Basics Node pools Authentication **Networking** Integrations Tags Review + create

You can change networking settings for your cluster, including enabling HTTP application routing and configuring your network using either the 'Basic' or 'Advanced' options:

- **'Basic'** networking creates a new VNet for your cluster using default values.
- **'Advanced'** networking allows clusters to use a new or existing VNet with customizable addresses. Application pods are connected directly to the VNet, which allows for native integration with VNet features.

[Learn more about networking in Azure Kubernetes Service](#)

Network configuration ⓘ ☒ Basic ☐ Advanced

Network settings

DNS name prefix \* ⓘ  ✓

Load balancer ⓘ Standard

Private cluster ⓘ ☐ Enabled ☒ Disabled

Network policy ⓘ ☐ None ☒ Calico ☐ Azure

ⓘ The Azure network policy is not compatible with basic networking.

HTTP application routing ⓘ ☐ Yes ☒ No

[Review + create](#) [< Previous](#) [Next : Integrations >](#)

*Figure 10.20: Kubernetes services networking*

11. Once you click on the **Integrations** tab, select the **Log Analytics workspace** under the Azure Monitor section.

12. Click on the **Next: Tags** button, as shown in *Figure 10.21*:

Basics Node pools Authentication Networking Integrations Tags Review + create

Connect your AKS cluster with additional services.

**Azure Container Registry**  
Connect your cluster to an Azure Container Registry to enable seamless deployments from a private image registry. You can create a new registry or choose one you already have. [Learn more about Azure Container Registry](#)

Container registry: None

**Azure Monitor**  
In addition to the CPU and memory metrics included in AKS by default, you can enable Container Insights for more comprehensive data on the overall performance and health of your cluster. Billing is based on data ingestion and retention settings.  
[Learn more about container performance and health monitoring](#)  
[Learn more about pricing](#)

Container monitoring: ☒ Enabled ☐ Disabled

Log Analytics workspace: DefaultWorkspace-656349f8-c973-4116-bb26-d65042ec51b6-EUS [Create new](#)

**Review + create** < Previous Next: Tags >

*Figure 10.21: Kubernetes services integration*

13. Here, provide the tag name and click on Create the Kubernetes Services. After the validation, click on **Next**, to create the Kubernetes services, as shown in *Figure 10.22*:

✔ Validation passed

Basics
Node pools
Authentication
Networking
Integrations
Tags
Review + create

**Basics**

|                         |                          |
|-------------------------|--------------------------|
| Subscription            | Visual Studio Enterprise |
| Resource group          | BPB                      |
| Region                  | North Europe             |
| Kubernetes cluster name | bpbkunernites            |
| Kubernetes version      | 1.15.11                  |

**Node pools**

|               |          |
|---------------|----------|
| Node pools    | 1        |
| Virtual nodes | Disabled |
| VM scale sets | Enabled  |

**Authentication**

|                                  |                                                          |
|----------------------------------|----------------------------------------------------------|
| Authentication method            | Service principal                                        |
| Role-based access control (RBAC) | Enabled                                                  |
| Encryption type                  | (Default) Encryption at-rest with a platform-managed key |

**Networking**

|                          |                   |
|--------------------------|-------------------|
| Network configuration    | Basic             |
| DNS name prefix          | bpbkunernites-dns |
| Load balancer            | Standard          |
| Private cluster          | Disabled          |
| Network policy           | Calico            |
| HTTP application routing | No                |

**Integrations**

|                         |                                                           |
|-------------------------|-----------------------------------------------------------|
| Container registry      | None                                                      |
| Container monitoring    | Enabled                                                   |
| Log Analytics workspace | DefaultWorkspace-656349f8-c973-4116-bb26-d65042ec51b6-EUS |

**Tags**  
 (none)

Create

< Previous

Next >

[Download a template for automation](#)

*Figure 10.22: Kubernetes services creation*

It will take 10 to 15 mins to create the Kubernetes services. After this, we will be able to use the services as per our requirements.

## Configure Scaling for AKS

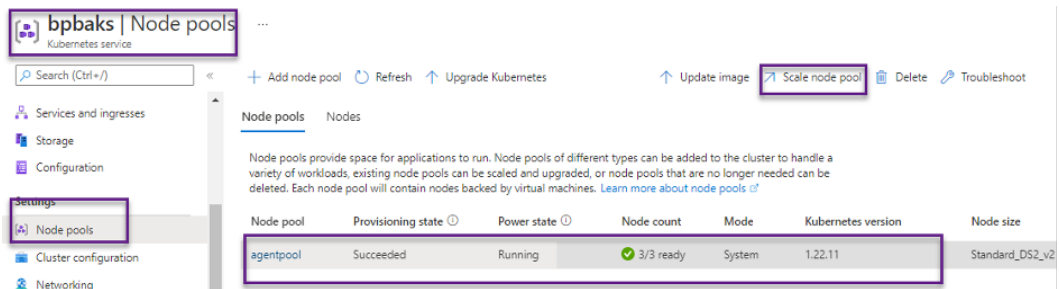
Scaling will help meet the changing application demand based on the workloads or traffic demands to application.

Cluster auto-scalers watch for pods and cannot schedule the on-nodes because of node resource constrain. In such a scenario, cluster will automatically increase the nodes.

Horizontal pod auto-scalers use the matrix server over Kubernetes cluster to monitor the resource demands of pod. If the application needs more resources, then it will automatically increase the nodes to meet the demand.

After creating the AKS cluster, if you want to change the scaling for Nodes, follow these steps for the same:

1. Go to the AKS cluster.
2. Under setting select the **Node pools**.
3. Select the scale node pool, as shown in *Figure 10.23*:



*Figure 10.23: Kubernetes services Scaling*

4. After clicking on scale node, scale modification window will open.
5. You can change the scaling of AKS either to manual or automatic, based on the client requirements. Refer to *Figure 10.24*:



**Scale node pool**  
agentpool

You can scale the number of nodes in your cluster to increase the total amount of cores and memory available for your container applications. [Learn more](#)

Scale method ☒ Manual ☐ Autoscale - Recommended

*This option is recommended so that the cluster is automatically sized correctly for the current running workloads.*

Node count

**Node pool capacity**

|                      |                                         |
|----------------------|-----------------------------------------|
| Virtual machine size | Standard DS2 v2 (2 vcpus, 7 GiB memory) |
| Cores                | 6 vCPUs                                 |
| Memory               | 21 GiB                                  |

Usage

*The metrics included here are intended to provide context regarding scaling. To view all cluster metrics, including node pool metrics, go to the cluster [metrics view](#).*

**Apply** Cancel

Figure 10.24: Kubernetes services scaling option

## Upgrade the AKS Cluster

To upgrade the AKS Cluster, follow these steps:

1. Go to the AKS cluster.
2. Under setting, select the **Cluster configuration**.
3. Then select **Upgrade version**, as shown in Figure 10.25:

**bpbaks | Cluster configuration** ...  
Kubernetes service

Search (Ctrl+/) Save Discard Troubleshoot

**Upgrade**  
You can upgrade your cluster to a newer version of Kubernetes or configure automatic upgrade settings. If you upgrade your cluster, you only the control plane or to also upgrade all node pools. To upgrade individual node pools, go to the 'Node pools' menu item instead.  
[Learn more about upgrading your AKS cluster](#)  
[View the Kubernetes changelog](#)

Kubernetes version **1.22.11** **Upgrade version**

API server availability ☒ 99.95% Optimize for availability. ☐ 99.5% Optimize for cost.

Enable secret store CSI driver ☐

**Cluster configuration**

- Namespaces
- Workloads
- Services and ingresses
- Storage
- Configuration
- Settings
  - Node pools
  - Cluster configuration**
  - Networking
  - Open Service Mesh

Figure 10.25: Kubernetes services Upgrade version

4. Check the upgrade version. If you find the older version, then you can choose to upgrade to a newer version. However, to do that, you have to complete all the prerequisites and make sure that you have backup of your application data before applying the changes for the updated Kubernetes.

Take a look at *Figure 10.26*:

## Upgrade Kubernetes version



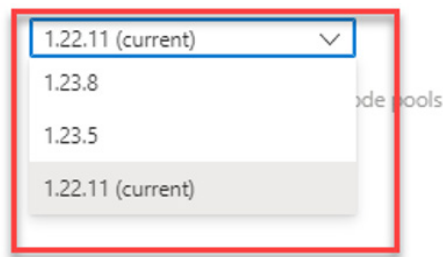
You can upgrade your cluster to a newer version of Kubernetes or configure automatic upgrade settings. If you upgrade your cluster, you can choose whether to upgrade only the control plane or to also upgrade all node pools. To upgrade individual node pools, go to the 'Node pools' menu item instead.

[Learn more about upgrading your AKS cluster](#)

[View the Kubernetes changelog](#)

Kubernetes version ⓘ

Upgrade scope ⓘ



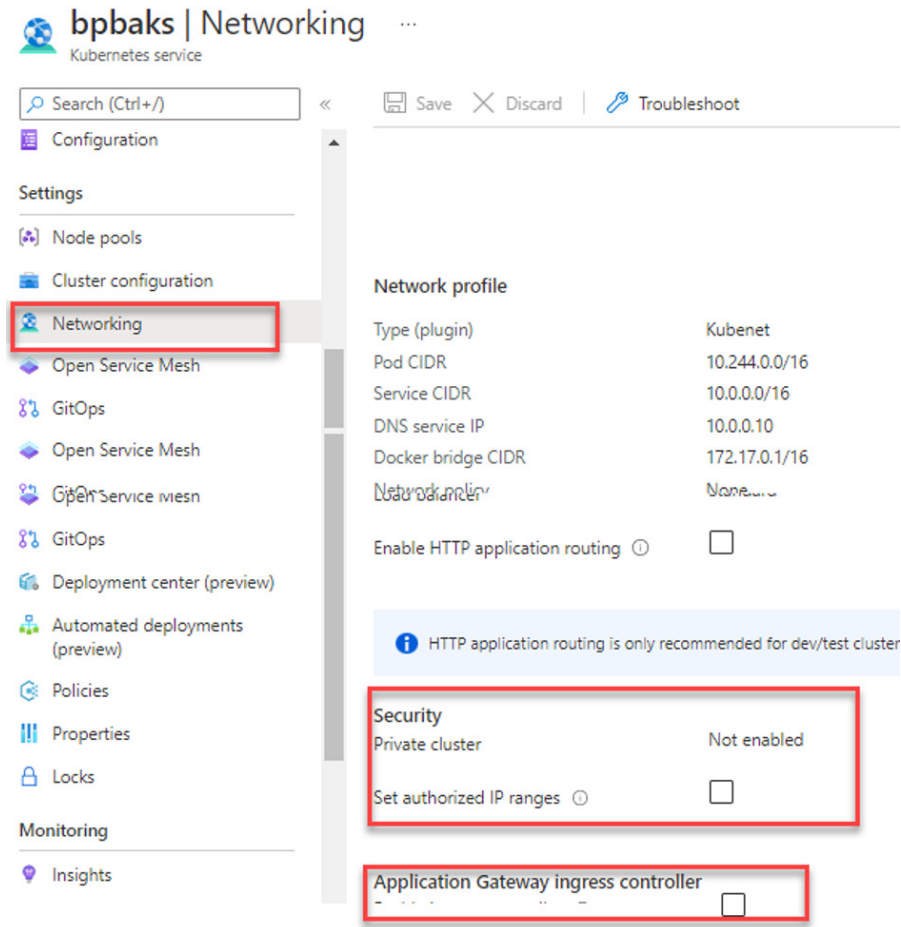
*Figure 10.26: Kubernetes services Various version*

## Configure network connecting for AKS

If you want to configure application gateway or specific IP address for network connection, which further connects to AKS for ingress traffic, follow these steps:

1. Under **Setting**, select **Networking**.
2. Then select the security check box and set authorized IP ranges, that you want to allow to connect privately.
3. If you want to enable the application gateway for ingress traffic, select the **Application Gateway ingress controller**. Then select the existing application gateway or create a new application gateway for the same.

Refer to *Figure 10.27*:



*Figure 10.27: Kubernetes services networking*

## Conclusion

In this chapter, we discussed the creation and configuration of Azure Container and Kubernetes. We also covered the Kubernetes resources, how to set up and configure the container and Kubernetes, and how it will help you and the customer manage the larger applications. We have also learned the Kubernetes networking, scaling, and upgrading the Kubernetes clusters. Even for customers, we have set the scaling and size changing option and it is helping to meet the application demand and provide the high availability for the same.

In the next chapter, we will discuss Azure app services and see how to create and deploy the app services in your Azure environments. We will also discuss the

configuration part on Web Apps which will help you to learn the Web Apps services more easily.

## Points to remember

- Container provides lightweight and immutable infrastructure for packaging the application and deployment.
- Scaling and sizing can be configured in app container, by going to the scale tab, and clicking on edit.
- AKS cluster can be upgraded from cluster configuration tab under settings.
- Container resources allocation is used to configure from app setting, while creating the container services.
- Application gateway ingress traffic for AKS can be enabled under setting, and then selecting the networking tab.

## Multiple choice questions

1. **What is Node Pool in Kubernetes?**
  - a. Collection of virtual machines.
  - b. Collection of network resources.
  - c. Collection of Azure storage.
2. **How to upgrade the Kubernetes version?**
  - a. From the Kubernetes cluster configuration.
  - b. Using the node pool configuration.
  - c. While selecting the configuration.

## Answers

1. a
2. a

# CHAPTER 11

# Creating and Configuring Web Apps

## Introduction

In this chapter, we will discuss the benefits of Azure app services, creating the app services, and configuring the app services plan. We will also discuss the Azure apps services components and how to use the web apps slot and custom domain configuration. We will then discuss how to secure your Azure web apps.

We are also covering scaling plan, network services integration and deployment slot stuff. For app services, backup is really important, and we will be walking through how you can take the backup of app services as well.

## Structure

The following topics will be covered in this chapter:

- App services
  - App services plan
- Create and configure app services
  - Custom domain configuration
  - App services security

- Configure network setting of app services
- App service backup
- Configure scaling setting in an app service plan
- Configure deployment slots

## Objectives

By the end of this chapter, the reader will know about the Azure app services and its use cases. We will also discuss the properties of its app services and see how to create and configure the app services using the Azure portal, so that the customer can utilize the Azure app services based on their requirements.

## App services

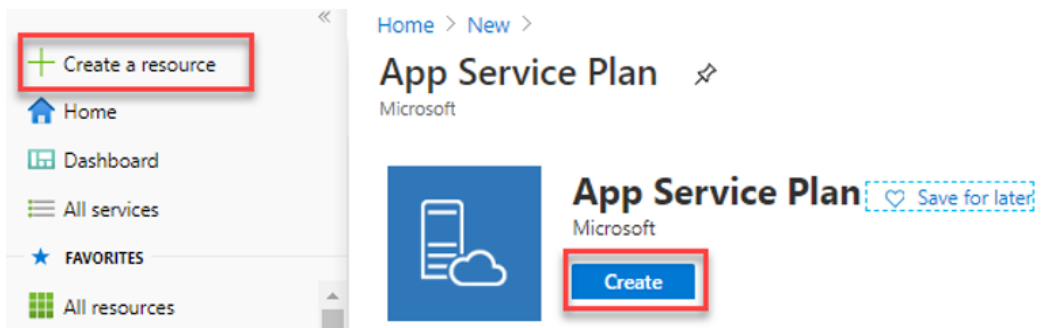
Azure app services are HTTP-based services which are used to host the application, similar to your on-premises IIS server. We can develop our application using .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python language. The app services automatically manage the patches, OS, and language framework.

## App services plan

The app services plan defines the SKU / size of the Azure app services instance, based on the app services plan. You will be able to utilize features like custom domain, VNet-integration, load balancing, and size of app services, such as 2 GB and 100 ACU, and so on.

To create the app services plan, follow these steps:

1. Click on the **+ Create a resource** option.
2. Search for **App Service Plan**.
3. Click on **Create**, as shown in *Figure 11.1*:



*Figure 11.1: App service plan*

Now that the app services plan is created, let us see how many plans we have in app services and their usage:

- **Shared compute:** In this plan, you will get the free apps services plan as well as the shared services plan, which can be used for the *dev/test* purpose, as shown in *Table 11.1*:

| Selected features        | Free | Shared |
|--------------------------|------|--------|
| Web, mobile, or API apps | 10   | 100    |
| Disk space               | 1 GB | 1 GB   |
| Auto scale               | NA   | NA     |
| Deployment slots         | NA   | NA     |
| Max instances            | NA   | NA     |

*Table 11.1: Web services shared plan*

- **Dedicated compute:** It is used for production purpose. In this plan, we get a **basic**, **standard**, **premium**, and **premium V2** tier. This can be seen in *Table 11.2*:

| Selected features        | Basic     | Standard  | Premium   |
|--------------------------|-----------|-----------|-----------|
| Web, mobile, or API apps | Unlimited | Unlimited | Unlimited |
| Disk space               | 10 GB     | 50 GB     | 250 GB    |
| Auto scale               | NA        | Supported | Supported |
| Deployment slots         | NA        | 5         | 20        |
| Max instances            | Up to 3   | Up to 10  | Up to 30  |

*Table 11.2: Web services dedicated plan*

- **Isolated compute:** This plan will provide the dedicated VM instance, which is integrated with the dedicated VNet. It provides complete isolation as well. Take a look *Table 11.3*:

| Selected features        | Isolated  |
|--------------------------|-----------|
| Web, mobile, or API apps | Unlimited |
| Disk space               | 1 TB      |
| Auto scale               | Supported |
| Deployment slots         | 20        |
| Max instances            | Up to 100 |

*Table 11.3: Web services isolated plans*

Refer to Figure 11.2:

**Dev / Test**  
For less demanding workloads

**Production**  
For most production workloads

**Isolated**  
Advanced networking and scale

**Recommended pricing tiers**

| Tier        | Resources                                                       | Price (Estimated)  |
|-------------|-----------------------------------------------------------------|--------------------|
| <b>S1</b>   | 100 total ACU<br>1.75 GB memory<br>A-Series compute equivalent  | 2895.02 INR/Month  |
| <b>P1V2</b> | 210 total ACU<br>3.5 GB memory<br>Dv2-Series compute equivalent | 9650.05 INR/Month  |
| <b>P2V2</b> | 420 total ACU<br>7 GB memory<br>Dv2-Series compute equivalent   | 19300.10 INR/Month |
| <b>P3V2</b> | 840 total ACU<br>14 GB memory<br>Dv2-Series compute equivalent  | 38600.21 INR/Month |

[See additional options](#)

**Included features**  
Every app hosted on this App Service plan will have access to these features:

- Custom domains / SSL**  
Configure and purchase custom domains with SNI and IP SSL bindings.
- Auto scale**  
Up to 10 instances. Subject to availability.
- Staging slots**  
Up to 5 staging slots to use for testing and deployments before swapping them into production.
- Daily backups**  
Backup your app 10 times daily.
- Traffic manager**  
Improve performance and availability by routing traffic between multiple instances of your app.

**Included hardware**  
Every instance of your App Service plan will include the following hardware configuration:

- Azure Compute Units (ACU)**  
Dedicated compute resources used to run applications deployed in the App Service Plan. [Learn more](#)
- Memory**  
Memory per instance available to run applications deployed and running in the App Service plan.
- Storage**  
50 GB disk storage shared by all apps deployed in the App Service plan.

Figure 11.2: App services plan size

Once you click on **Create app service**, follow the given steps:

1. Select the resource group.
2. Provide the name of the app service.
3. Select the OS: **Windows** / **Linux**, as per your requirements.
4. Click on **Review + create**, as shown in Figure 11.3:



## Create App Service Plan

App Service plans give you the flexibility to allocate specific apps to a given set of resources and further optimize your Azure resource utilization. This way, if you want to save money on your testing environment you can share a plan across multiple apps. [Learn more](#)

### Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource Group \* ⓘ  [Create new](#)

**App Service Plan details**

Name \*  ✓

Operating System \* ☐ Linux ☒ Windows

Region \*

### Pricing Tier

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. [Learn more](#)

Sku and size \* **Standard S1**  
100 total ACU, 1.75 GB memory  
[Change size](#)

[Review + create](#) < Previous Next : Tags >

Figure 11.3: App service plan creation

Once you click on **Review + create**, your app service plan will be created in 5 to 10 minutes.

## Create and configure app services

Let us now create the app services, since we have already created and understood the app services plan. To do this, follow the given steps:

1. Click on **+ Create a resource**.
2. Search for Azure app services.

3. Click on **Web App**, as shown in Figure 11.4:

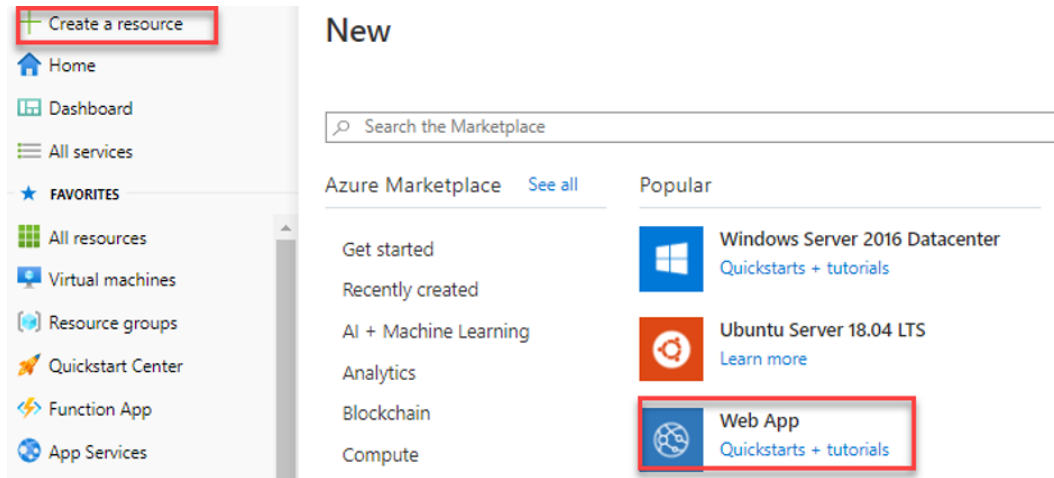


Figure 11.4: Web app

4. Once you click on **Web App**, provide the following details to create the new app services:
  - a. Subscription.
  - b. Resource group.
  - c. Provide the name of the instance.
  - d. Publish can be **Code** or **Docker Container** as per your customer/project requirements.
5. Select the runtime stack as. **.NET CORE 3.1 (LTS)**.
6. Select the OS. It can be either **Windows** or **Linux**.
7. Select the region.

8. Click on windows size or **App Service Plan** in app services. Take a look at *Figure 11.5*:

### Create Web App

[Basics](#) [Monitoring](#) [Tags](#) [Review + create](#)

App Service Web Apps lets you quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. Meet rigorous performance, scalability, security and compliance requirements while using a fully managed platform to perform infrastructure maintenance. [Learn more](#)

#### Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*  ⓘ [Subscription] ▼

Resource Group \*  ⓘ BPB ▼  
[Create new](#)

#### Instance Details

Name \* bpb4 ✓ .azurewebsites.net

Publish \* ☒ Code ☐ Docker Container

Runtime stack \* .NET Core 3.1 (LTS) ▼

Operating System \* ☐ Linux ☒ Windows

Region \* East US ▼  
 ⓘ Not finding your App Service Plan? Try a different region.

#### App Service Plan

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. [Learn more](#)

Windows Plan (East US) \*  ⓘ (New) ASP-BPB-a83f ▼  
[Create new](#)

Sku and size \* **Standard S1**  
100 total ACU, 1.75 GB memory  
[Change size](#)

Review + create
< Previous
Next : Monitoring >

*Figure 11.5: Web app details*

9. Click on **Next: Monitoring >** and select the **Monitoring** tab. Create a new application insight for monitoring of app services.

10. Once this is done, click on **Review + create**, and after 10 minutes, your app services will be created. Take a look at *Figure 11.6*:

Basics **Monitoring** Tags Review + create

Application Insights is a code-less attach to provide detailed observability in to your application. [Learn more](#)

Application Insights

Enable Application Insights \* ☐ No ☒ Yes

Application Insights \* (New) bpb4 (East US) [Create new](#)

Region East US

**Review + create** < Previous Next : Tags >

*Figure 11.6: Web app creation*

## Custom domain configuration

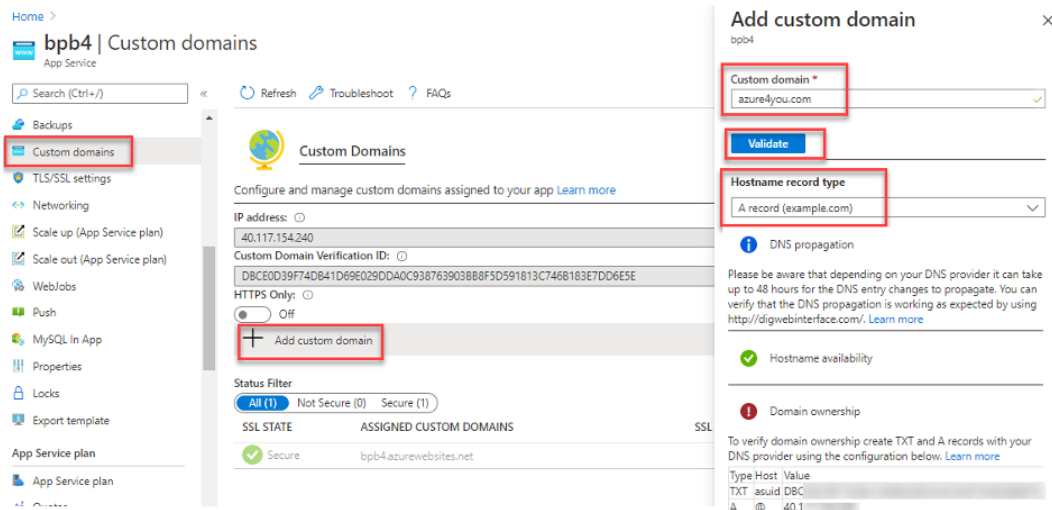
A custom domain is used to configure your own custom domain for your web apps. For example, if you want to configure the *xyz.com* to *bpb.com*, then you need to configure the custom domain.

Let us configure the custom domain for app services. Follow the given steps:

1. Go to **App Service**.
2. Click on **Custom domains**.
3. Click on **+ Add custom domain**.
4. Provide the custom domain name.
5. Click on the **Validate** button.

Once you click on **Validate**, add the *A record* and *TXT record* in your public domain registration to validate, and then try to validate the same.

Once the validation is done, you can configure the Azure web apps services. Take a look at the *Figure 11.7*:

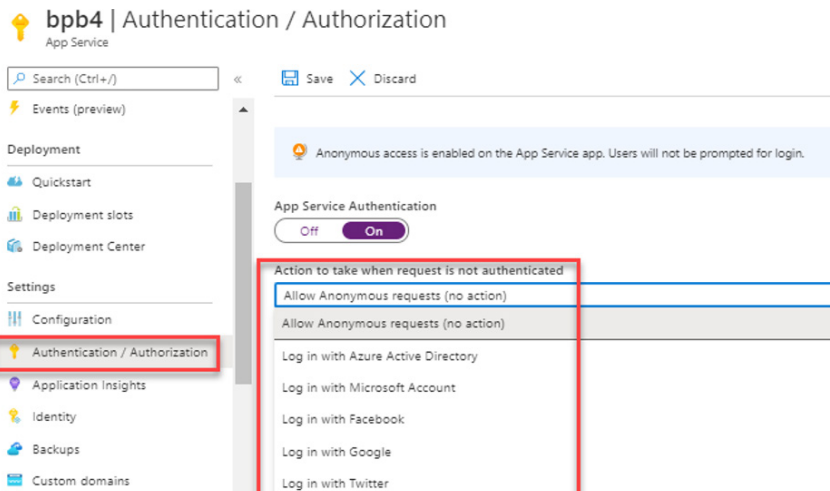


*Figure 11.7: Custom domain*

## App Services Security

### Authentication

The app services security will help you reduce the attack and enable the authentication to your web apps for your users. For example, you can integrate it with Azure AD, Facebook, Microsoft account, Google, and Twitter account. For more details, take a look at *Figure 11.8*:



*Figure 11.8: Authentication*

## TLS/SSL Configuration

We can even enable the **Transport Layer Security (TLS)** to services and add the TLS/SSL certificate binding, for the HTTPS configuration under the TLS/SSL settings configuration.

- **TLS:** It stands for **Transport Layer Security**, which is designed to provide the privacy and data security of communication over the internet.
- **SSL:** It is a **Secure Socket Layer** that helps to protect the connection between the server and client while encrypting the link. The examples include websites, main servers, browsers, and so on. Take a look at *Figure 11.9*:

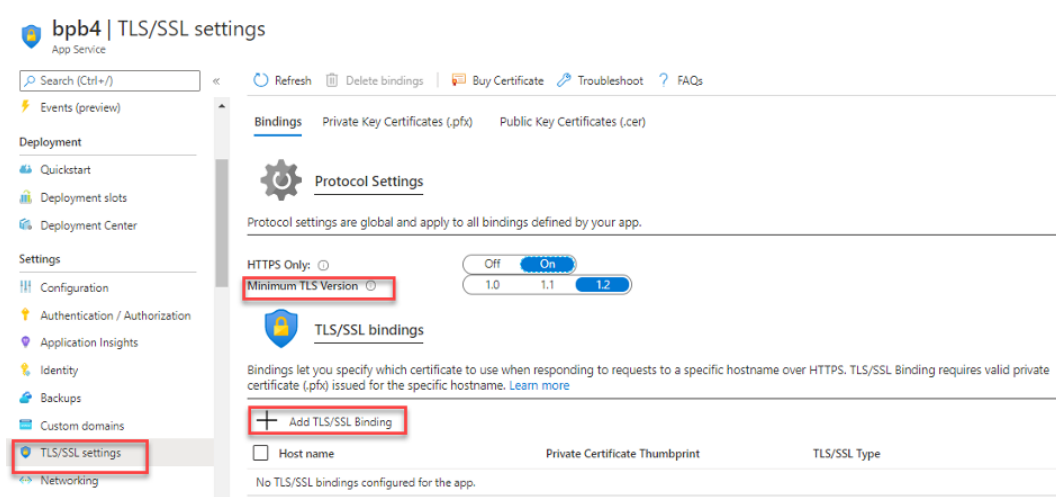


Figure 11.9: TLS/SSL settings

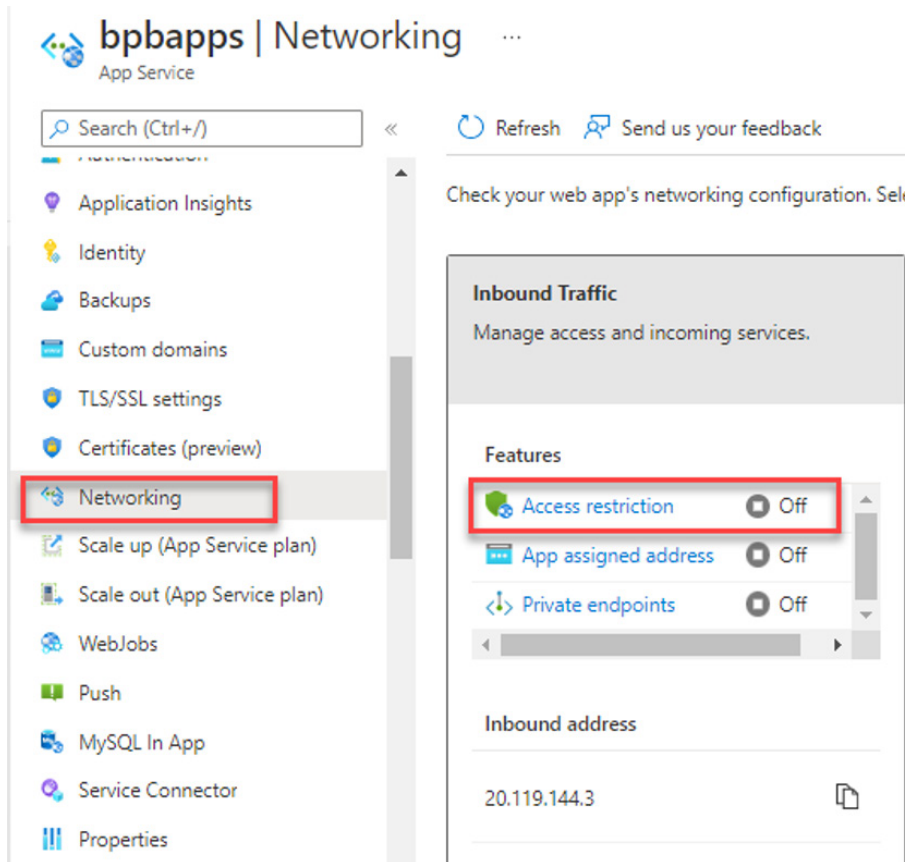
## Configure network setting of app services

We want to secure the app services and only then will networking play a very important role in it. We can enable the private endpoint and app assign address for ingress traffic. For egress traffic, we can integrate the VPN and hybrid connection. That is how we can secure in and out traffic for app services.

To enable the networking, follow these steps:

1. To enable the access restriction, you can go to the networking tab under settings.
2. Click on the **Access restriction**.

Refer to *Figure 11.10*:



*Figure 11.10: Access restriction*

3. Once you click on the **Access restriction**, click on **Add rule**. The **Rule** tab will open in new windows.
4. Provide the rule name based on your organization standard.
5. Select the section to allow or deny.
6. Mention the priority.
7. Provide the description and IPv4.
8. Provide the Source setting IP type and other http headers setting if required, and click on **Add rule**.
9. Once you will add those rules, it will allow only specific IP address as per your rule.

Refer to Figure 11.11:

**Access Restrictions**

Access restrictions allow you to define lists of allow/deny rules to control address. [Learn more](#)

**Add rule**

**General settings**

Name: Allow ✓

Action: **Allow** Deny

Priority: 301 ✓

Description: allow access ✓

**Source settings**

Type: IPv4 ✓

IP Address Block: 10.0.0.0/24 ✓

**HTTP headers filter settings**

X-Forwarded-Host: Ex. exampleOne.com, exampleTwo.com

X-Forwarded-For:

| Priority | Name      | Source |
|----------|-----------|--------|
| 1        | Allow all | Any    |

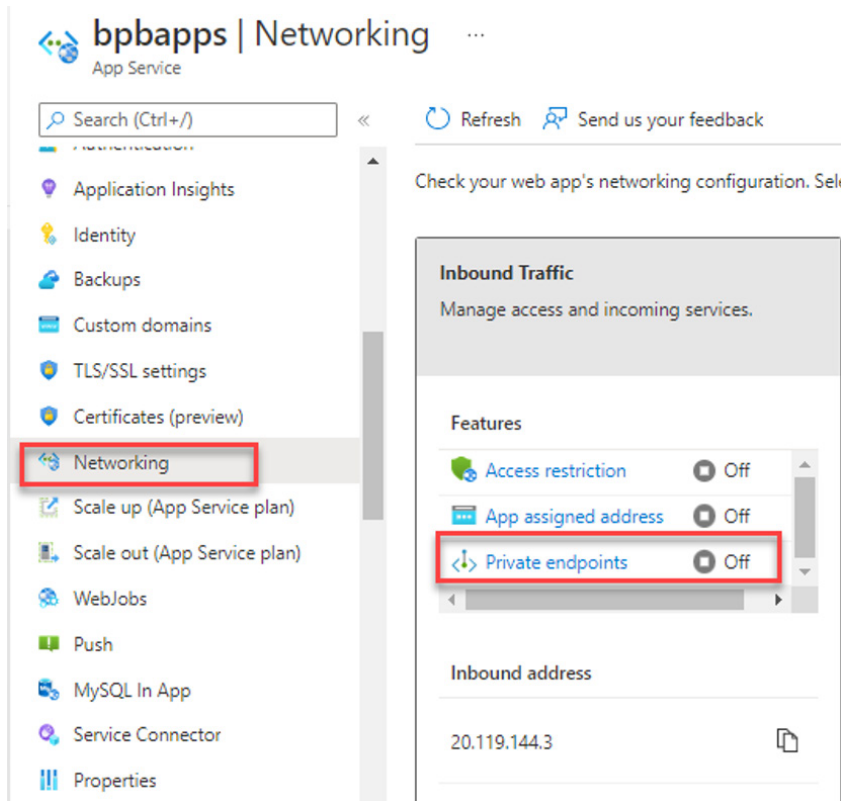
Figure 11.11: Access restriction configuration

Once this is done, we can work on enabling the Private endpoint for apps services, which will allow a one-way ingress communication to connect app services securely. Follow these steps to enable the private endpoint:

1. To enable the Private endpoint, you can go to the **Networking** tab under settings.
2. Click on **Private endpoints**.
3. Once you will click on **Private endpoints**, it will open new window.



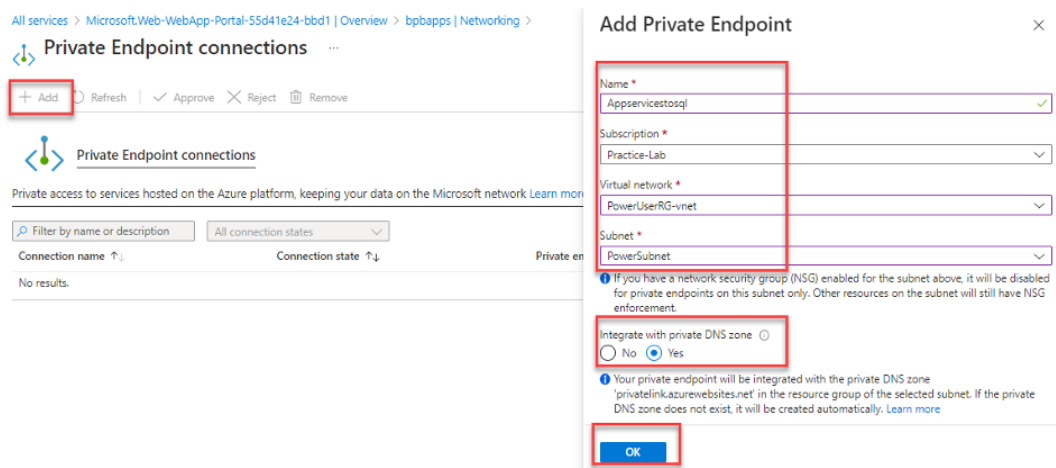
Refer to *Figure 11.12*:



*Figure 11.12: Private endpoint*

4. Provide the private endpoint name, Subscription details, VNet Name and subnet name.
5. Provide the DNS integration as shown in *Figure 11.13*. You can choose your own DNS as well and update the DNS address under VNet.
6. Once these steps are completed, click on **OK**, to add the VNet integration for the same.

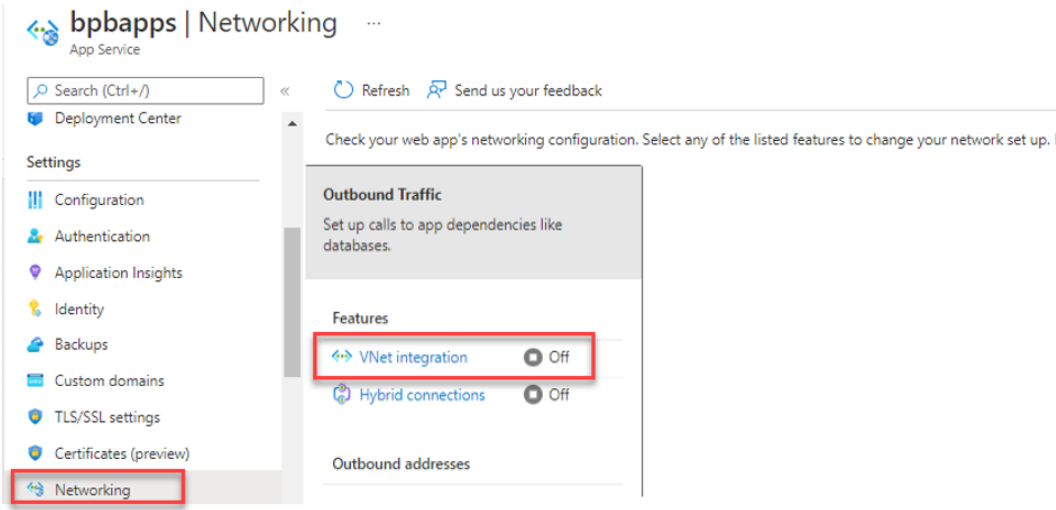
Refer to *Figure 11.13*:



*Figure 11.13: Private endpoint configuration*

For outbound access, we need to integrate the VNet or hybrid connection, so that the app services can connect to internet or can access publicly. To ensure that this is possible, follow these steps:

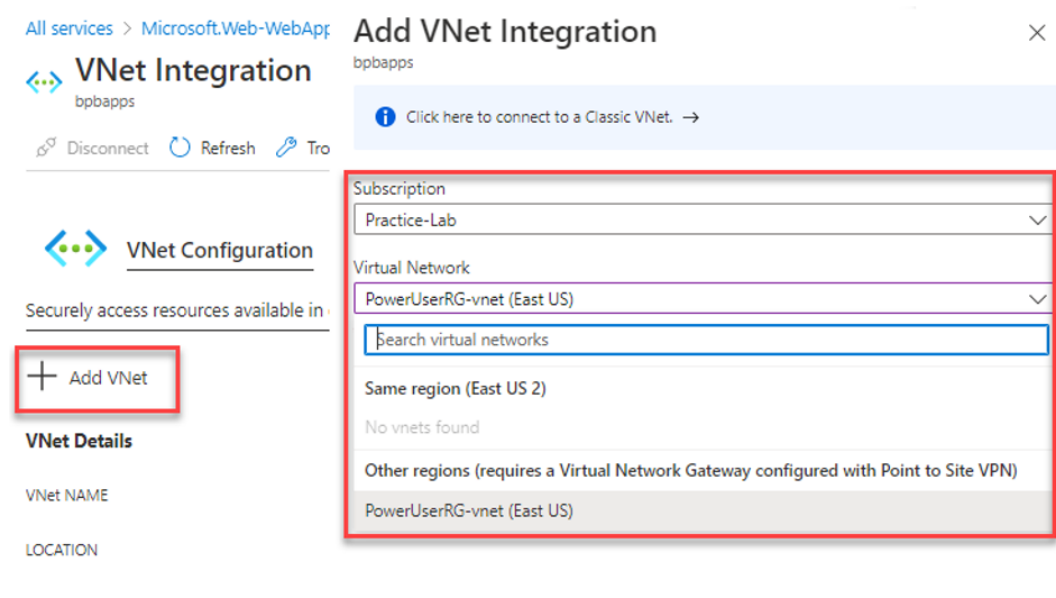
1. To enable the Virtual network, you can go to the **Networking** tab under **Settings**.
2. Click on the **Virtual Network**.
3. This will open a new window, as shown in *Figure 11.14*:



*Figure 11.14: VNet Integration*

4. Click on **Add VNet** integration. This will open a new tab.
5. Provide the Subscription name.
6. Provide the virtual network name which has VNet gateway integration. Otherwise, it will not allow to configure the same.
7. Click on **Ok**.

Refer to *Figure 11.15*:



*Figure 11.15: VNet Integration configuration*

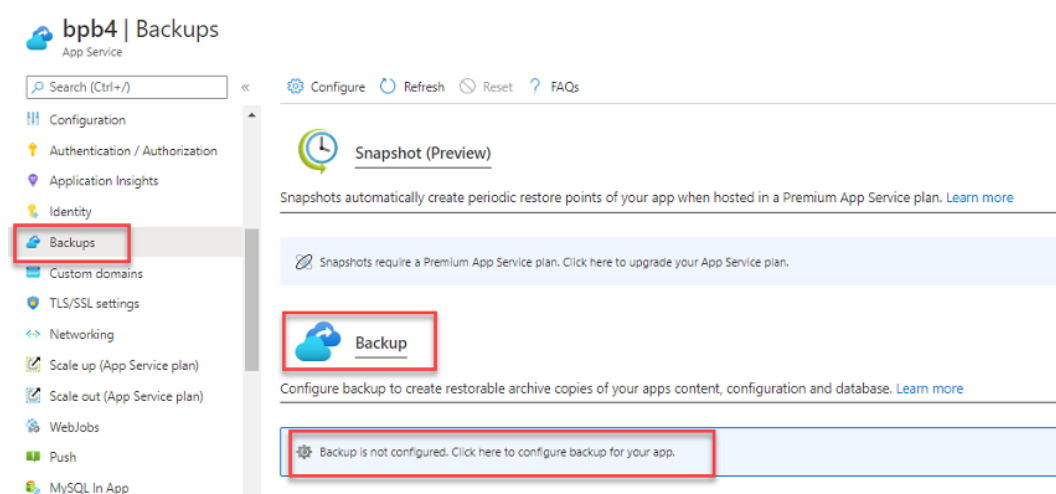
Once the vent configuration is added, you can access the app services publicly.

## App services backup

If you need to enable the backup of Azure app services, it cannot be done directly from the **backup vault**. However, the app services can use the backup vault with their configuration. Follow the given steps to configure the app services backup:

1. Go to **App Service**.
2. Click on the **Backups** option.

3. Click on **Backup** to configure, as highlighted in *Figure 11.16*:



*Figure 11.16: App backup*

4. Click on the **Storage** tab and select the storage account for backup.
5. Select the **On** button for enabling the backup.
6. Set up the backup frequency.
7. Mention the backup schedule start.
8. Select the retention period.
9. Click on the **Save** button, and your app services backup will be enabled. Take a look at *Figure 11.17* for more details:

## Backup Configuration


**Backup Storage**

Select the target container to store your app backup.

Storage Settings

bpbcontainer


**Backup Schedule**

Configure the schedule for your app backup.

Scheduled backup ☒ On ☐ Off

Backup Every \*  Days Hours

Start backup schedule from \*    
 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Retention (Days) \*  ⓘ

Keep at least one backup ☐ No ☒ Yes


**Backup Database**

Select the databases to include with your backup. The backup database list is based on the app's configured connection strings. Note: The maximum size of content and growing, use Azure Backup for database backup instead.

| <input type="checkbox"/> Include in Backup                                             | Connection String Name | Database |
|----------------------------------------------------------------------------------------|------------------------|----------|
| No supported connection strings of type SQL Database or MySQL found configured in app. |                        |          |

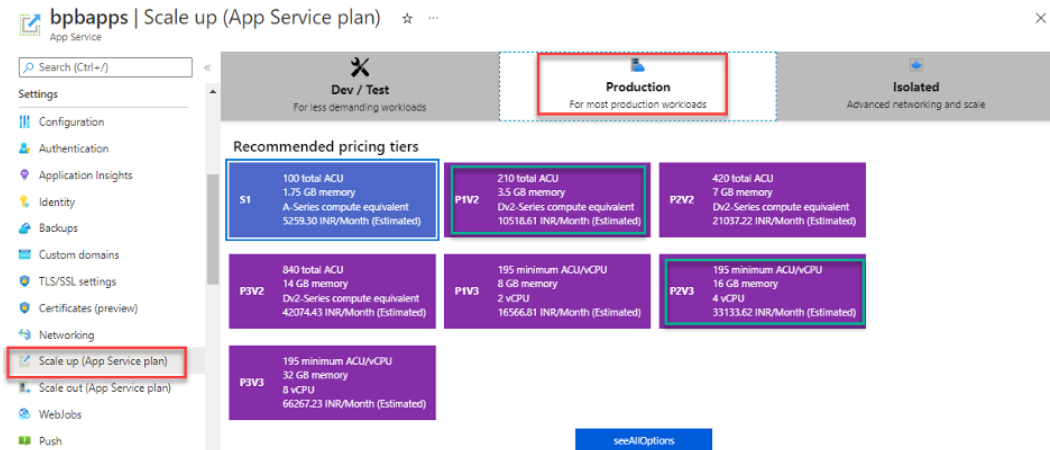
Figure 11.17: App backup configure

## Configure scaling setting in an App Service plan

App services scaling plans help you to upgrade the app services plan in terms of CPU, RAM, and so on, using scale up plan, and can scale up the instance based on the scale out plan. Follow the given steps:

1. Select the app services, and under **Settings**, click on **Scale up** plan. This will open a new window.
2. Select the appropriate plan based on your requirements.
3. There are 3 plans: Dev / test, Production and Isolated.
4. Once you choose one and select the plan, click **Ok**. You can upgrade or downgrade the app services plan based on your customer requirements.

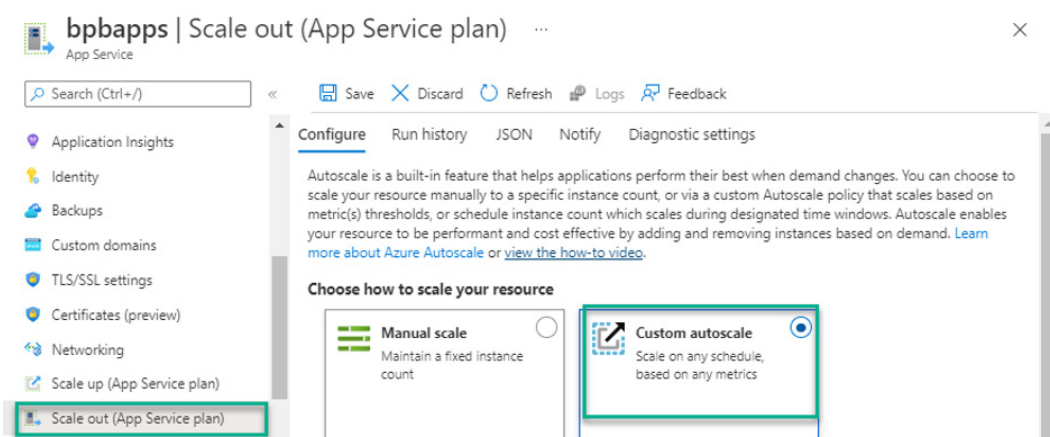
Take a look at *Figure 11.18*:



*Figure 11.18: App Scale up plan*

Now, let us configure the scale out plan with the custom auto scale configuration, which will help to meet the application demand. Based on consumption it could either be CPU, https queue length, data in and out, memory percentage, and so on. You can choose another configuration based on the metric as well. Follow these steps to perform scale out configurations:

1. Choose the appropriate app services you want to configure scale out on.
2. Click on **Scale out** option under settings, with app services configuration.
3. Select the **Custom autoscale** option to process further.
4. You can also check the run history and notify the admin while selecting appropriate tabs, mentioned in *Figure 11.19*:



*Figure 11.19: App Scale out plan*

5. Provide the autoscaling setting name.
6. Select the appropriate resource group name.
7. In Auto create scale condition, click on edit and select the scale mode to scale, based on the metric.
8. Click on **Add rules**, as shown in *Figure 11.20*, and select the appropriate metric configurations:

**Scale rule** [X]

Metric source  
Current resource (ASP-bpb-a4ad)

Resource type: App Service plans | Resource: ASP-bpb-a4ad

☒ Criteria

Time aggregation \* ⓘ  
Average

Metric namespace \* | Metric name  
App Service plans standard metrics | CPU Percentage

Dimension Name  
Instance

If you select multiple values for a dimension, the rule will evaluate the metric for each selected value, not evaluate the metric for the dimension.

80%  
60%  
40%  
20%  
0%

**Add**

*Figure 11.20: App Scale rule*

9. Once you will add the scale rule, click on **Add Rule**. You can add the multiple condition for scale out plan. Select the instance count to scale out instance limit.
10. App instance count will increase or decrease, based on the metric rule conditions which you have put in the rule.
11. Click on **Save**, and after some time, the configuration will be saved.

Refer to Figure 11.21:

Save Discard Refresh Logs Feedback

**Configure** Run history JSON Notify Diagnostic settings

Autoscale is a built-in feature that helps applications perform their best when demand changes. You can choose to scale your resource manually to a specific instance count, or via a custom Autoscale policy that scales based on metric(s) thresholds, or schedule instance count which scales during designated time windows. Autoscale enables your resource to be performant and cost effective by adding and removing instances based on demand. [Learn more about Azure Autoscale](#) or [view the how-to video](#).

**Choose how to scale your resource**

**Manual scale**  
Maintain a fixed instance count

**Custom autoscale**  
Scale on any schedule, based on any metrics

Custom autoscale

Autoscale setting name \* ASP-bpb-a4ad-Autoscale-111

Resource group bpb

Instance count 1

**Default** Auto created scale condition

Delete warning

Scale mode

Rules

Instance limits

Schedule

+ Add a scale condition

The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale is based on a metric

Scale to a specific instance count

Scale is based on metric trigger rules but no rule(s) is defined; click **Add a rule** to create a rule. For example: 'Add a rule that increases instance count by 1 when CPU Percentage is above 70%'. If no rules is defined, the resource will be set to default instance count.

Minimum 1

Maximum 1

Default 1

This scale condition is executed when none of the other scale condition(s) match

Figure 11.21: App Scale rule

Now that we have learned how to configure the scale up and scale out with app services, make sure to test them out in your own subscription.



## Configure deployment slots

Deployment slots will help configure your apps in staging environments, while also providing the feature to rollback or swap between production environments apps. Let us consider a scenario where you have an app which you want to upgrade to a newer version but cannot deploy the code directly to the production. In such a case, you need similar environments where deployment slots will help to create the same app, and route some of the traffic (around 30 or 70%) to standing apps and understand the behaviours of the apps.

This way it helps you provide the success test and enable the better testing of apps. Moreover, without any additional configuration, you can swap between staging/testing/dev apps to production.

Take a look at *Table 11.4*:

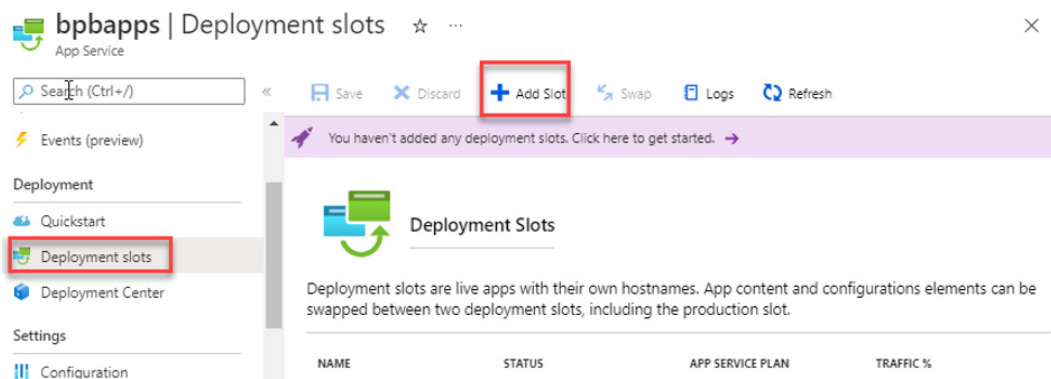
| Deployment Slot Limitation                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| App settings that are swapped supported                                                                                                                                                                                                                                                                                                                                                             | App settings swapped not supported                                                                                                                                                                                                                                                                                                                                                                 |
| <p>General settings, such as framework version, 32/64-bit, web sockets.</p> <p>App settings (can be configured to stick to a slot)</p> <p>Connection strings (can be configured to stick to a slot).</p> <p>Handler mappings</p> <p>Public certificates</p> <p>WebJobs content</p> <p>Hybrid connections*</p> <p>Service endpoints*</p> <p>Azure Content Delivery Network*</p> <p>Path mappings</p> | <p>Publishing endpoints</p> <p>Custom domain names</p> <p>Non-public certificates and TLS/SSL settings</p> <p>Scale settings</p> <p>WebJobs schedulers</p> <p>IP restrictions</p> <p>Always On</p> <p>Diagnostic settings</p> <p>Cross-origin resource sharing (CORS)</p> <p>Virtual network integration</p> <p>Managed identities</p> <p>Settings that end with the suffix _EXTENSION_VERSION</p> |

*Table 11.4: Web services isolated plans*

Let us now configure the deployment within the apps services and see how that works. Follow these steps:

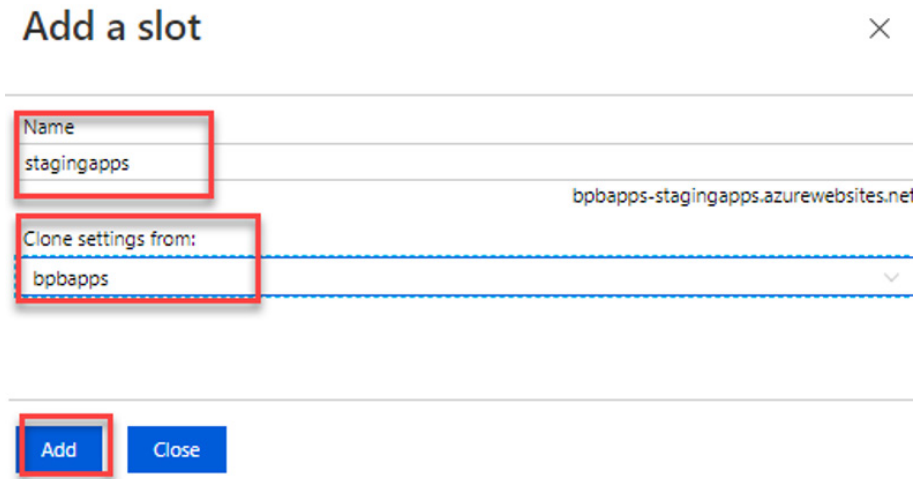
1. Select the appropriate app services and under deployment, click on **Deployment slots**.

2. Now click on **Add Slot**, as shown in *Figure 11.22*:



*Figure 11.22: App deployment slot*

3. Once you will click on the add slot, another slot will open. Provide the ame, and also the clone setting – you can either select the existing app or create a new one. In *Figure 11.23*, we are creating one with an existing app:



*Figure 11.23: App deployment slot configuration*

4. If you want to transfer the traffic to staging app deployment that you have created recently, select the staging app and put the percentage in the box.
5. In *Figure 11.24*, we only transfer the 20% traffic. You can see that the traffic has been reduced from production, and that it now has only 80% going to production environments.
6. Once the above-mentioned steps are completed, click on the **Swap** option, as shown in *Figure 11.24*:

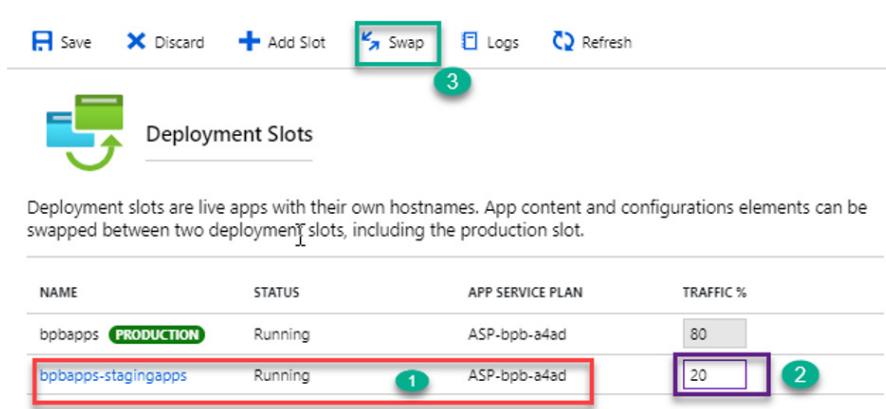


Figure 11.24: App deployment slot swap

- Now you can see that the swap option has popped up in a new window.
- Select the source and destination for the same.
- You can refer to Figure 11.25 if it meets with your requirements, or you can choose between slots if you have more than 1 slots.
- Now click on **Swap**. It will take few seconds to swap the between apps.

Take a look at Figure 11.25:

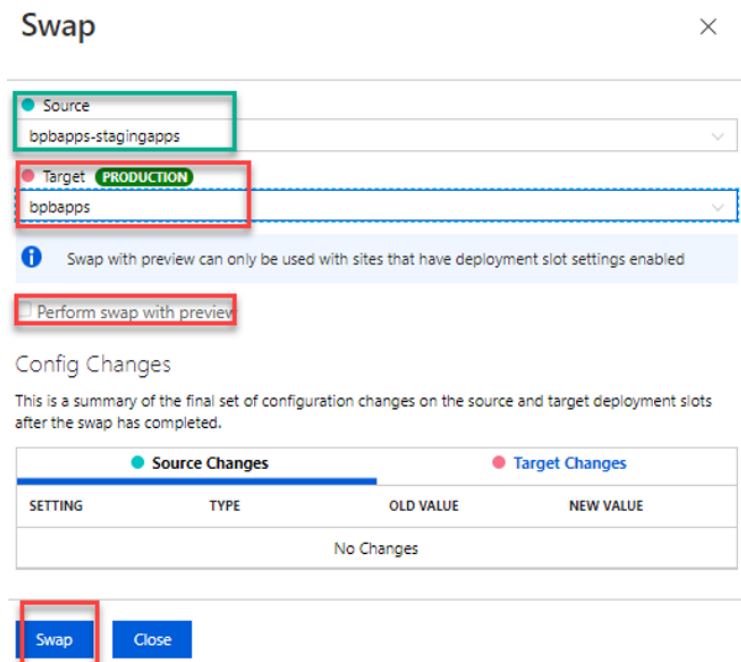


Figure 11.25: App deployment slot swap configuration

Now we have learned how to swap the application between 2 different apps and can create multiple slots based on standard, premium or isolated plans.

## Conclusion

In this chapter, we discussed the Azure app services and app services plan. We also discussed how to configure the Azure app services backup and custom domain, and app services security. Then we moved on to configuring the scaling setting, apps services networking settings configuration and how to configure deployment slot, all of which will help to swap between apps.

In the next chapter, we will discuss how to integrate the on-premises network to Azure, using the site-to-site connection and express route. We will also discuss the VNet-to-VNet peering and more.

## Points to remember

- Azure app services are HTTP-based services that are used to host the application, similar to your on-premises IIS server.
- You can configure the custom domain in Azure app services.
- App services can be secure while configuring the network setting in app services.
- App services backup will help take the backup of your app services data.
- App services deployment will help create a kind of replica of your app services as well as in the live testing, while transferring the real traffic to those services.
- We can configure the TLS/SSL 1.2 binding to secure the apps.
- While deploying the app, we can choose app services plans based on the consumption. This can be used for production, test, development environment, and so on.

## Multiple choice questions

1. What is the services plan to choose for dev and test environments?
  - a. Dedicated compute.
  - b. Premium.
  - c. Standard and shared.

**2. How to configure the deployment slot?**

- a. Go to deployment setting and click on deployment centre.
- b. Click on deployment and select deployment slot.
- c. Click on setting and go to configuration option.

**3. How to configure custom domain?**

- a. In App services under setting custom DNS.
- b. Go to Deployment center and click on configuration.
- c. Go to setting and click on Configuration.

## Answers

- 1. **c**
- 2. **b**
- 3. **a**



# CHAPTER 12

# Virtual Network Configuration and Integration On-Prem to Azure

## Introduction

In this chapter, we will discuss the networking services and use their components such as the Azure Virtual Network, and see how to create and use these services. We will also cover the VNet peering that can be used to connect to VNet, as well as configuring the VNet-to-VNet connectivity and the Azure Virtual Network gateway. Let us start with all of these topics and learn how to use networking services. We will also cover how you are going to manage your azure networking using the virtual WAN, along with configuration of end-to-end virtual wan configuration.

## Structure

The following topics will be covered in this chapter:

- Azure Virtual Network
- ExpressRoute connection
- ExpressRoute configuration
- Configure Azure Virtual WAN

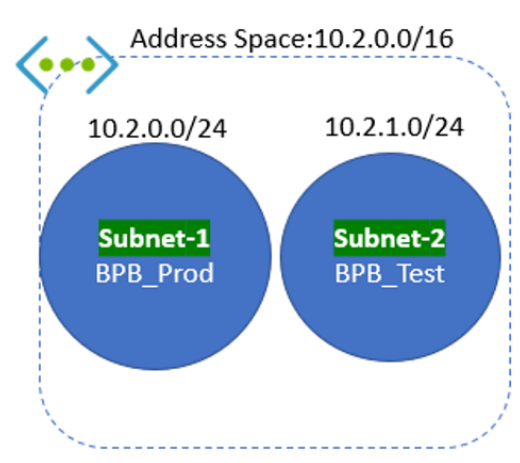
## Objectives

In this chapter, you will learn how to define the network in your Azure subscription, using Azure VNet and subnet. We will discuss how to configure a site-to-site connection and on-premises to Azure connectivity using ExpressRoute.

## Azure Virtual Network

An Azure Virtual Network is defined as the Azure network within your subscription. VNet integration enables you to access Azure resources such as Azure virtual machine, SQLDB, and so on, securely to the Azure network or on-premises network. It is just like you are in an on-premises network that you have configured and have access to, in your data centre. The following components are required to create the virtual network:

- **Address space:** An address space is nothing but a range of your virtual network IP address.
- **Subnet:** A subnet is a collection of the IP address which can be used to assign an Azure virtual machine. Refer to *Figure 12.1*:



*Figure 12.1: Azure address space and subnet*

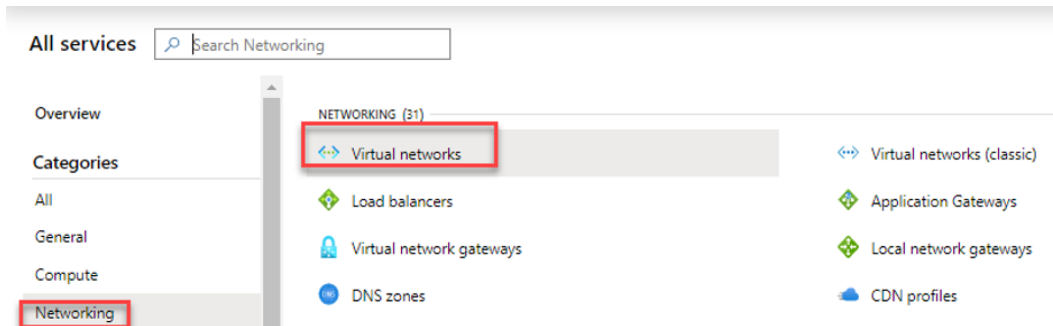
## Azure Virtual Network creation

If you need to create the Azure Virtual Network, then follow the given steps:

1. Log in to the portal.
2. Go to **All services** and click on **Networking**.



3. Select **Virtual networks**, as shown in *Figure 12.2*:



*Figure 12.2: Azure Virtual Network*

4. Provide the virtual network name.
5. Mention the address space as per your requirements.
6. Select the subscription, location, and resources group.
7. Provide the name of the subnet.
8. Then provide the range of the subnet, within the address space range.
9. Click on **Create**, and after that, it will take some time to create the virtual network. Refer to *Figure 12.3*:

*Figure 12.3: Azure Virtual Network details*

Once the virtual network is created, you can see the following details, as shown in Figure 12.4:

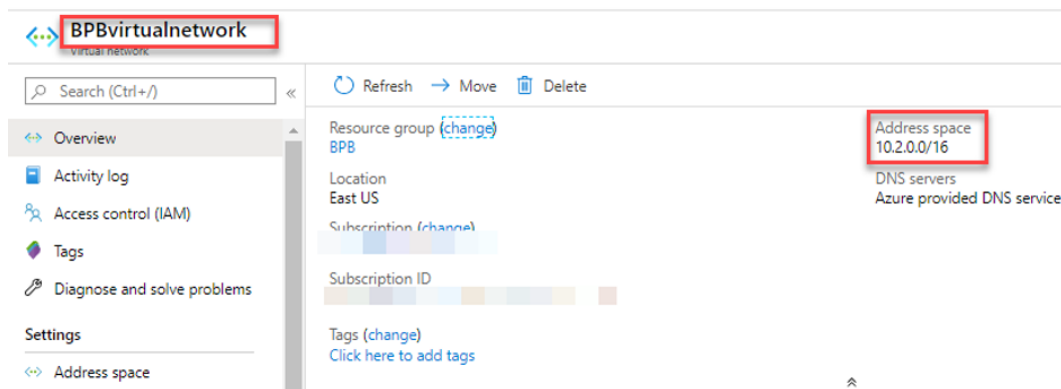


Figure 12.4: VNet configuration

## Azure VNet peering

The Azure Virtual Network can be used to connect two different virtual networks. It provides a seamless connectivity from the Microsoft backbone infrastructure. VNet peering can connect two different Vnets, and also provide low-latency and high-bandwidth.

Azure VNet peering are of two types:

- **VNet peering:** It is used to connect two virtual networks within the same region.
- **Global VNet peering:** It is used to connect two virtual networks across regions.

Refer to Figure 12.5:

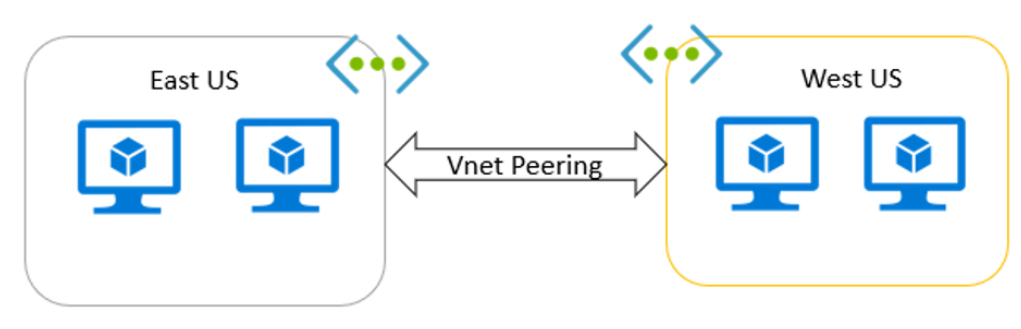
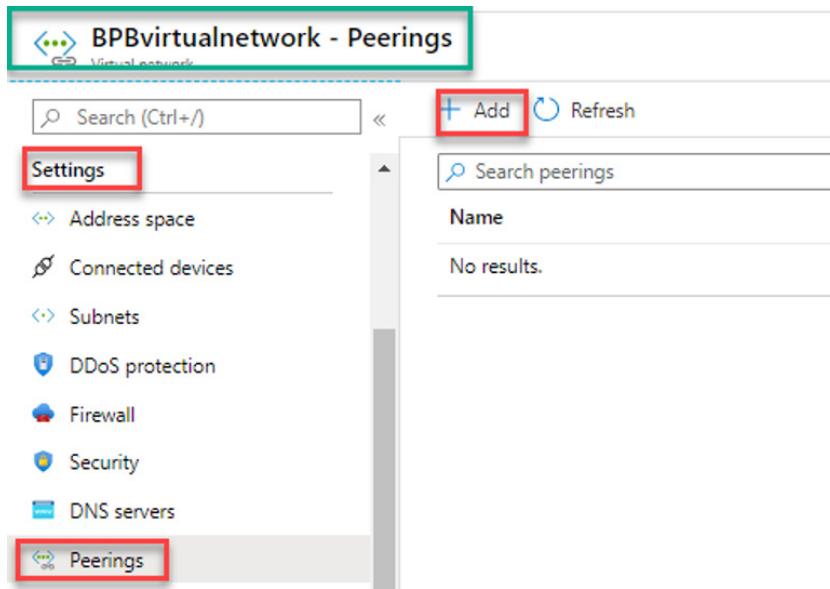


Figure 12.5: VNet peering

We have now understood the use of Azure VNet peering. Let us also understand how to create the Azure VNet peering.

Suppose we have multiple Vnets from various environments and want to communicate with all the Vnets. This is when we can have VNet peering. For VNet peering, we require a minimum of two Vnets, either in the same region or different regions. Follow the given steps to create the VNet peering:

1. Log in to the portal and choose the two Vnets in which you want to configure the VNet peering.
2. Select the VNet you want to peer.
3. Please select the VNet.
4. Under the **Settings** tab, select the **Peering's** option.
5. Click on **+ Add**. Take a look to configure the VNet peering, as shown in *Figure 12.6*:



*Figure 12.6: VNet peering configuration*

6. Provide the VNet peering name.
7. Select the deployment **Resources manager** as default. The classic model can be used if you have resources in the classic mode (it is an old model and MS has stopped supporting this model).
8. Then, select the second virtual network name from the drop-down menu for which you want to enable the VNet peering.

9. Provide the name of VNet peering again for the second VNet configuration. Refer to *Figure 12.7*:

**Add peering**  
BPBvirtualnetwork

**i** For peering to work, a peering link must be created from BPBvirtualnetwork to BPB-vnet as well as from BPB-vnet to BPBvirtualnetwork.

**Name of the peering from BPBvirtualnetwork to BPB-vnet \***  
bpbvnetpeering ✓

**Peer details**  
Virtual network deployment model ⓘ  
☒ Resource manager ☐ Classic  
☐ I know my resource ID ⓘ

**Subscription \*** ⓘ  
[Dropdown menu]

**Virtual network \***  
BPB-vnet (BPB) ✓

**Name of the peering from BPB-vnet to BPBvirtualnetwork \***  
bpbeastus ✓

*Figure 12.7: VNet peering configuration details*

10. Please select the configuration setting to enable and allow the VNet traffic from VNet 1 to VNet 2. You can even enable traffic from VNet 2 to 1, if required by your organization. The gateway transit is only required if VNet is configured with a virtual network gateway.
11. Click on the **OK** button to configure it.
12. Once you click on **Ok**, it will take some time to configure, and will allow traffic in both the Vnets. Refer to *Figure 12.8*:

Configuration

Configure virtual network access settings

Allow virtual network access from BPBvirtualnetwork to BPB-vnet ⓘ

☐ Disabled ☒ Enabled

Allow virtual network access from BPB-vnet to BPBvirtualnetwork ⓘ

☐ Disabled ☒ Enabled

Configure forwarded traffic settings

Allow forwarded traffic from BPB-vnet to BPBvirtualnetwork ⓘ

☐ Disabled ☒ Enabled

Allow forwarded traffic from BPBvirtualnetwork to BPB-vnet ⓘ

☐ Disabled ☒ Enabled

Configure gateway transit settings

☐ Allow gateway transit ⓘ

OK

Figure 12.8: VNet peering configuration settings

- Once the VNet peering is done, verify the connectivity under the **Peerings** section, as shown in Figure 12.9:

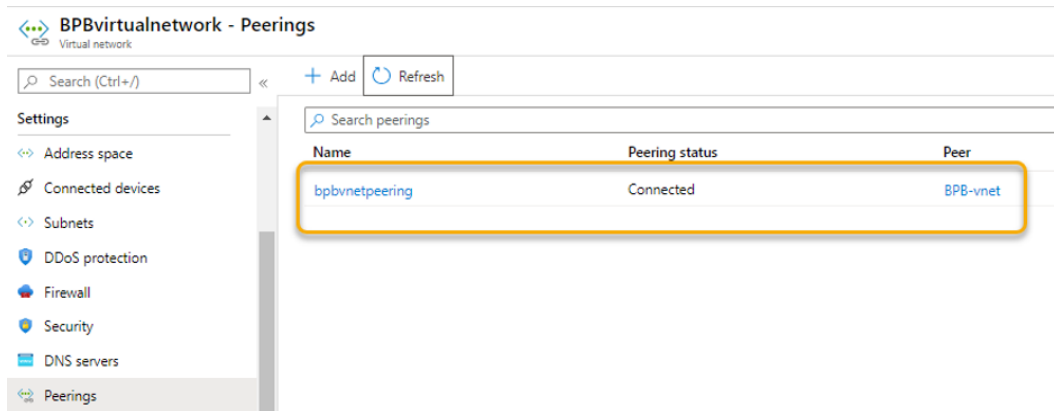


Figure 12.9: VNet connectivity verification

## Virtual network gateway

The Azure Virtual Network gateway is used to send the encrypted traffic from the Azure network to the on-premises network. In other words, it is used to create connectivity between the Azure and on-premise network. A virtual network gateway

is used to send the encrypted traffic over the Microsoft network. In a single VNet, you can configure only one VPN gateway. However, if you want to connect from multiple connections, then you can use the same VPN gateway.

For the configuration, the following are pre-requisites:

- Azure VNet
- You might need a gateway subnet under the same VNet if you want to configure the virtual network gateway.
- You might need a gateway in which you can choose either a VPN or express route based on your requirements.
- It requires a public IP as well.

Before we create the virtual network, please make sure to understand the connectivity you want to use. If you need VNet-to-VNet and site-to-site connection, you can use the VPN, but if you want to configure with the express route, then select the gateway type as EXPRESS ROUTE. Follow these steps to configure the Azure Virtual Network gateway:

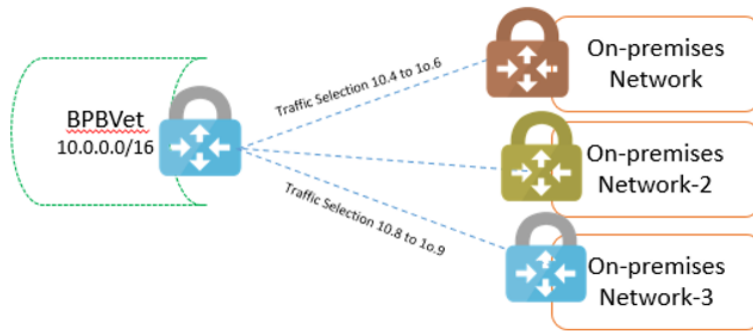
1. Go to the marketplace and search for the Azure Virtual Network gateway.
2. Select **Virtual network gateway** and click on **Create**. The following *Figure 12.10*, shows the VNet network gateway creation:



*Figure 12.10: VNet network gateway creation*

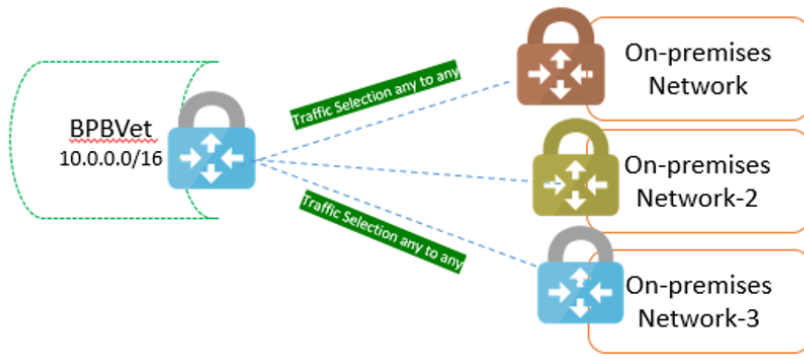
3. Provide the subscription and resource group name of your virtual network resources.
4. Then, provide the virtual network gateway name and region for which you want to create the VNet gateway, and it will provide the same location as your VNet.
5. Choose the VNet gateway type, from the following:

- a. **VPN:** It is used to connect the VNet-to-VNet and site-to-site connectivity.
- b. **Express route:** If you are planning for the express route connectivity, then please select the express route gateway type.
- c. The VPN type is explained as follows:
  - i. **Policy-based:** It is a combination of both the networks and is based on the firewall policy. It will filter the encrypted/decrypted traffic. It is a built-in firewall device which performs traffic filtering. In another way, it is a static VPN device configuration and it has some limitations. Take a look at *Figure 12.11*:



*Figure 12.11: VPN type policy-based*

- ii. **Route-based:** In this scenario, VPN devices are used to send the traffic or route/filter the traffic from any device, to any device or internet, through an IPsec tunnel. Refer to *Figure 12.12*:



*Figure 12.12: VPN type route-based*

6. Select the VPN SKU. It is nothing but a VNet device capability configuration. For more details, please take a look at *Figure 12.13*:

| VPN        | SKU      | S2S/VNet-to-VNet | P2S              | P2S           | Aggregate            | BGP           | Zone-redundant |
|------------|----------|------------------|------------------|---------------|----------------------|---------------|----------------|
| Gateway    |          | Tunnels          | SSTP Connections | IKEv2/OpenVPN | Throughput Benchmark |               |                |
| Generation |          |                  |                  |               |                      |               |                |
| Generatio  | Basic    | Max. 10          | Max. 128         | Not Supp      | 100 Mbps             | Not Supported | No             |
| Generatio  | VpnGw1   | Max. 30*         | Max. 128         | Max. 250      | 650 Mbps             | Supported     | No             |
| Generatio  | VpnGw2   | Max. 30*         | Max. 128         | Max. 500      | 1 Gbps               | Supported     | No             |
| Generatio  | VpnGw3   | Max. 30*         | Max. 128         | Max. 1000     | 1.25 Gbps            | Supported     | No             |
| Generatio  | VpnGw1AZ | Max. 30*         | Max. 128         | Max. 250      | 650 Mbps             |               |                |

*Figure 12.13: VPN SKU*

7. Once you provide all the details and select the option, it will look as shown in *Figure 12.14*:

**Create virtual network gateway**

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more.](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group  Select a virtual network to get resource group

**Instance details**

Name \*

Region \*

Gateway type \* ☒ VPN ☐ ExpressRoute

VPN type \* ☒ Route-based ☐ Policy-based

SKU \*

*Figure 12.14: VPN gateway configuration*

8. Select the generation, in our case, it is **Generation 1**.
9. Select the virtual network from the drop-down menu.
10. Provide the public IP name or use an existing one.
11. Select **Enable active-active mode** which will be the default value. However, if you want to configure it, then you need to add another public IP in the configuration.



12. Select the default option in **Configure BGP ASN** as **Disabled**.

13. Click on **Review + create**. Take a look at Figure 12.15:

Generation ⓘ Generation1 ▼

**VIRTUAL NETWORK**

Virtual network \* ⓘ Filter virtual networks ▼

Only virtual networks in the currently selected subscription and region are listed.

**Public IP address**

Public IP address \* ⓘ ☒ Create new ☐ Use existing

Public IP address name \* bpbpublicIP ✓

Public IP address SKU Basic

Assignment ☒ Dynamic ☐ Static

Enable active-active mode \* ⓘ ☐ Enabled ☒ Disabled

Configure BGP ASN \* ⓘ ☐ Enabled ☒ Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

**Review + create** < Previous Next : Tags > [Download a template for automation](#)

Figure 12.15: VPN gateway creation

It will take up 30 to 45 minutes to create a VNet gateway. Once it gets created, you can configure the site-to-site VPN and VNet-to-VNet connectivity, and we will explain this in the next section.

Now, let us see how to configure the VNet-to-VNet gateway. The VNet gateway is required to be created for both the Vnets, and it is used to connect the two subscriptions and two different regions.

## Site-to-site VPN

The Azure site-to-site VPN is used to connect the Azure network to on-premises data centers over the IPsec IPsec/IKE (IKEv1 or IKEv2) tunnel. It

requires an on-premises VPN device to configure an S2S connection. Take a look at Figure 12.16:

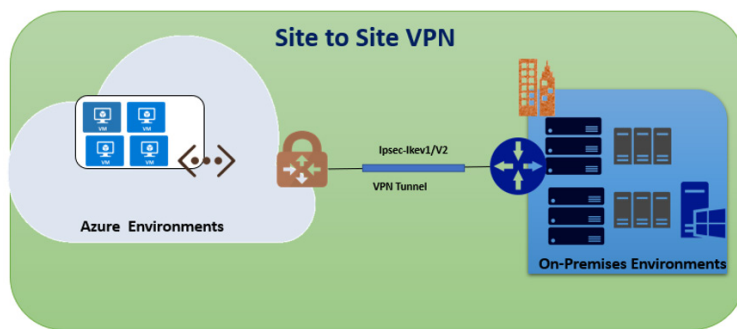


Figure 12.16: Azure site-to-site VPN

Creating a site-to-site VPN requires the following requirement list:

- Azure VNet
- VNet gateway
- Local area network gateway
- Connection
- On-premises VNet connection

**Local Area network Gateway:** It represents the hardware or software VPN device in your local network. We can use this with a connection to set up a site-to-site VPN connection between an Azure Virtual Network and your local network.

Since we have already covered the steps to creating the VNet and VNet gateway, let us now see how to create a local area network. Follow the given steps:

1. Please go to marketplace and search for **Local network gateway**. Refer to Figure 12.17:

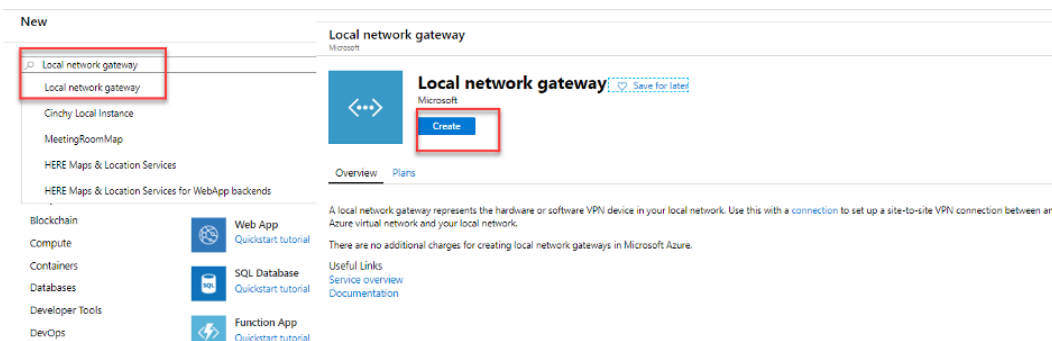


Figure 12.17: Azure local area network gateway

2. Please provide the local gateway name, the public IP address of your on-premises VPN devices and the address range of the on-premises network.
3. Please provide the resources group, name, and location. Then click on **Create**, as shown in *Figure 12.18*:

**Create local network gate...** □

**Name \***  
BPBLocalgateway ✓

**IP address \* ⓘ**  
106.51.111.1 ✓

**Address space ⓘ**  
172.168.0.0/16 ...  
[Add additional address range](#) ...

☐ **Configure BGP settings**

**Subscription \***  
[Dropdown menu]

**Resource group \* ⓘ**  
BPB [Dropdown menu]  
[Create new](#)

**Location \***  
(US) East US [Dropdown menu]

**Create** [Automation options](#)

*Figure 12.18: Azure local area network gateway details*

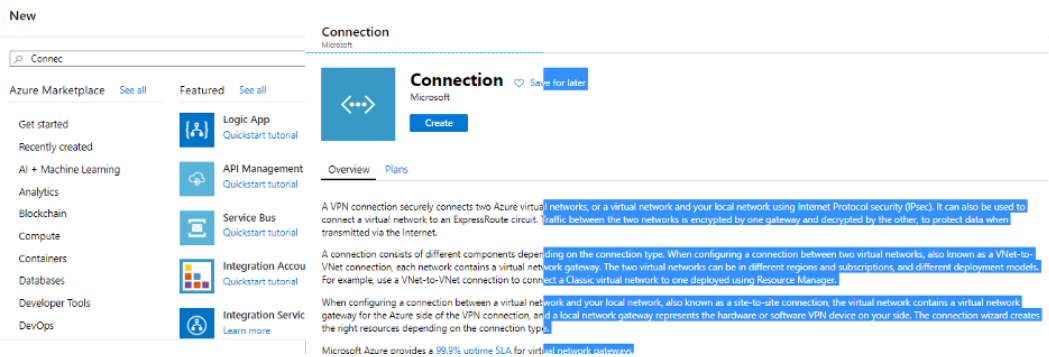
Once the local area network gateway is created, please create the connection and configure the site-to-site VPN.

## Site-to-site VPN connection creation

Once you configure the site-to-site VPN, follow the given steps:

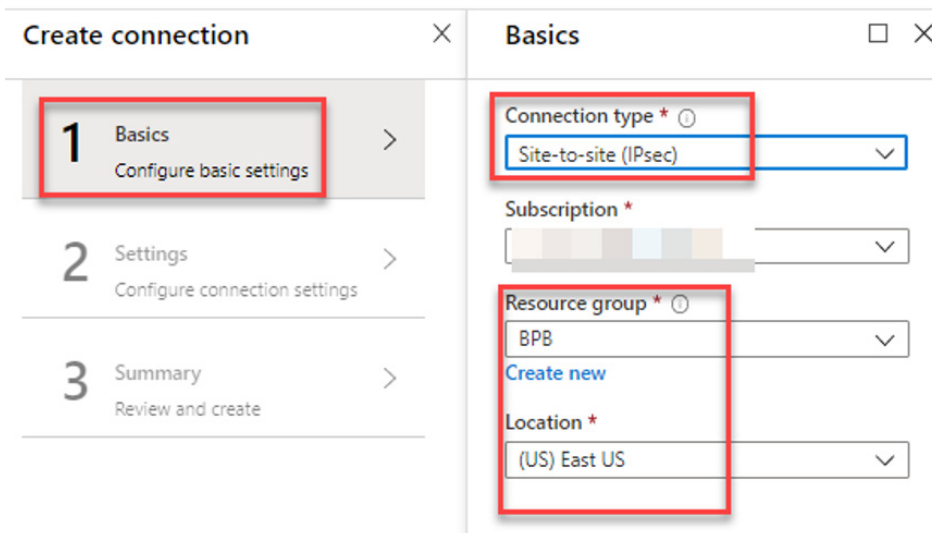
1. Please go to the marketplace and search for **Connection**.
2. Click on **Connection**.

3. Click on **Create**. Refer to *Figure 12.19*:



*Figure 12.19: Azure S2S connection creation*

4. Once you click on **Create**, follow the given steps:
  - a. Please select the connection type as **Site-to-site (IPsec)**, **VNet-to-VNet**, or **ExpressRoute** from the drop-down menu.
  - b. Select the subscription. And then select the resource group.
  - c. Lastly, select the location, as shown in *Figure 12.20*:



*Figure 12.20: Azure S2S connection basic details*

5. Go to the **Settings** tab and perform the following steps:
  - a. Please select the VNet gateway in your specific region.
  - b. Select the local area network gateway we created earlier.

- c. Provide the name of the connection.
- d. Provide the passkey. It can be created in your on-premises VPN device or Azure connections.
- e. Select the protocol IKEv2 and let it be the default value.
- f. Click on **OK**. Take a look at *Figure 12.21*:

**Create connection** × **Settings** □ ×

- 1 Basics ✓  
Configure basic settings
- 2 Settings >  
Configure connection settings
- 3 Summary >  
Review and create

\*Virtual network gateway ⓘ  
BPBVnet

\*Local network gateway ⓘ  
BPBLocalgateway

Connection name \*  
BPBVnet-BPBLocalgateway ✓

Shared key (PSK) \* ⓘ  
bpb@123 ✓

IKE Protocol ⓘ  
☐ IKEv1 ☒ IKEv2

☐ Enable BGP ⓘ

*Figure 12.21: Azure S2S connection basic details*

In the Conclusion part toward the end, please verify the details and click on **OK** to create the connection. Please take a look at *Figure 12.22*:

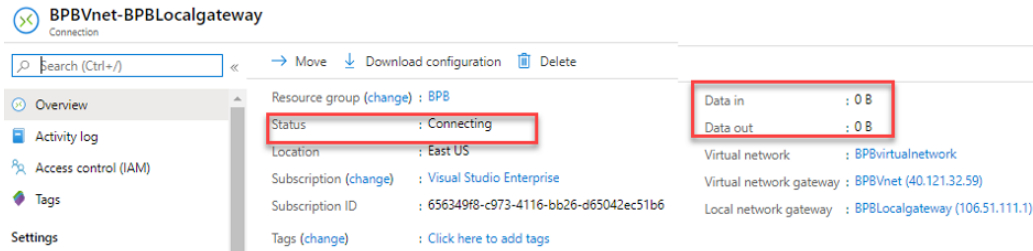
**Create connection** × **Summary**

- 1 Basics ✓  
Configure basic settings
- 2 Settings ✓  
Configure connection settings
- 3 Summary >  
Review and create

|                         |                          |
|-------------------------|--------------------------|
| <b>Basics</b>           |                          |
| Connection type         | Site-to-site (IPsec)     |
| Subscription            | Visual Studio Enterprise |
| Resource Group          | BPB                      |
| Location                | (US) East US             |
| <b>Settings</b>         |                          |
| Virtual network gateway | BPBVnet                  |
| Local network gateway   | BPBLocalgateway          |
| Connection name         | BPBVnet-BPBLocalgateway  |
| Shared key (PSK)        | bpb@123                  |
| IKE Protocol            |                          |

*Figure 12.22: Azure S2S connection summary*

Once the connection is created, you will see the status connecting, and the data in and out values. It will take some time to connect, and after that, you need to ask your network team to create the S2S tunnel in your on-premises VPN device as well. Refer to *Figure 12.23*:



*Figure 12.23: Azure S2S connection summary*

Now you can create an S2S connection. Let us see how to create the VNet-to-VNet connectivity.

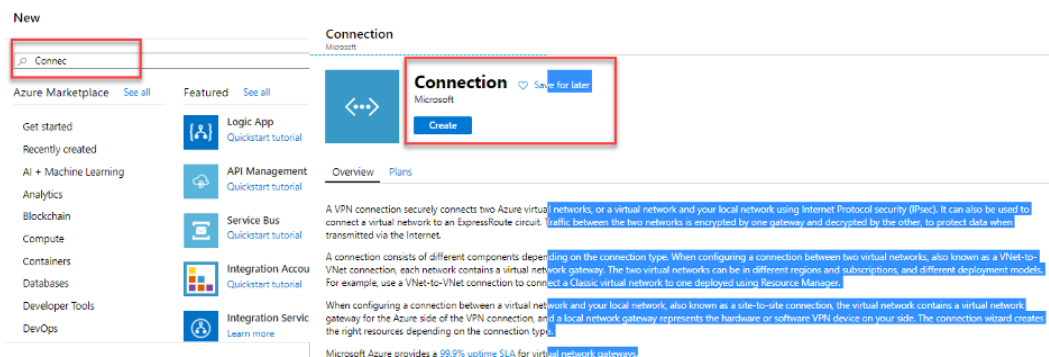
## VNet-to-VNet connectivity creation

Let us see how to create the VNet-to-VNet connectivity. You would require the following configuration before you set up the VNet-to-VNet connections:

- Azure VNet
- Two VNet gateways for both the Vnets
- Connection

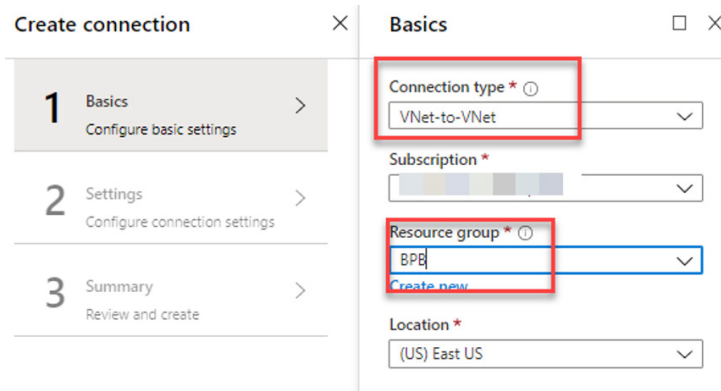
Once you set up the preceding components, follow the given steps to create the connections:

1. Go to the marketplace and search for a **Connection**.
2. Then, click on the **Connection** to create the VNet-to-VNet connection. Refer to *Figure 12.24*:



*Figure 12.24: Azure VNet-to-VNet connection summary*

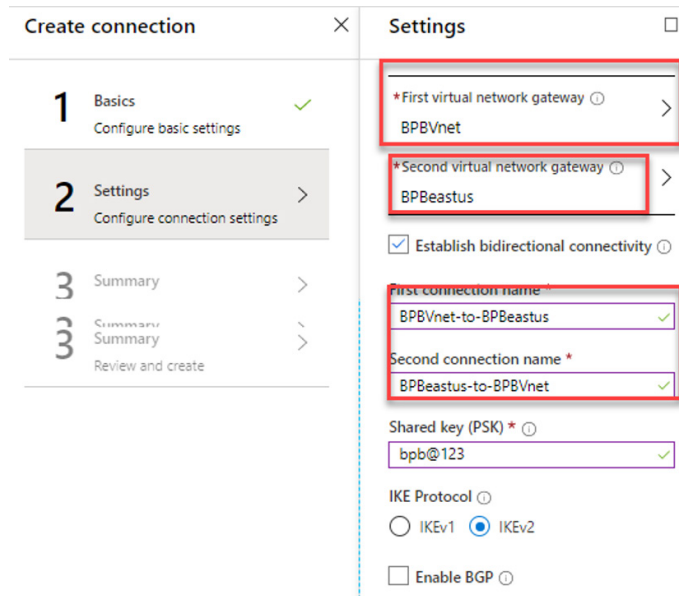
3. Select the connection type **Vnet-to-Vnet**.
4. Select the subscription and resources group.
5. Select the location as (US) East US. Refer to *Figure 12.25*:



The screenshot shows the 'Create connection' dialog box with the 'Basics' tab selected. The 'Connection type' is set to 'VNet-to-VNet'. The 'Subscription' is set to 'BPB'. The 'Resource group' is set to 'BPB'. The 'Location' is set to '(US) East US'.

*Figure 12.25: Azure VNet to VNet connection basic settings*

6. Select the source and destination VNet gateway.
7. Provide the name of the connections.
8. Provide the shared access key.
9. Click on **OK**. Refer to *Figure 12.26*:



The screenshot shows the 'Create connection' dialog box with the 'Settings' tab selected. The 'First virtual network gateway' is set to 'BPBVnet'. The 'Second virtual network gateway' is set to 'BPBeastus'. The 'Establish bidirectional connectivity' checkbox is checked. The 'First connection name' is set to 'BPBVnet-to-BPBeastus'. The 'Second connection name' is set to 'BPBeastus-to-BPBVnet'. The 'Shared key (PSK)' is set to 'bpb@123'. The 'IKE Protocol' is set to 'IKEv2'.

*Figure 12.26: Azure VNet-to-VNet connection settings*

10. Please verify the **Summary** section and click on **OK** to create the VNet-to-VNet connections. Refer to *Figure 12.27*:

| Create connection |                               | Summary                                      |  |
|-------------------|-------------------------------|----------------------------------------------|--|
| 1 Basics          | Configure basic settings      | Basics                                       |  |
| 2 Settings        | Configure connection settings | Connection type: VNet-to-VNet                |  |
| 3 Summary         | Review and create             | Subscription: Visual Studio Enterprise       |  |
|                   |                               | Resource Group: BPB                          |  |
|                   |                               | Location: (US) East US                       |  |
|                   |                               | Settings                                     |  |
|                   |                               | First virtual network gateway: BPBVnet       |  |
|                   |                               | Second virtual network gateway: BPBeastus    |  |
|                   |                               | Establish bidirectional connectivity: Yes    |  |
|                   |                               | First connection name: BPBVnet-to-BPBeastus  |  |
|                   |                               | Second connection name: BPBeastus-to-BPBVnet |  |
|                   |                               | Shared key (PSK): bpb@123                    |  |
|                   |                               | IKE Protocol                                 |  |

*Figure 12.27: Azure VNet-to-VNet connection summary*

11. Once the VNet connection is created, you can see that the status is **Connected**. Take a look at *Figure 12.28*:

| BPBVnet-to-BPBeastus      |                                        |
|---------------------------|----------------------------------------|
| Resource group (change)   | : BPB                                  |
| Status                    | : Connected                            |
| Location                  | : East US                              |
| Subscription (change)     | : Visual Studio Enterprise             |
| Subscription ID           | : 7f7c1b1e-1b1e-1b1e-1b1e-1b1e1b1e1b1e |
| Tags (change)             | : Click here to add tags               |
| Data in                   | : 0 B                                  |
| Data out                  | : 0 B                                  |
| Virtual network           | : BPBVnet, NetworkWatcherRG-vnet       |
| Virtual network gateway 1 | : BPBVnet (40.121.32.59)               |
| Virtual network gateway 2 | : BPBeastus (40.121.56.169)            |

*Figure 12.28: Azure Vnet-to-VNet connection status*

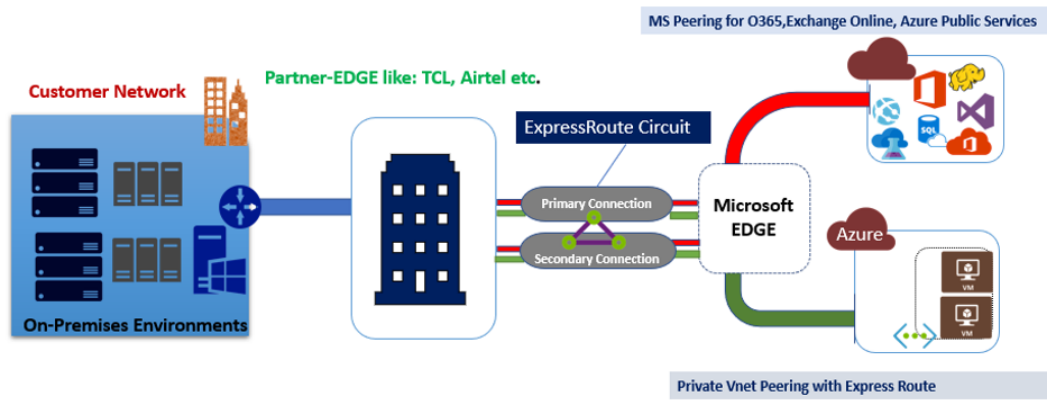
We have now learned how to configure the site-to-site connection and Vnet-to-Vnet connectivity. In the next section, we will discuss the express route and set up the express route connection, which is almost the same as we did in the site-to-site connectivity.

# ExpressRoute connection

ExpressRoute is a direct, dedicated connection from your **Wide Area Network (WAN)**, not over the public internet, to Microsoft services and Azure. We can configure the site-to-site VPN and ExpressRoute connections for the same virtual network for load balancing or high availability.



We can configure a site-to-site VPN as a secure failover path for ExpressRoute, or use site-to-site VPNs to connect to sites that are not part of your network, but that are connected through ExpressRoute. Refer to *Figure 12.29*:



*Figure 12.29: ExpressRoute*

## ExpressRoute configuration

We will now discuss how to configure the express route. For this, we require the following:

- Azure VNet
- ExpressRoute circuit
- VNet gateway with ExpressRoute
- Connection

We have already gone over how to create an Azure VNet and VNet gateway. Let us now see how to configure the ExpressRoute circuit in Azure:

1. Search for express route from the marketplace.
2. Click on **+Add**.
3. Provide the express route circuit name.
4. Provide the name that will be your ISP provider name, such as Airtel, AT&T, and so on.
5. Select the peering location from the drop-down menu.
6. Select the bandwidth 50Mbps to 10Gbps.
7. Then, click on **Create**.

Please take a look at the following *Figure 12.30*:

The screenshot displays the Azure portal interface for managing ExpressRoute circuits. On the left, the 'ExpressRoute circuits' list is shown with an 'Add' button highlighted. The main area on the right is the 'Create ExpressRoute circuit' form. The form includes the following fields and options:

- Create new or import from classic:** Buttons for 'Create new' and 'Import'.
- Circuit name:** Text input field containing 'bpbCircute'.
- Provider:** Dropdown menu with 'Airtel' selected.
- Peering location:** Dropdown menu with 'Chennai2' selected.
- Bandwidth:** Dropdown menu with '50Mbps' selected.
- SKU:** Radio buttons for 'Standard' and 'Premium', with 'Standard' selected.
- Create:** A blue button at the bottom left of the form, highlighted with a red box.
- Automation options:** A link to view automation options.

Below the 'Create' button, a disclaimer states: 'By clicking the create button, you understand that billing will start immediately upon creation of the ExpressRoute and you agree to accept the charges.'

*Figure 12.30: ExpressRoute circuit*

- Once the ExpressRoute circuit is created, follow the site-to-site connection steps and select the ExpressRoute circuit name. Then, create the connections.

**Note:** ISP providers can configure the on-premises express route setup . The circuit creation will be done by your ISP, with your network team.

## Configure Azure Virtual WAN

Azure virtual WAN brings more functionalities for networking, security, and routing together, which provides the single operational interface. Virtual WAN architecture is a hub and spoke architecture, with scale and performance built in for branches, which enables the global transition network architecture.

The main features of virtual WAN are as follows:

- Site to site and Point to site VPN.
- Private connectivity for express route.
- Intra cloud connectivity.

- Routing, Azure firewall and encryption for private connectivity.

Figure 12.31 is a high-level diagram for explaining virtual WAN:

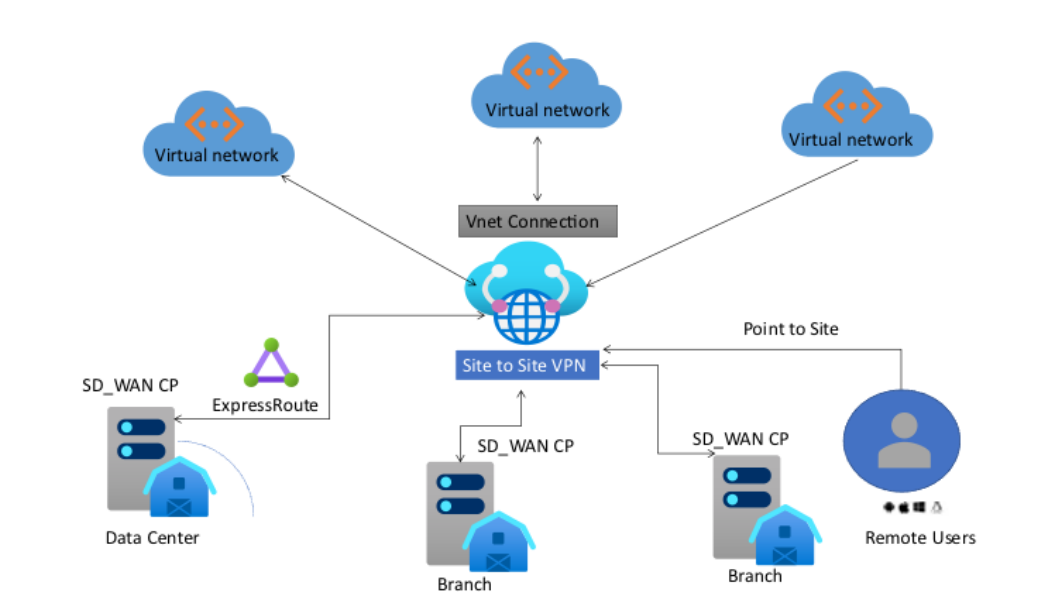


Figure 12.31: Virtual WAN

Let us create a virtual WAN and configure the same. Follow the given steps:

1. Click on create new.
2. Search for virtual wan, and follow the given steps as per Figure 12.32:

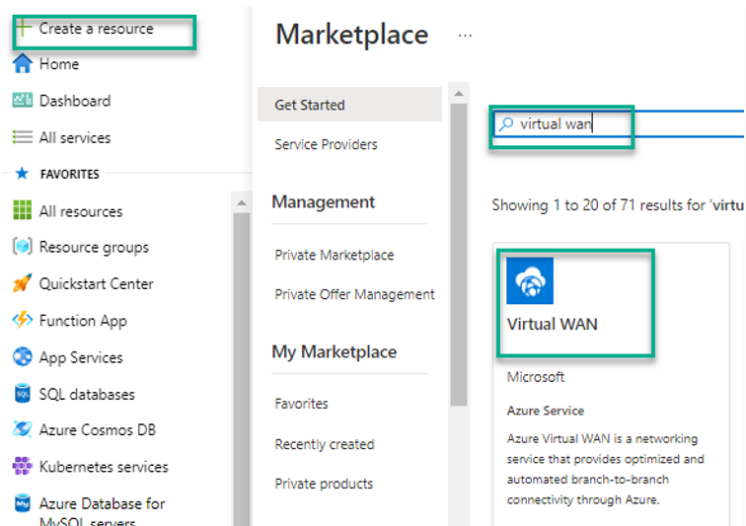


Figure 12.32: Virtual WAN Creation

3. Provide the subscription details.
4. Select the **Resources group** or create new resources group while clicking on create new resources group.
5. Provide the region where you want to create virtual wan.
6. Then select the Name of the virtual wan.
7. Select the virtual Wan plan: Standard or basic, based on your organization requirements. Then click on **Create**.

Refer to *Figure 12.33*:

## Create WAN ...

Basics Review + create

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#)

Project details

Subscription \*

Resource group \*

East US

bpb

Create new

Virtual WAN details

Region \*

Name \*

Type ⓘ

East US

BpBVirtualWanesu2

Standard

Review + create

Previous

Next : Review + create >

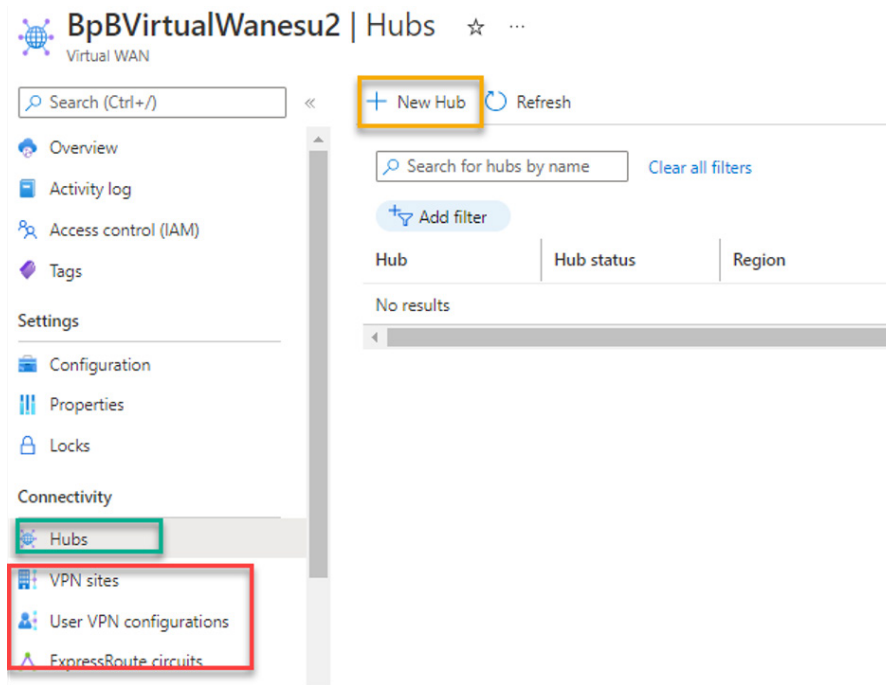
*Figure 12.33: Virtual WAN Creation details*

After that, your virtual wan will be created.

Let us see how to configure the hub which includes the sites and site VPN, point to site and express route connection. You can also create those components individually as well. Follow the given steps:

1. Select the Virtual Wan.
2. Go to configuration tab if you want to configure site 2 site connection, Potin to site connection or even express route individually. We are going to create a hub which includes all of those connection.

3. Click on **New Hub**, as shown in *Figure 12.34*:



*Figure 12.34: Virtual WAN Creation details*

4. Once you will create a new hub, another window will open.
5. Validate the subscription name and resources group.
6. Provide the region and name of the Virtual Wan.
7. Select the virtual hub capacity; you can select up to 50 routing and 50000 VM capacity in single virtual wan.

Refer to *Figure 12.35* for more details:

**Create virtual hub** ...

your on-premises network (vpnsite). [Learn more](#)

**Project details**

The hub will be created under the same subscription and resource group as the vWAN.

Subscription: [Dropdown]

Resource group: bpb [Dropdown]

**Virtual Hub Details**

Region \*: Central US [Dropdown]

Name \*: bpbvirtualhub [Dropdown] ✓

Hub private address space \*: 10.10.10.0/16 [Dropdown] ✓

Virtual hub capacity \*: 4 Routing Infrastructure Units, 4 Gbps Router, Supports 4000 VMs [Dropdown] ✓

*Figure 12.35: Virtual Hub*

8. Select the site-to-site configuration to enable.
9. AS number will be automatically populated.
10. Select the gateway scale units and Routing preference to Microsoft network or Internet, based on your requirements.

Then follow the steps as shown in *Figure 12.36*:

**Basics** **Site to site** Point to site ExpressRoute Tags Review + create

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)? **Yes** No

AS Number: 65515 [Text]

Gateway scale units \*: 1 scale unit - 500 Mbps x 2 [Dropdown]

Routing preference: ☒ Microsoft network ☐ Internet

*Figure 12.36: Site to site VPN*

11. Once you will click on **Next**, it will ask to provide the point to site configuration details.
12. Select the option yes, if you want to configure the same.

13. It is important to note the gateway unit based on how many clients one needs. In our case here, we are selecting 2 scale unit with 500 clients.

14. Provide the point to site configuration and routing preference.

Then follow the steps as shown in *Figure 12.37*:

Basics Site to site **Point to site** ExpressRoute Tags Review + create

If you plan to use this hub with Point-to-site connections, you will need to enable Point-to-site gateway before connecting end-user devices. You can do this after hub creation, but doing now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Point to site (User VPN gateway)? **Yes** No

Gateway scale units \* ① 2 scale units - 1 Gbps x 2, supports 500 clients

Point to site configuration \* ① Select a configuration [Create new](#)

Routing preference ① ☒ Microsoft network ☐ Internet

Use Remote/On-premises RADIUS server ① ☐

*Figure 12.37: Point to site vpn*

15. If you want to configure the expressroute, then select the **Yes** option.

16. Provide the gateway scale units and click on **Next**. Refer to *Figure 12.38*:

Basics Site to site Point to site **ExpressRoute** Tags Review + create

If you plan to use this hub with ExpressRoutes, you will need to enable an ExpressRoute gateway before connecting to ExpressRoute circuits. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create an ExpressRoute gateway? ① **Yes** No

Gateway scale units \* ① 1 scale unit - 2 Gbps

*Figure 12.38: Expressroute*

After that, you can click on review and create the hub configuration. It will take few minutes to create and configure the virtual Wan.

Now we have learned how to create and configure the virtual wan. We shall explore that in the next chapters.

## Conclusion

In this chapter, we discussed VNet and how to set up the VNet gateway and configure the site-to-site connection, express route, and VNet-to-VNet connections. In the next chapter, we will discuss the Azure network security group and IP address types. We will also discuss how to create and configure the Azure security group rules and how to associate a subnet NSG with VMs and subnets. We also have to cover configuring the virtual wan, since using that, you can manage your networking component centrally.

## Points to remember

- We can connect to on-premises environments using the expressroute connection.
- Expressroute connection is secure and reliable, and provides connectivity to Azure/O365 and so on. It is a dedicated line from client datacentre to Microsoft, using ISP provider services.
- Site to site connectivity will also help to connect on-premises to Azure, while building the S2S tunnel from Azure to on-premises supported firewall. You do not need any ISP providers to support on this.
- Gateway Subnet should be created before you create Vnet gateway.
- Vnet peering used to connect 2 vnet with in the same region or different region to enable the resources connectivity.

## Multiple choice questions

1. **What does vnet peering do?**
  - a. Enable the traffic between azure to On-premises.
  - b. Enable the traffic between O365 to Azure.
  - c. Occurs between 2 Vnets either in same region or different region.
2. **What are the components required to connect Azure to on-premises?**
  - a. Vnet, Subnet, Gateway.
  - b. Vnet, Subnet, Subnet Gateway, Vnet Gateway and connection.
  - c. Site to site VPN and expressroute.

## Answers

1. c
2. b



# CHAPTER 13

# Configuring Load Balancing

## Introduction

In this chapter, we will discuss Azure DNS and learn how to create public and private DNS zones. We will also discuss the Azure load balancer and see how to create and configure the Azure load balancer and DNS. We will also cover the Azure application gateway and traffic manager.

## Structure

The following topics will be covered in this chapter:

- Azure DNS
  - Azure DNS Creation
  - Azure DNS Record Creation
  - Azure Load Balancer
  - Azure Internal Load Balancer
- Front-end IP Configuration
- Azure Backend Pool

- Health Probes
- Application Gateway
- Azure Traffic Manager

## Objectives

In this chapter, you will learn how to configure and set up the load balancer for Azure **Virtual Machines** (VMs)/applications using the Azure load balancer, Traffic manager, and application gateway. We will also cover Azure DNS and see how to create your custom Azure DNS and configure it.

## Azure DNS

Azure DNS is a hosting service that provides the DNS domain and the name resolutions using the Azure infrastructure. You can host the domains in Azure and manage the records. Using Azure DNS, you cannot however buy the custom domain. To buy the domain name, you need to use third-party domain register name sites like godaddy.com, and so on.

Azure DNS manages the Azure records, and we can use it for external resources as well. It is an integrated part of the Azure portal and it is used for Azure services such as billing, support contract, and so on.

The following are the details of the Azure DNS delegation, zones, and DNS registrar usage:

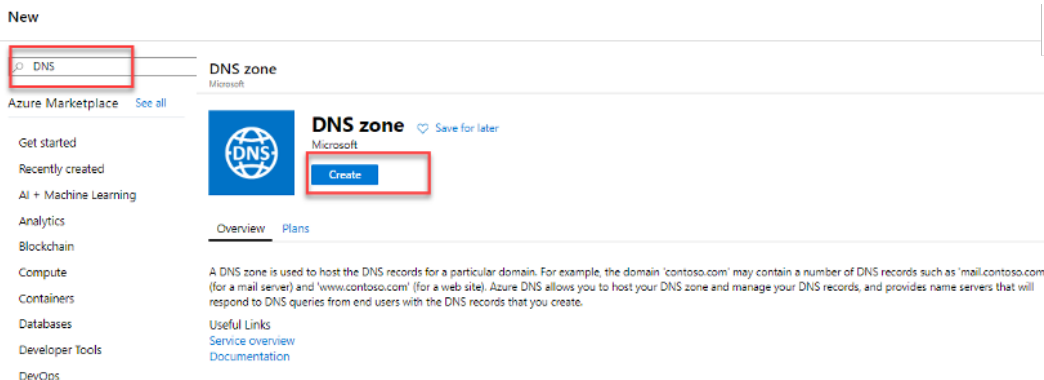
- Zone delegation
  - Azure DNS allows us to host a DNS zone and manage the DNS records for a domain in Azure.
  - Azure DNS is not the domain registrar.
- Domains and zones
  - The domain name system is a hierarchy of domains. The hierarchy starts with the root domain.
  - Some Top-level domains are .com, .net, .org, .uk, or .jp.
  - Second-level domains include org.uk or co.jp, and so on.
  - The domains in the DNS hierarchy are hosted using separate DNS zones.
  - Zones are globally distributed and hosted by DNS name servers around the world.

- DNS zone
  - The domain is a unique name in the domain name system, for example, Bpbcloud.com.
  - A DNS zone is used to host the DNS records for a domain.
  - For example, the domain rcloudweb.com may contain several DNS records such as *mail.rcloudweb.com* (for a mail server) and *www.rcloudweb.com* (for a website).
- Domain registrar
  - The domain registrar is a company that can provide internet domain names.
  - They will verify if the internet domain you want to use is available, and if it is, allows you to purchase it.
  - Once the domain name is registered, you will be the legal owner of the domain name.
- If you already have an internet domain, you will be able to use the current domain registrar to delegate to Azure DNS.

## Azure DNS Creation

Now, let us try and create the Azure DNS services from the Azure portal. Follow the given steps:

1. Go to the marketplace.
2. Search for **DNS** and click on **DNS zone**.
3. Click on **Create**, as shown in *Figure 13.1*:



*Figure 13.1: Azure DNS creation*

4. Select the subscription and resource group name.
5. Provide the DNS name in this format: XYZ.com.
6. Click on **Review + create**, as shown in Figure 13.2:

**Create DNS zone**

Basics Tags Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more.](#)

**Project details**

Subscription \*

Resource group \*  [Create new](#)

**Instance details**

Name \*  ✓

Resource group location ⓘ

[Review + create](#) < Previous Next : Tags > [Download a template for automation](#)

Figure 13.2: Azure DNS

Once the DNS zones are created, it will look like Figure 13.3:

**bpbdns.com**  
DNS zone

Search (Ctrl=/) « + Record set → Move Delete zone Refresh

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Settings  
Properties  
Locks  
Export template

Monitoring  
Alerts  
Metrics

Support + troubleshooting  
New support request

Resource group (change) : bpb  
Subscription (change) : Visual Studio Enterprise  
Subscription ID : 656349f8-c973-4116-bb26-d65042ec51b6  
Tags (change) : [Click here to add tags](#)

**Name server 1 : ns1-04.azure-dns.com.  
Name server 2 : ns2-04.azure-dns.net.  
Name server 3 : ns3-04.azure-dns.org.  
Name server 4 : ns4-04.azure-dns.info.**

**You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.**

| Name | Type | TTL    | Value                                                                                                                                                                                                                                                       | Alias resource type |
|------|------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Ⓜ    | NS   | 172800 | ns1-04.azure-dns.com.<br>ns2-04.azure-dns.net.<br>ns3-04.azure-dns.org.<br>ns4-04.azure-dns.info.<br>Email: azuredns-hostmaster...<br>Host: ns1-04.azure-dns.com.<br>Refresh: 3600<br>Retry: 300<br>Expire: 2419200<br>Minimum TTL: 300<br>Serial number: 1 |                     |
| Ⓜ    | SOA  | 3600   |                                                                                                                                                                                                                                                             |                     |

Figure 13.3: Azure DNS configuration

## Azure DNS record creation

Azure DNS records various types of data, and helps to identify the services based on the records. Generally, records map a domain to its IP address. The following records shown in *Table 13.1*, will help you to understand the usage of each record:

| Record name           | Full name          | Usage                                                                                                                                                 |
|-----------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| A(IPv4)<br>AAAA(IPv6) | Address            | It maps a host name like, mail.bpb.com to an IP address 153.120.10.20.                                                                                |
| CNAME                 | Chronicle name     | It is used to point one host record to another like test.Bpb.com to email.Azure4you.com.                                                              |
| MX                    | Mail exchange      | It points to the host that will receive an email from that domain. The MX record must be a point to A record not to the CNAME record.                 |
| NS                    | Name server        | It delegates a DNS zone to the specified authoritative name server.                                                                                   |
| SOA                   | Start of authority | It defines the authoritative record of zones.                                                                                                         |
| SRV                   | Services           | It is a location host that provides specific services like <b>Skype-Session Initiation Protocol (SIP)</b> , which is used in Skype, Teams, and so on. |
| TXT                   | Text               | It records a human-readable text field in DNS.                                                                                                        |

*Table 13.1: Record names and their usage*

Let us try and create the Azure DNS records. Follow the given steps:

1. Go to DNS zone.
2. Click on **+Record set**.
3. Provide the name of the A record.
4. Select the type of record from the drop-down menu.
5. Provide the **Time-to-Live (TTL)** value.

6. The IP address of the A record or any other record name/IP is based on the description asked. Take a look at *Figure 13.4*:

The screenshot shows the Azure DNS management interface for the zone 'bpbdns.com'. On the left, a sidebar contains navigation links like Overview, Activity log, Access control, Tags, and Settings. The main area displays details for the 'cloud' record set, including its resource group, subscription, and tags. A '+ Record set' button is highlighted with a red box. On the right, the 'Add record set' dialog is open, with several fields highlighted by red boxes: 'Name' (cloud), 'Type' (A), 'TTL' (1) and 'TTL unit' (Hours), and 'IP address' (10.0.2.1). The dialog also includes an 'Alias record set' section with 'Yes' and 'No' radio buttons, and an 'OK' button at the bottom.

*Figure 13.4: Azure DNS configuration*

Thus, we now know how to create the DNS server in Azure and explained its usage.

## Azure Load Balancer

The Azure Load Balancer can be used to distribute the traffic across the backend server and resources, which will help to scale your services and create a high availability of your services. It provides low latency and high throughput. Load balancers support **Transmission Control Protocol (TCP)** and **User Datagram Protocol (UDP)**.

Azure load balancers are of the following two types:

- **Internal load balancer:** It is used to load balance the internal traffic between Azure virtual machines. You can use hybrid connectivity if you want to load balance the on-premises VMs. In this load balancer, there are private IP addresses that are assigned to the front-end IP configuration.
- **External load balancer:** It is used for your external applications, which communicate with the internet traffic. In this load balancer, there are public IP addresses that are assigned to the front-end IP configuration.

Azure load balancers provide the following two types of **Stock-keeping-Unit (SKU)**:

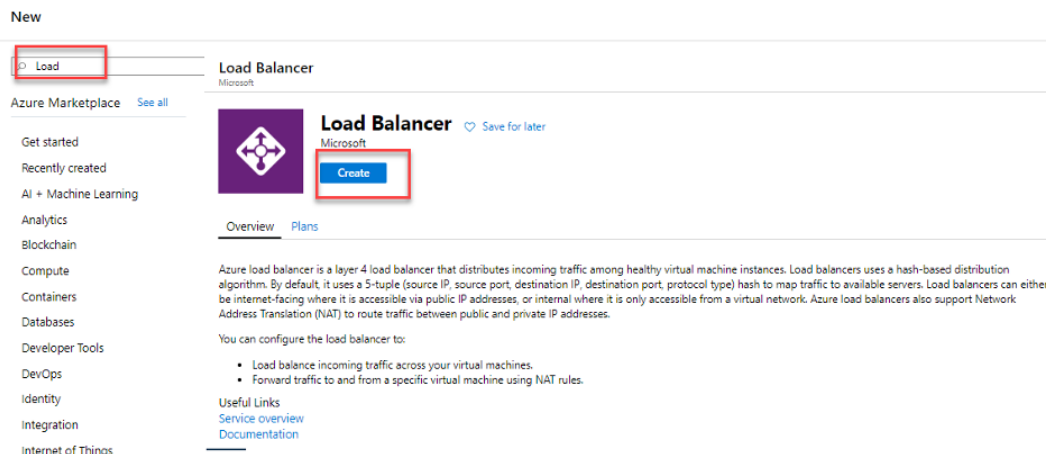
- **Basic:** The basic SKU supports up to 100 instances and the virtual machine should be in an availability set, single, or in the scale set. The protocol has been supported on TCP and UDP. It does not support TCP reset on idle, SLA, multiple front-end and availability zone, and so on.

- **Standard:** The standard SKU supports up to 1000 instances and the virtual machine should be in an availability set, single or in a scale set. The protocol has been supported on TCP, HTTP, and HTTPS. It supports TCP reset on idle, SLA, multiple front-end and availability zone, and so on.

## Azure Internal Load Balancer

Let us try to create an Azure private load balancer and understand its components. Before you create an Azure internal load, you need an Azure virtual network to be created and Azure virtual machine in an availability set or single VMs, which can be used to associate with the Azure internal load balancer backend pool. Follow the given steps:

1. Go to the marketplace and search for an Azure load balancer.
2. Click on **Create**, as shown in *Figure 13.5*:



*Figure 13.5: Azure load balancer*

3. Select the subscription for which you want to create an internal load balancer.
4. Then select the appropriate resource group.
5. Provide the name of the load balancer.
6. Select the region for which you want to deploy the load balancer.
7. Next, select the load balancer type: internal or external, based on your project.
8. Select the SKU type as **Basic**.
9. Select the virtual network and subnet.

10. Now select the IP address assignment. Let it be the default. However, if you are deploying for production, select **Static** instead of **Dynamic**.
11. Click on **Review + create**, as shown in Figure 13.6:

**Create load balancer**

**Project details**

Subscription \*  
Resource group \* BPB [Create new](#)

**Instance details**

Name \* BPBinternalload ✓  
Region \* (US) East US  
Type \* ☒ Internal ☐ Public  
SKU \* ☒ Basic ☐ Standard

**Configure virtual network.**

Virtual network \* BPB-vnet  
Subnet \* default (10.1.0.0/24) [Manage subnet configuration](#)

IP address assignment \* ☐ Static ☒ Dynamic

[Review + create](#) < Previous Next : Tags > [Download a template for automation](#)

Figure 13.6: Azure load balancer creation details

12. Once you click on create, the Azure load balancer will be created after 10 to 15 minutes. Once it is created, it will look like Figure 13.7:

**BPBinternalload**  
Load balancer

Search (Ctrl+/)

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Settings  
Frontend IP configuration  
Backend pools

Move Delete Refresh

Resource group (change) BPB  
Location East US  
Subscription (change)  
Subscription ID  
SKU Basic  
Tags (change) [Click here to add tags](#)

Backend pool  
Health probe  
Load balancing rule  
NAT rules  
0 inbound  
Private IP address  
10.1.0.6

Figure 13.7: Azure load balancer overview



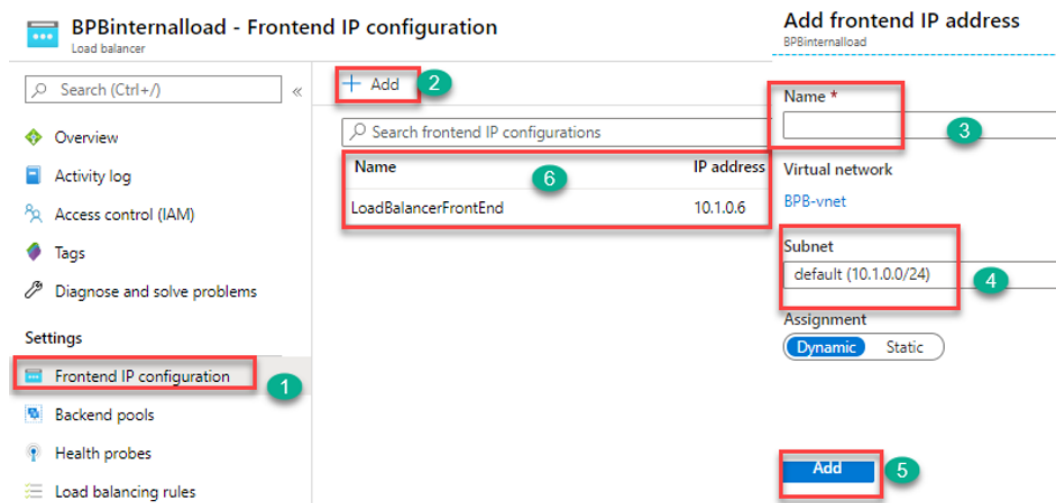
Let us now see how to configure the backend pool, health probe, load balancing rule, NAT rule, and so on.

## Front-end IP configuration

All the traffic will come first to the front-end IP address, and it will distribute the traffic, based on the backend pool connectivity and the load balancers rule. Follow the given steps:

1. Go to the load balancer and select **Frontend IP configuration** under the **Settings** tab.
2. Click on **+ Add**.
3. Provide the name of the front-end load balancer.
4. Select the subnet from the drop-down menu.
5. Click on **Add** to add the frontend IP.

By default, when you create the load balancer, an automatic frontend IP configuration will be configured. However, if you want to add the frontend IP, you need to follow the preceding process to add the new front-end configuration. Take a look at *Figure 13.8*:



*Figure 13.8: Azure load balancer frontend IP configuration*

Once your front-end IP configuration is done, please configure the backend pool.

## Azure backend pool

The Azure backend pool has your server or services configuration, which needs to be load-balanced and it also routes the traffic from the front-end IP. It should be a single virtual machine or scale set to configure it. Follow the given steps to configure the backend pool:

1. Provide the backend pool name.
2. Select the virtual machine or scale set you want to associate.
3. Select the virtual machine and the IP address from the drop-down menu.
4. Click on **+ Add**, as shown in Figure 13.9:

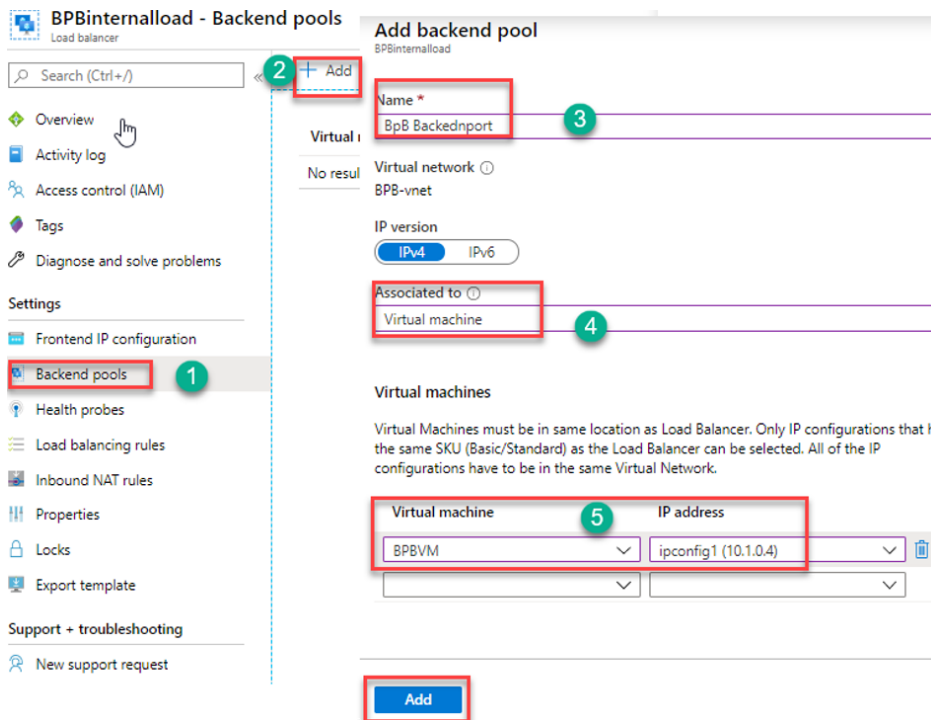


Figure 13.9: Azure load balancer backend pool configuration

## Health probes

It helps to find the failure of the application on the backend endpoint. The health probe helps to find out when to send the new traffic flow to the backend endpoint just like a busy / free status. If the backend endpoint status fails, it stops and does not send any new traffic flow to that instance.

Let us create the health probe for the load balancer configuration. Follow the given steps:

1. Go to **Health probes** under the **Settings** tab.
2. Click on **+ Add**.
3. Provide the name of the health probe.
4. Select the TCP/UDP protocol from the drop-down menu.
5. Let the **Interval** be set to the default value, which means the health probe will check the backend endpoint status in a specific time as configured in the interval.
6. Configure the **Unhealthy threshold** as per your project requirements. It means that if it continuously fails for two times or more, then it will consider the backed endpoint status as failed and stop sending the traffic.
7. Click on **OK** to add the health probe.

Take a look at *Figure 13.10*:

The screenshot displays the 'Add health probe' configuration window in the Azure portal. The left sidebar shows the 'Settings' tab with 'Health probes' selected. The main form contains the following fields and values:

- Name:** BobhealtProbe
- Protocol:** TCP
- Port:** 80
- Interval:** 5 seconds
- Unhealthy threshold:** 2 consecutive failures
- OK button:** At the bottom of the form.

Numbered callouts (1-6) indicate the sequence of steps: 1. Select 'Health probes' in the left sidebar; 2. Click the '+ Add' button; 3. Enter the probe name; 4. Select the protocol; 5. Set the unhealthy threshold; 6. Click the OK button.

*Figure 13.10: Azure load balancer health probe configuration*

8. Click on **Load balancing rules** under the **Settings** tab.
9. Provide the rule name.
10. Provide the protocol type TCP/UDP.
11. Provide the port number and backend port of services.
12. Select the backend pool and health probe.

13. Select the session persistence and idle timeout.

14. Click on the **OK** button to create a load balancing rule.

Take a look at *Figure 13.11*:

The screenshot shows the 'Add load balancing rule' configuration page in the Azure portal. The left sidebar has 'Load balancing rules' highlighted. The main form contains the following fields and values:

- Name:** (empty text box)
- IP Version:** ☒ IPv4, ☐ IPv6
- Frontend IP address:** 10.1.0.6 (LoadBalancerFrontEnd)
- Protocol:** ☒ TCP, ☐ UDP
- Port:** 80
- Backend port:** 80
- Backend pool:** bpbloadbalancer (1 virtual machine)
- Health probe:** BpbhealthProbe (TCP:80)
- Session persistence:** None
- Idle timeout (minutes):** 4
- Floating IP (direct server return):** Disabled
- OK button:** (blue button at the bottom)

*Figure 13.11: Azure load balancer rule configuration*

Now, your load balance configuration has been completed and your services will use the Azure load balancer capability.

## Application gateway

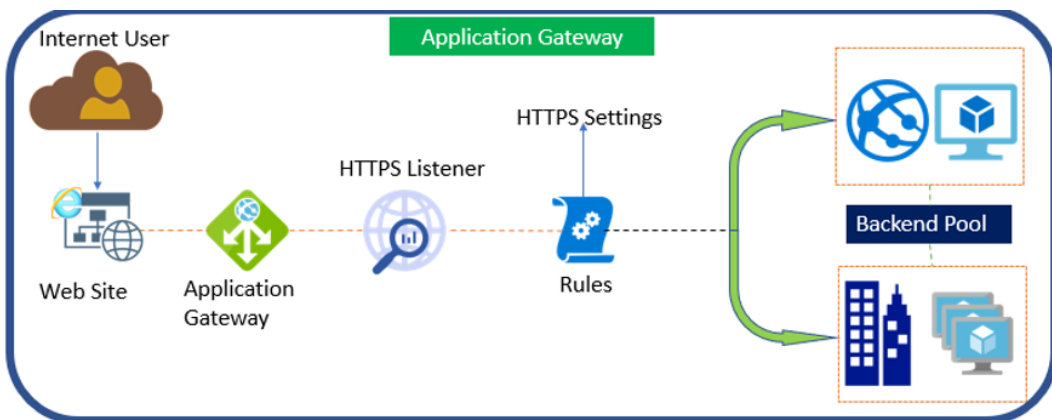
An application gateway is an application layer (OSI layer 7) load balancing, which helps the web traffic load balancer to enable the management traffic to your web applications. The application gateway can make the routing decision as per the HTTP/HTTPS request, to route the traffic to the URI path or the host VM.

The Azure application gateway can do the URL based routing. It provides the following features:

- **Secure Sockets Layer (SSL/TLS) termination:** In this feature, the application gateway provides an SSL/TLS termination at the gateway and after that, traffic will flow (encrypted) to the backend servers/applications.

- **Autoscaling:** The application gateway standard\_v2 supports and provides an autoscaling feature that helps to scale up and down the application gateway, if there are any changes in the traffic load.
- **Zone redundancy:** The application gateway standard\_v2 supports multiple zones availability.
- **Static Virtual IP address (VIP):** The application gateway standard\_v2 supports a static VIP which means it will make sure your VIP associated with this application gateway does not change.
- **Web application firewall:** It provides centralized protection to your web application for common vulnerabilities. It is based on the OWASP 3.1, 3.0, and 2.9. It helps you protect from a **Structured Query Language (SQL)** injection, scripting attack, and so on.
- **URL-based routing:** This URL-based routing allows you to route traffic to the backend server pool based on your URL path. Let us say, <https://bpb.com/video> or <https://bpb.com/images>, and so on.
- **Multiple-site hosting:** We can host up 100 web applications in one application gateway, and each application can be directed to its backend pool.
- **Redirection:** It provides the HTTP/HTTPS based redirection to make sure all the communication between users and its application has been encrypted.
- **Session affinity:** The cookie-based session provides the feature – if you want the user session on the same server for processing the request.

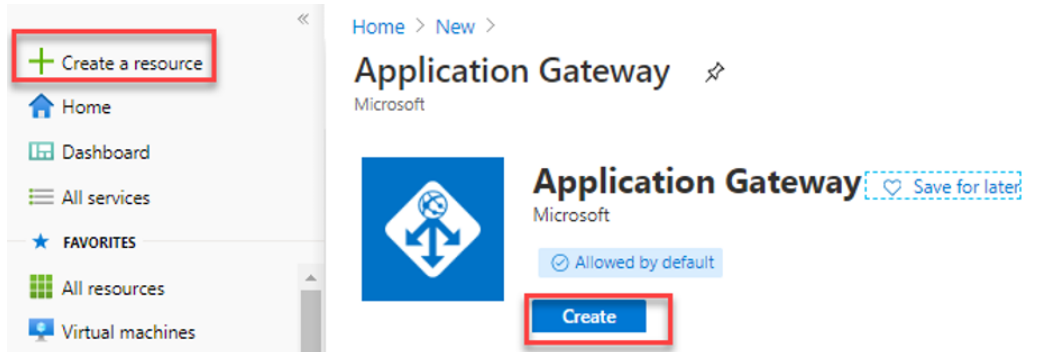
Take a look at *Figure 13.12*:



*Figure 13.12: Application gateway*

Let us see how to create the application gateway and configure it. Follow the given steps:

1. Please click on **Create a resource**.
2. Search for **Application gateway**.
3. Click on the **Create** button to create an application gateway , as shown in *Figure 13.13*:



*Figure 13.13: Application gateway creation*

Once you click on the application gateway creation, follow the given steps:

1. Select the subscription for which you want to create an application gateway.
2. Create or select an existing resources group.
3. Provide the application gateway name as per your organization's standard.
4. Select the region.
5. Select the tier:
  - a. **Standard**: This standard tier does not support autoscaling and zone redundancy.
  - b. **Standard V2**: This standard tier supports autoscaling and zone redundancy.
  - c. **WAF**: It supports WAF 2.9 and 3.0.
  - d. **WAF V2**: It supports WAF 3.1.
6. Provide the autoscaling as Yes or No. If yes, then provide the minimum and maximum scale unit.
7. Provide the virtual network and subnet which does not have a routing table.
8. Once you provide all the details, as shown in *Figure 13.14*, click on Next to configure the front-end configuration:

## Create application gateway

1 Basics 2 Frontends 3 Backends 4 Configuration 5 Tags 6 Review + create

An application gateway is a web traffic load balancer that enables you to manage traffic to your web application. [Learn more about application gateway](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*  [Create new](#)

### Instance details

Application gateway name \*

Region \*

Tier

Enable autoscaling ☒ Yes ☐ No

Minimum scale units \*

Maximum scale units

Availability zone

HTTP2 ☒ Disabled ☐ Enabled

### Configure virtual network

Virtual network \*  [Create new](#)

Subnet \*  [Manage subnet configuration](#)

Figure 13.14: Application gateway basic

The application gateway front-end is where all the reapplication traffic will arrive and then get routed to your apps.

Let us configure the front-end IP configuration and follow the given configuration:

- **Public:** If you have a public-facing application, then select **Public** and configure the public IP.
- **Private:** If you have your internal application, then configure the **Private** option.
- **Both:** If you want to configure your public and internal application, then select **Both**.

Take a look at *Figure 13.15*:

✓ Basics 2 Frontends 3 Backends 4 Configuration 5 Tags 6 Review + create

Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type.

Frontend IP address type ☒ Public ☐ Private ☐ Both

Firewall public IP address \* Choose public IP address   
 Add new

Add a public IP

Name \* appip ✓

SKU ☐ Basic ☒ Standard

Assignment ☐ Dynamic ☒ Static

OK Cancel

Previous Next: Backends >

*Figure 13.15: Application gateway front-end configuration*

Once you are done with this configuration, please select the backend configuration. The application backend pool is where your application/host has been configured to route the traffic, based on your user request. Follow these steps:

1. Click on **Add a backend pool**.
2. Provide the name of the backend pool.
3. Select Yes or No in **Add backend pool without targets**. If yes, provide the backend pool configuration as follows:
  - a. IP address or FQDN name
  - b. Virtual machine
  - c. VMMS
  - d. App services
4. Once you select this, please click on Next for the configuration, as shown in *Figure 13.16*:



**Create application gateway**

✓ Basics ✓ Frontends **3 Backends**

**Add a backend pool**

Backend pool

No results

**Add a backend pool.**

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name \*

Add backend pool without targets ☐ Yes ☒ No

Backend targets

1 item

| Target type                                     | Target                                |
|-------------------------------------------------|---------------------------------------|
| <input type="text" value="IP address or FQDN"/> | <input type="text" value="10.0.0.3"/> |
| <input type="text" value="IP address or FQDN"/> | <input type="text" value=""/>         |

Figure 13.16: Application gateway backend configuration

Once you are done with the backend configuration, let us move to the configuration part, where you need to set up the routing rule for your application.

We will now configure the HTTP/HTTPS listener and backend routing rule, to redirect the traffic. Let us configure the listener by following the given steps:

1. Provide the name of the listener.
2. Select the front-end.
3. Select the protocol HTTP or HTTPS and port 80 or 443.
4. Select the listener type as **Multi site** if you are planning to add multiple sites, or select **Basic**.
5. Select the **Error page url**, as shown in Figure 13.17:

**\* Listener** \* Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name \*

Frontend IP \*

Protocol ☒ HTTP ☐ HTTPS

Port \*

Additional settings

Listener type ☒ Basic ☐ Multi site

Error page url ☐ Yes ☒ No

**Add** **Cancel**

Figure 13.17: Application gateway listener

As we have configured the listener, we will now configure the backend target, by following the given steps:

1. Provide the **Rule name**.
2. Select the **Target type** either as **Backend pool** or **Redirection**, based on your requirements.
3. Select the backend pool from the drop-down menu, as shown in *Figure 13.18*:

**Add a routing rule** ✕

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name \*  ✓

\*Listener \*Backend targets

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type ☒ Backend pool ☐ Redirection

Backend target \* ⓘ  Add new

HTTP settings \* ⓘ  Add new

**Path-based routing**

You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of HTTP settings based on the URL path.

| Path                             | Target name | HTTP setting name | Backend pool |
|----------------------------------|-------------|-------------------|--------------|
| No additional targets to display |             |                   |              |

[Add multiple targets to create a path-based rule](#)

**Add** **Cancel**

*Figure 13.18: Application gateway backend target*

4. Click on HTTP settings and click on Add new.
5. Provide the **HTTP settings name**.
6. Select the **Backend protocol** and **Backend port** number.
7. Select the **Cookie-based affinity** and **Connection draining** as per your requirements.
8. Select the request timeout.

9. If you need to configure a new hostname or the custom hostname, you can also configure it, as shown in *Figure 13.19*:

**Add a HTTP setting**

← Discard changes and go back to routing rules

HTTP settings name \*

Backend protocol ☒ HTTP ☐ HTTPS

Backend port \*

**Additional settings**

Cookie-based affinity ☐ Enable ☒ Disable

Connection draining ☐ Enable ☒ Disable

Request time-out (seconds) \*

Override backend path

**Host name**

By default, Application Gateway does not change the incoming HTTP host header from the client and sends the header unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header.

Override with new host name ☐ Yes ☒ No

Host name override ☐ Pick host name from backend target ☒ Override with specific domain name

Create custom probes ☐ Yes ☒ No

**Add** **Cancel**

*Figure 13.19: Application gateway HTTP setting*

Once we are done with this configuration, click on the **Tags** tab. If you want to add the tags, click on **Review + create**, as shown in *Figure 13.20*:

✓ Basics ✓ Frontends ✓ Backends ✓ Configuration ✓ Tags **6 Review + create**

**Basics**

|                      |                             |
|----------------------|-----------------------------|
| Subscription         | Visual Studio Enterprise    |
| Resource group       | BPB                         |
| Name                 | bpbappgateway               |
| Region               | East US                     |
| Tier                 | Standard_v2                 |
| Enable autoscaling   | Enabled                     |
| Minimum scale units  | 1                           |
| Maximum scale units  | 5                           |
| Availability zone    | Zones 1, 2                  |
| HTTP2                | Disabled                    |
| Virtual network      | vnetbpb                     |
| Subnet               | appgatewaysub (10.0.1.0/26) |
| Subnet address space | 10.0.1.0/26                 |

**Create** **Previous** **Next** [Download a template for automation](#)

*Figure 13.20: Application gateway creation*

When you click on the application gateway creation, the application gateway will get created in 10 to 15 minutes.

## Azure Traffic Manager

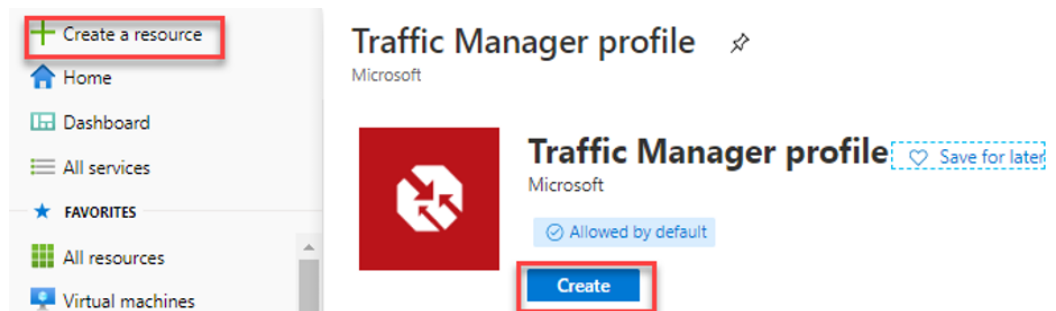
The Azure Traffic Manager is a DNS-based traffic load balancer that enables the distribution of traffic and provides high availability to web applications. The traffic manager uses a DNS to direct the traffic to the most appropriate service endpoint based on the traffic routing method.

It provides the following features:

- Application availability
- Application performance
- Hybrid application
- Distributes the traffic to complex environments

Let us create an Azure Traffic Manager and configure it. Follow the given steps:

1. Click on **Create a resource**.
2. Search for the traffic manager.
3. Click on the **Create** button to create the traffic manager, as shown in *Figure 13.21*:



*Figure 13.21: Traffic manager profile creation*

4. Provide the name of the traffic manager.
5. Provide the routing method from the following to configure it:
  - a. **Priority:** It is used when you want to configure the primary site's endpoint for all the traffic, and secondary sites for backup.

- b. **Weighted:** Weighted can be configured when you want to distribute the traffic to set off endpoints, according to the weight.
  - c. **Performance:** It is used when you want to route the traffic to geographic locations, and you want the closest endpoint for low network latency.
  - d. **Geographic:** It is used to redirect the traffic to a specific endpoint, such as Azure, external, and so on, based on the geographic location.
  - e. **Multi-Value:** This can be configured only when the endpoint has an IPv4/IPv6 address.
  - f. **Subnet:** Subnet traffic-routing is used to map sets of end-users IP address (subnet) ranges to a specific endpoint in the traffic manager profile.
6. Select the subscription.
  7. Select the resource group.
  8. Click on the **Create** button, as shown in *Figure 13.22*:

Create Traffic M... □ ×

Name \*  
bpbtrafficmgr ✓  
.trafficmanager.net

Routing method  
Performance ▼

Subscription \*

Resource group \*  
BPB ▼

Create new

Resource group location ⓘ  
East US ▼

Performance  
Weighted  
Priority  
Geographic  
MultiValue  
Subnet

Create Automation options

*Figure 13.22: Traffic manager creation*

Now, we can create the traffic manager and route the traffic using various routing methods in the traffic manager profile.

## Conclusion

In this chapter, we discussed the configuration of Azure DNS and how to set up the Azure DNS private and public zones. We also discussed the Azure DNS components and records. We covered the usage of the Azure load balancer and explained how to configure and set up the Azure load balancer. We covered the application gateway and traffic manager profile. We also covered how to configure the application and how to load balance and secure your application.

## Points to remember

- Azure load balancer works on **Open Systems Interconnection (OSI)** layer 4 and you can create internal and external load balancer.
- Traffic manager is a DNS based load balanced mechanism and can route the traffic globally.
- Application gateway work is OSI layer 7.
- Application Gateway makes the routing decisions, based on additional attributes of an HTTP request, or URL based routing.
- You create public and private DNS zone based on the customer requirements.

## Multiple choice questions

1. A customer wants to configure load balance with WAF. Which load balance should they choose?
  - a. Traffic manager
  - b. Load Balancer
  - c. Application gateway
2. Clients want to configure the DNS based routing. What would you suggest?
  - a. Create a rule and configure in Azure load balancer
  - b. Create a routing method in traffic manager
  - c. Configure the application gateway

## Answers

1. c
2. b

# CHAPTER 14

# Securing Access to Virtual Networks

## Introduction

In this chapter, we will explain the network security group and its uses. The network security group contains the security rules which allow or deny the inbound/outbound traffic within the subscription and to the outer world. We will discuss network routes and learn how the routes will help to distribute the traffic as per route rules. We will explain the types of IP addresses and learn how they can be assigned to Azure VMs. We will cover the Azure firewall, route table and how to access the **Virtual Machine (VM)** using Azure Bastion services. Azure private endpoints will help to connect services privately and securely. We will be covering the same in this chapter.

## Structure

The following topics will be covered in this chapter:

- Configuration of Private and Public IP Addresses
- Network security group
- Route table
- Configure and deploy the Azure Firewall
- Configure and deploy Azure Bastion services

- Evaluate effective security rules
- Azure private network

## Objectives

One of the major objectives of this chapter is to discuss the Azure firewall and its features. We will discuss how you can protect your Azure network using the Azure firewall. We will also discuss situations where your customer might want to connect VMs securely, in which case, the Azure Bastion services will be used.

## Configuration of private and public IP addresses

The public IP address can be used if you want to connect your application publicly or outside the Azure network. Refer to the public IP addresses and association, shown in *Table 14.1*:

| Public IP addresses | IP address association       | Dynamic | Static |
|---------------------|------------------------------|---------|--------|
| Virtual machine     | Network Interface Card (NIC) | Yes     | Yes    |
| Load balancer       | Front-end configuration      | Yes     | Yes    |
| VPN gateway         | Gateway IP configuration     | Yes     | No     |
| Application gateway | Front-end configuration      | Yes     | No     |

*Table 14.1: Public IP VS private IP*

The private IP address can be used for internal communication within the Azure network. Refer to the following *Table 14.2*:

| IP addresses           | IP address association  | Dynamic | Static |
|------------------------|-------------------------|---------|--------|
| Virtual machine        | NIC                     | Yes     | Yes    |
| Internal load balancer | Front-end configuration | Yes     | Yes    |
| Application gateway    | Front-end configuration | Yes     | Yes    |

*Table 14.2: IP Address association*

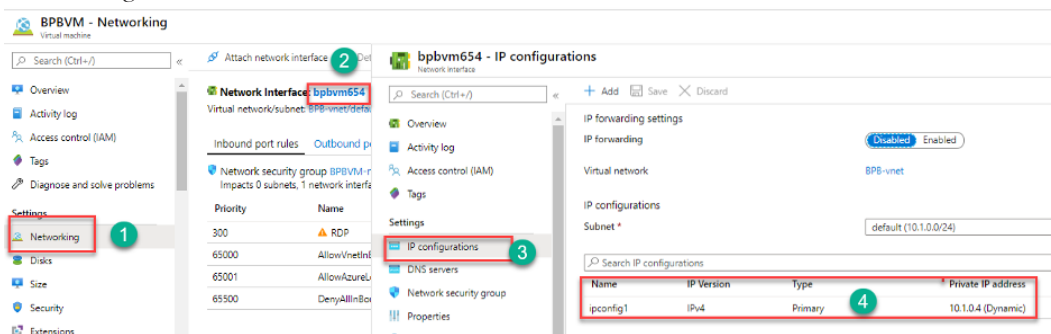
IP addresses can be assigned dynamically by default from the Azure portal. You have to make them static IP addresses. Let us now understand what static IP and dynamic IP addresses are.

Static IP is a fixed IP address, and it cannot be changed even if you restart your services and deallocate the VM. Dynamic IP is the dynamic IP address that can be changed if you restart your services or deallocate the VM.



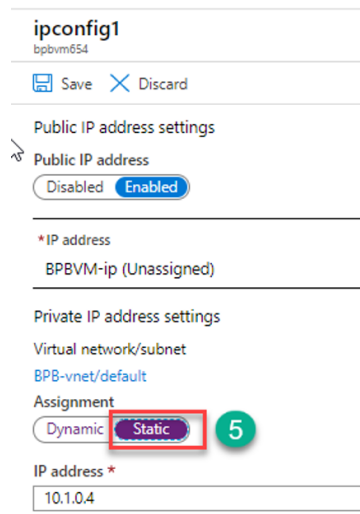
Let us understand how to make changes in IP addresses. For this, we will try to change dynamic IP to static IP. Follow the given steps:

1. Select the Azure VMs for which you want to change the IP address from dynamic IP to static IP.
2. Under the **Settings** tab, click on **Networking**.
3. Click on the NIC card name.
4. Go to the **IP configurations** tab.
5. Click on the IP address on the right-hand side of the screen. Take a look at *Figure 14.1*:



*Figure 14.1: Azure private IP configuration*

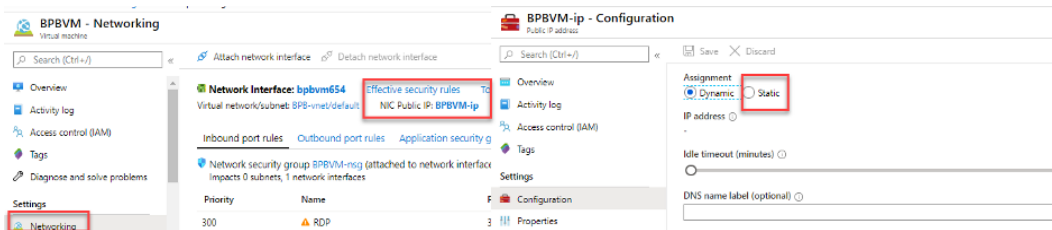
6. Change dynamic to static, and click on the **Save** button.
7. After a few minutes, your dynamic IP address will change to static IP, as shown in *Figure 14.2*:



*Figure 14.2: Azure private IP dynamic IP to static IP*

If you want to change the public IP address from dynamic IP to static IP, follow the given steps:

1. Go to the **Networking** tab.
2. Select the public IP address name and click on **Configuration**.
3. Change the selection from **Dynamic** to **Static**.
4. Now, your public IP address will change to static IP address. Take a look at *Figure 14.3*:



*Figure 14.3: Azure public IP dynamic IP to static IP*

## Network security group

Azure network security rules contain the setup of security rules and are used to allow or deny traffic in your Azure network. **Network Security Group (NSG)** is followed by two types of rules which are inbound and outbound rules, where you can define the port number, IP address, and source and destination for which you want to allow or deny the network traffic.

- **Inbound rule:** The network traffic that allows traffic from the internet to your VM is called an inbound rule. It can also allow calls/traffic to your VM from the outer world.
- **Outbound rule:** The network traffic that allows traffic from your VM to the internet is called an inbound rule. It denies calls/traffic to your VM from the outer world.

Let us see how to create a network security group and how to add an inbound and outbound rule:

1. Go to the marketplace and search for the **Network security group**.
2. Click on **Create**, as shown in *Figure 14.4*:

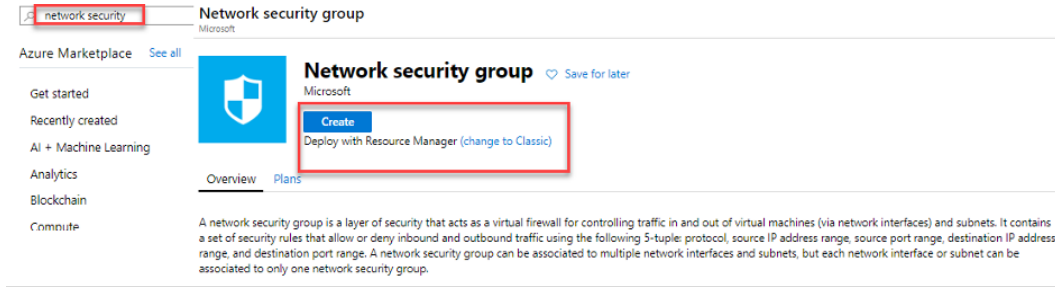


Figure 14.4: Network security group

3. Provide the network security group subscription and resource group.
4. Provide the security group name.
5. Select the region you want to create the NSG.
6. Click on **Review + create** the NSG. Take a look at Figure 14.5:

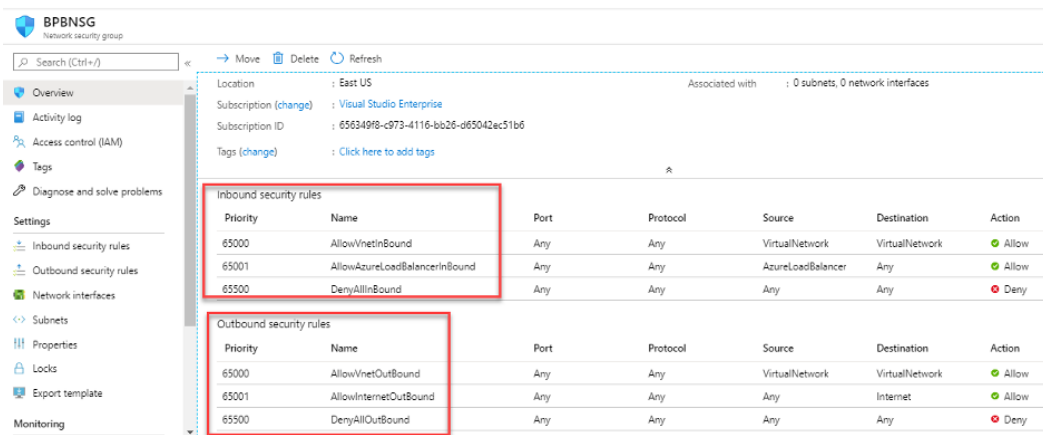
The screenshot shows the 'Create network security group' wizard in the 'Review + create' step. The 'Subscription' and 'Resource group' dropdowns are highlighted in red. The 'Name' field is set to 'BPBNSG' and the 'Region' is set to '(US) East US', both also highlighted in red. The 'Review + create' button is highlighted in red. The wizard includes tabs for 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is active, showing the 'Project details' and 'Instance details' sections.

Figure 14.5: Network security group creation

After a few minutes, your network security group will be created and it will look as follows:

- After the creation of NSG, the default rule will be created with the priority of 65000, 65001, and 65500.

- You can set the maximum rules that will be created up to 65500 and not more than that. Take a look at *Figure 14.6*:

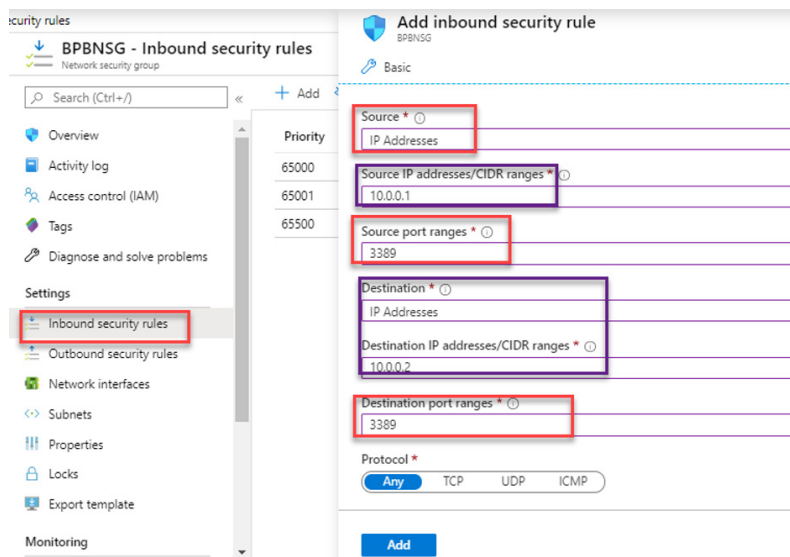


| BPBNSG Network security group                                      |                               |      |          |                   |                |        |              |
|--------------------------------------------------------------------|-------------------------------|------|----------|-------------------|----------------|--------|--------------|
| Location: East US Associated with: 0 subnets, 0 network interfaces |                               |      |          |                   |                |        |              |
| Subscription (change): Visual Studio Enterprise                    |                               |      |          |                   |                |        |              |
| Subscription ID: 656349f8-c973-4116-bb26-d65042ec51b6              |                               |      |          |                   |                |        |              |
| Tags (change): Click here to add tags                              |                               |      |          |                   |                |        |              |
| Inbound security rules                                             |                               |      |          |                   |                |        |              |
| Priority                                                           | Name                          | Port | Protocol | Source            | Destination    | Action |              |
| 65000                                                              | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  | Green circle |
| 65001                                                              | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | Allow  | Green circle |
| 65500                                                              | DenyAllInBound                | Any  | Any      | Any               | Any            | Deny   | Red circle   |
| Outbound security rules                                            |                               |      |          |                   |                |        |              |
| Priority                                                           | Name                          | Port | Protocol | Source            | Destination    | Action |              |
| 65000                                                              | AllowVnetOutBound             | Any  | Any      | VirtualNetwork    | VirtualNetwork | Allow  | Green circle |
| 65001                                                              | AllowInternetOutBound         | Any  | Any      | Any               | Internet       | Allow  | Green circle |
| 65500                                                              | DenyAllOutBound               | Any  | Any      | Any               | Any            | Deny   | Red circle   |

*Figure 14.6: Network security group default rule*

Let us create the inbound rules in NSG:

- Select the **Source** as IP Addresses, virtual network, or services tag.
- Provide the **Source IP addresses**.
- Provide the port number you want to allow.
- Provide the destination as IP Addresses, virtual network, or services tag, as shown in *Figure 14.7*:



**BPBNSG - Inbound security rules**

Search (Ctrl+/)

**Add inbound security rule**

Basic

Source \*

Source IP addresses/CIDR ranges \*

Source port ranges \*

Destination \*

Destination IP addresses/CIDR ranges \*

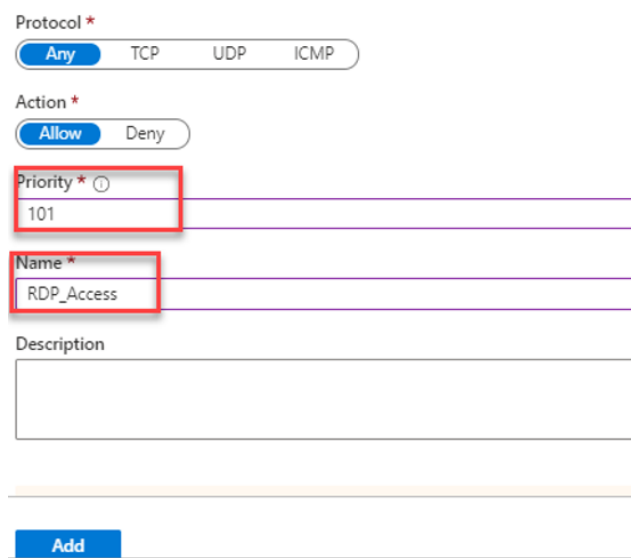
Destination port ranges \*

Protocol \* ☐ Any ☐ TCP ☐ UDP ☐ ICMP

**Add**

*Figure 14.7: Network security group inbound rule*

5. Select the action either as **Allow** or **Deny**.
6. Provide the priority 100 or above, as the NSG priority will start from 100 to 65500. The lower the priority, higher will be the importance, which means that the rule that has lower priority, such as 100, will be applied first.
7. Provide the name of NSG and description, and click on **Add**, as shown in Figure 14.8:



Protocol \*

Any TCP UDP ICMP

Action \*

Allow Deny

Priority \* ⓘ

101

Name \*

RDP\_Access

Description

Add

Figure 14.8: Network security group inbound rule

Similarly, if you need to create the outbound rule, you can follow the same steps as given in the inbound rule creation.

## Network security group association

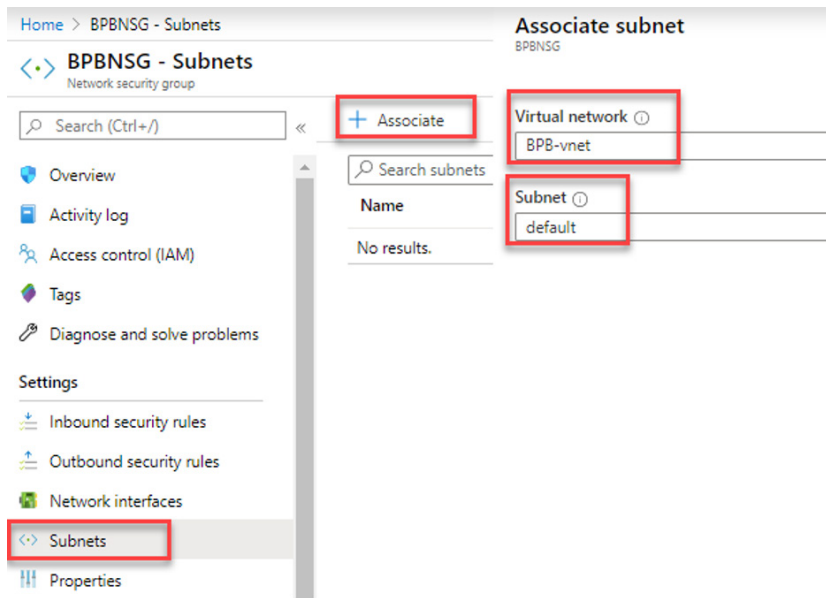
The network security group can be associated with Azure VMs, NICs and subnet levels.

NSG, when applied on the VM NIC card will have high priority. Let us understand this. If you create NSG rule 3389 in the subnet with allowed action and virtual NIC, you have NSG, which has denied rule with port number 3389. In that case, your traffic will drop as virtual machine NSG will have priority. You can allow the common ports to the subnet and block the specific port in VMs NIC NSG.

Let us see how to associate the NSG in the subnet:

1. Select the NSG you want to associate with the subnet.
2. Click on **Subnets** under the **Settings** tab.

3. Click on **+ Associate**.
4. Select the **Virtual network**.
5. Select the **Subnet** under the virtual network, which you want to associate the NSG with.
6. Click on **OK** to process further, as shown in *Figure 14.9*:



*Figure 14.9: Network security associate with subnet*

Let us see how to associate the NSG in the NIC card of the VM:

1. Select the **Networking** under the **Settings** tab.
2. Click on the NIC card.
3. Select the **Network security group** option under the **Settings** tab.
4. Click on **Edit**, as shown in *Figure 14.10*:

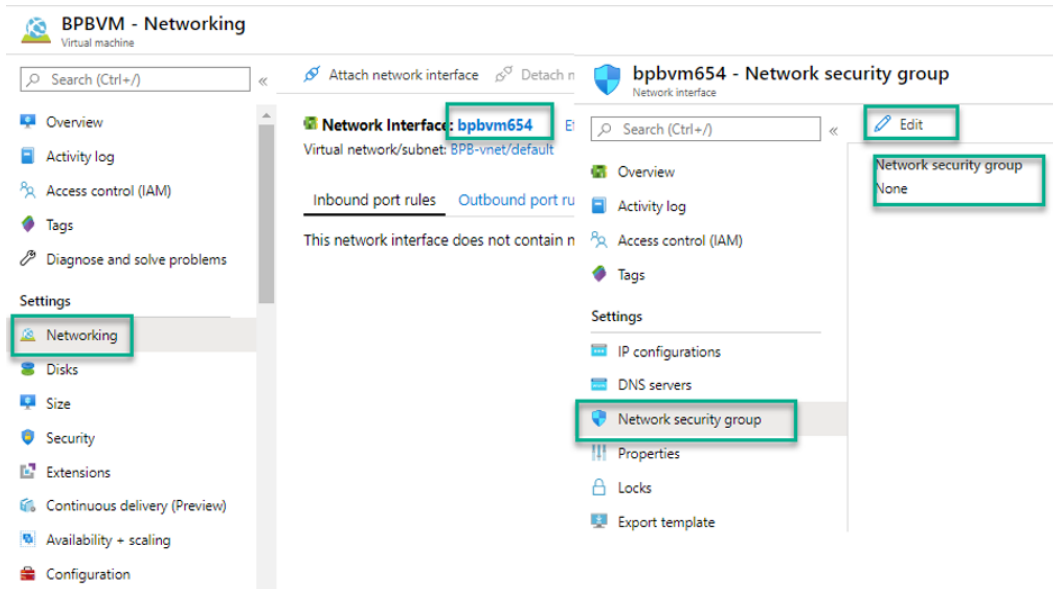


Figure 14.10: Network security associate with VM's NIC

5. Select the NSG and click on **Save**. After some time, NSG will be associated with the VMs NIC and you will be able to see all the rules, as shown in Figure 14.11:

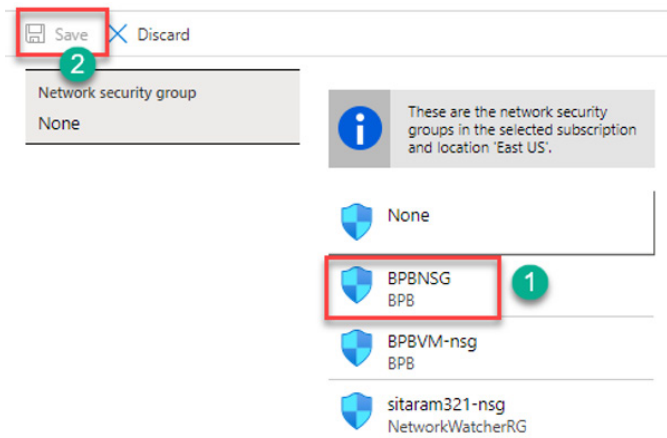


Figure 14.11: Network security in VM's NIC

## Route table

The Azure route table can be used to route the traffic in Azure and on-premises network. Routes will be created automatically when you create the subnet and

associate it automatically. You can create the custom routes to define how the traffic route use the route table. Let us say you have configured the firewall in-between the Azure and on-premises. You can configure the route table and set the rule, that all the traffic will firstly go to the firewall and then to the internet. Hence, you can control the network traffic in Azure and route it as per your organization standards.

Now, let us see how to create the route table and configure it. Follow these steps:

1. Search for Route tables in the marketplace.
2. Click on **+ Add**.
3. Provide the route table name.
4. Select the **Resource group** name and **Location**.
5. Click on **Create**. After some time, your route table will be created, as shown in *Figure 14.12*:

The screenshot displays the Azure portal interface for creating a route table. On the left, the 'Route tables' page shows a list with an '+ Add' button highlighted. Below the list, a message states 'No route tables to display' and provides instructions on when to create a route table. On the right, the 'Create route table' form is shown with the following details:

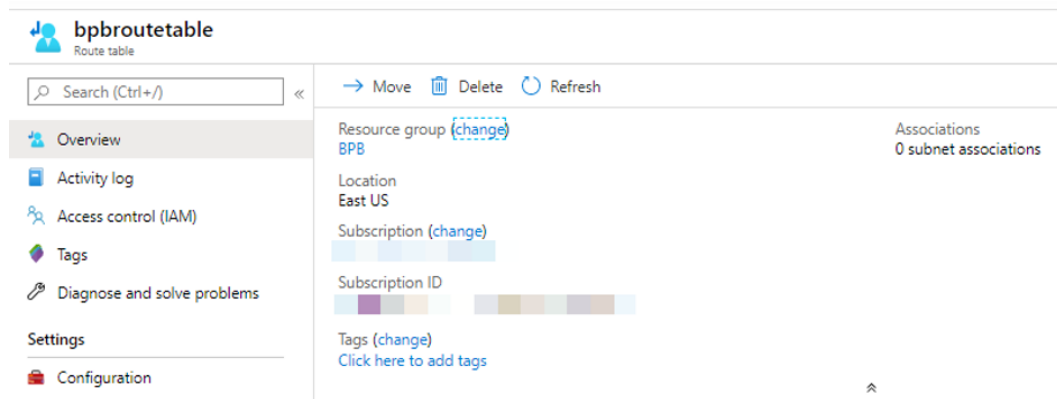
- Name \***: bpbrouetable
- Subscription \***: (selected)
- Resource group \***: BPE (selected from a dropdown list)
- Location \***: (US) East US (selected from a dropdown list)
- Virtual network gateway route propagation**: Enabled (selected from a toggle)

At the bottom of the form, there is a 'Create' button and a link to 'Automation options'.

*Figure 14.12: Route table creation*



Once the route table is created, it will look like *Figure 14.13*:

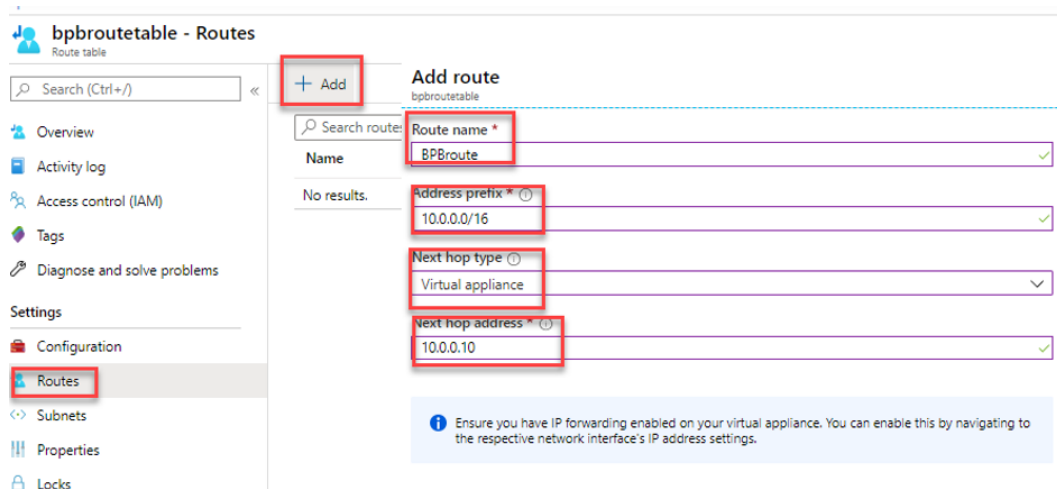


*Figure 14.13: Route table*

Now, we will configure the route table:

1. Click on **Routes** under the **Settings** section.
2. Click on **+ Add**.
3. Provide the name of the route table.
4. Provide the **Address prefix** range.
5. Select the virtual appliance (firewall), VNet, VNet gateway, and internet.
6. Click on **Add** to add routes.

Take a look at *Figure 14.14*:



*Figure 14.14: Route table configuration*

7. Once the route is configured, associate it with the subnet.
8. Select **Subnets** under the **Settings** tab.
9. Click on **+ Associate**.
10. Select the VNet.
11. Select the subnet from the drop-down menu.
12. Click on **OK** and associate the VNet. It will take some time to save the settings, as shown in *Figure 14.15*:

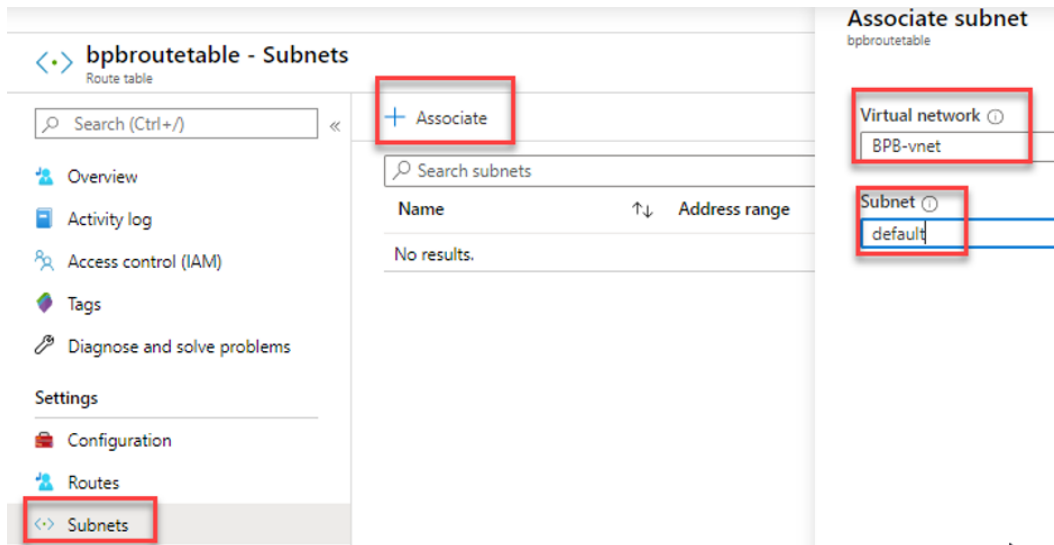


Figure 14.15: Route table subnet association

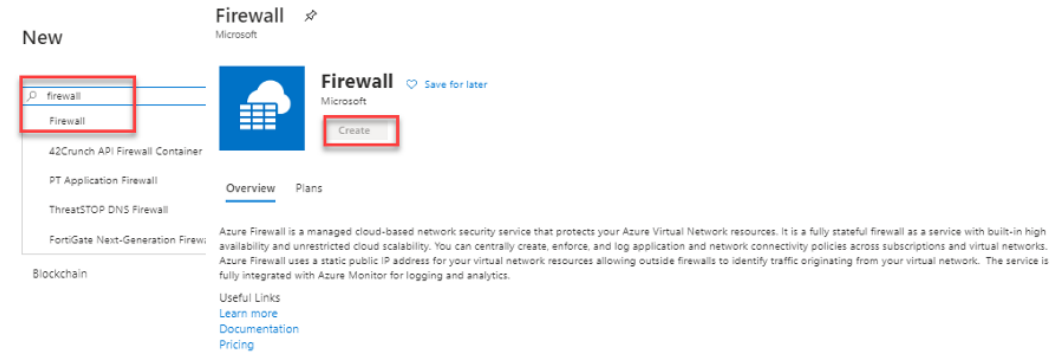
## Configure and deploy the Azure firewall

Azure firewalls manage the Azure network security and its services, which is managed by a virtual network. It is a fully stateful firewall as a service, which provides built-in high availability and cloud scalability.

The Azure firewall can be created centrally and managed to enforce the rules, log application, and network connectivity policies across subscriptions and virtual networks. The Azure firewall is fully integrated with the Azure Monitor, for logging and analytics purpose.

Let us see how to create the Azure firewall and configure it for our subscription:

1. Go to the marketplace or search for **Firewall**.
2. Click on the **Create** button, as shown in *Figure 14.16*:



*Figure 14.16: Azure firewall*

When you click on **Create**, follow the given steps and provide the details as follows:

- Subscription and resource group.
- Name of the firewall.
- Region and availability zone.
- If you want to use an existing or new VNet, select one as per your requirements.
- Provide the virtual network name and address space.
- Provide the subnet.
- Provide the firewall IP address and click on **Review + Create**.

- Once you provide all the details, click on **Review + Create**, as shown in Figure 14.17:

## Create a firewall

Basics Tags Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more.](#)

Project details

Subscription \*

Resource group \*  [Create new](#)

Instance details

Name \*  ✓

Region \*  ✓

Availability zone ⓘ  ✓

Choose a virtual network ☒ Create new ☐ Use existing

Virtual network name \*  ✓

Address space \*  ✓  
10.0.0.0 - 10.0.255.255 (65536 addresses)

Subnet

Subnet address space \*  ✓  
10.0.0.0 - 10.0.0.63 (64 addresses)

Firewall public IP address \*  [Add new](#)

Forced tunneling ⓘ ☐ Disabled

**Review + create** Previous Next : Tags > [Download a template for automation](#)

Figure 14.17: Azure firewall creation

It will take a few minutes to create the Azure firewall. Let us see how we can configure the Azure firewall rule. Go to the Azure firewall and follow the given steps:

1. Provide the name of the rule.
2. Provide the priority of the rule.

3. Provide the following details, as shown in *Figure 14.18*:
  - a. **Protocol**: TCP/UDP.
  - b. **Source type**: IP address/IP group.
  - c. Provide the **Source** and destination IP.
  - d. Provide the **Translated address** and **Translated Port**.

Once done, you will be able to create the NAT rule.

Add NAT rule collection ×

Name \*  ✓

Priority \*  ✓

Action Destination Network Address Translation (DNAT) ▾

Rules

| Protocol     | Source type  | Source                  | Destination Addr... | Destination Ports | Translated address | Translated port |
|--------------|--------------|-------------------------|---------------------|-------------------|--------------------|-----------------|
| TCP ▾        | IP address ▾ | 10.0.0.1 ✓              | 192.168.0.0 ✓       | 3389 ✓            | 192.168.0.0 ✓      | 3389 ✓          |
| 0 selected ▾ | IP address ▾ | *, 192.168.10.1, 192... | 192.168.10.0        | 8080              | 192.168.10.0       | 8080            |

*Figure 14.18: Azure firewall NAT rule creation*

Once we configure the NAT rule, it will allow the **Remote Desktop Protocol (RDP)** access to the services.

Let us try to configure an application rule, which helps to allow the URL or specific domain URL services such as **http://www.microsoft.com**, \*.windows.net, and so on. Follow the given steps:

1. Provide the name of the rule.
2. Provide the priority of the rule and action as either **Allow/Deny**.
3. Provide the following details, as shown in *Figure 14.19*:
  - a. **FQDN Tags** are as follows:
    - i. Name of the rule.
    - ii. Source type as either IP address/IP group.
    - iii. Source IP address.
    - iv. Add the tags in the drop-down menu.

b. **Target FQDNs** are as follows:

- i. Name of the rule.
- ii. Source type as either IP address/IP group.
- iii. Source IP address.
- iv. Protocol will be in **msql:1433, TCP:80**, and so on.
- v. Provide the target FQDN or URL you are trying to connect and then click on **Add**, as shown in *Figure 14.19*:

Add application rule collection ×

Name \* bpbrule ✓  
Priority \* 101 ✓  
Action \* Allow ✓

Rules  
FQDN tags

| name          | Source type  | Source                                     | FQDN tags       |
|---------------|--------------|--------------------------------------------|-----------------|
| externalapp ✓ | IP address ✓ | 192.168.0.0/24 ✓                           | WindowsUpdate ✓ |
|               | IP address ✓ | *, 192.168.10.1, 192.168.10.0/24, 192.1... | 0 selected ✓    |

*FQDN tags may require additional configuration. [Learn more.](#)*

| name       | Source type  | Source                            | Protocol:Port                     | Target FQDNs                   |
|------------|--------------|-----------------------------------|-----------------------------------|--------------------------------|
| Azurerue ✓ | IP address ✓ | * ✓                               | mssql:1433 ✓                      | www.microsoft.com ✓            |
|            | IP address ✓ | *, 192.168.10.1, 192.168.10.0/... | http, http:8080, https, mssql:... | www.microsoft.com, *.micros... |

**Add**

*Figure 14.19: Azure firewall application rule*

When you click on **Add**, your application rule will be added to the firewall and your Azure services will be able to access the specific target.

## Configure and deploy Azure Bastion services

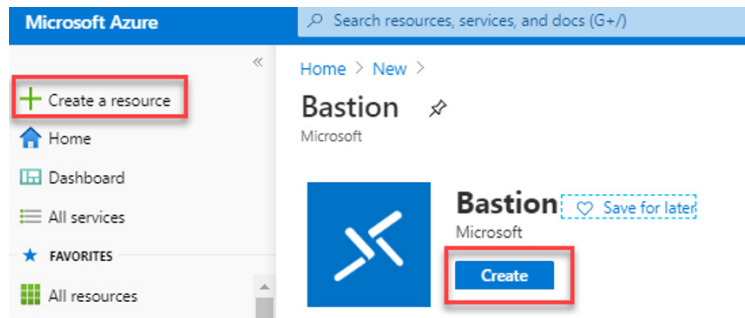
Azure Bastion provides a secure and seamless RDP/SSH access to your virtual machine in your Azure portal. It is a PaaS service, that has to be provisioned inside your virtual network. If you try and connect the VMs through Bastion services, then your VM does not require a public IP to be associated with it.

It provides the following features of the services:

- **RDP and SSH directly in Azure portal:** We can directly connect the RDP and SSH session from the Azure portal using a single click.
- **Remote session:** It uses an HTML5-based web client that is automatically streamed to your local device, so that we can connect to the RDP/SSH session over TLS on port 443.
- **Does not need a public IP to VM:** Azure Bastion opens the RDP/SSH connection to your Azure virtual machine using private IP on your VM. You do not need a public IP on your virtual machine.
- **No hassle of managing NSGs:** You do not require to manage the NSG rules and so on, as it is internally hardened to provide the RDP/SSH connection securely.

Let us just see how we can create the Azure Bastion services in Azure. Follow the given steps:

1. Go to the Azure portal.
2. Click on **Create a resource**.
3. Search for **Bastion** and click on **Create**, as shown in *Figure 14.20*:



*Figure 14.20: Azure Bastion*

4. When you click on **Create**, you will need to fill-up the following parameters:
  - a. Subscription.
  - b. Resources group.
  - c. Name.
  - d. Region.
  - e. Virtual network.
  - f. Subnet with the name of the Azure Bastion subnet with a prefix of at least with /27.
  - g. Provide public IP address details.

Refer to *Figure 14.21*:

### Create a Bastion

Basics Tags Review + create

Bastion allows web based RDP access to your vnet VM. [Learn more.](#)

**Project details**

Subscription \* Visual Studio Enterprise

Resource group \* BPB [Create new](#)

**Instance details**

Name \* azurebastionbpb ✓

Region \* East US

**Configure virtual networks**

Virtual network \* azurefirewall [Create new](#)

Subnet \* AzureBastionsubnet (10.0.1.0/27) [Manage subnet configuration](#)

**Public IP address**

Public IP address \* ☒ Create new ☐ Use existing

Public IP address name \* azurefirewall-ip ✓

Public IP address SKU Standard

Assignment ☐ Dynamic ☒ Static

[Review + create](#) Previous Next : Tags > [Download a template for automation](#)

*Figure 14.21: Azure Bastion creation*

Once you are done with the Azure Bastion services creation, verify the services connecting to RDP over the browser. Click on the Azure VM, and then follow the given steps:

1. Go to the Azure VM settings.
2. Then, click on **Connect**.
3. Select **BASTION**.
4. Provide the user ID/password, as shown in *Figure 14.22*:



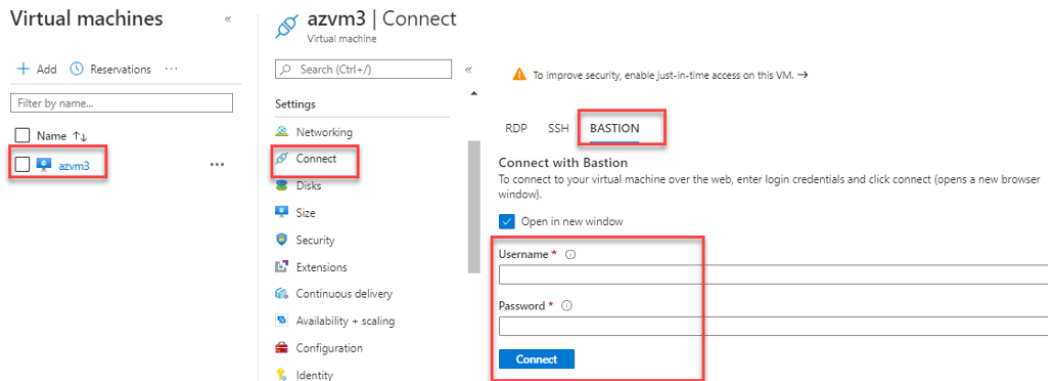


Figure 14.22: Azure Bastion verification

When you click on **Connect**, you will be able to connect to the VM, as shown in Figure 14.23:

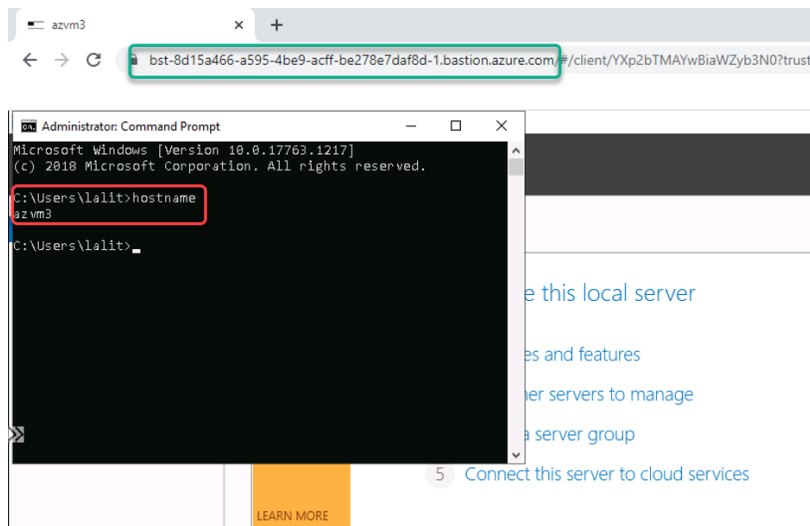


Figure 14.23: Azure Bastion RDP access

Now, we can access the VM using the Bastion services.

## Evaluate effective security rules

Network security group effective rules will help you to understand the rules that have been enabled in inbound/outbound on the same page. You can review all those NSG rules at a one-shot. Let us now see how we can see those rules.

Go to the network security group, select the **Network security group** option and follow the given steps:

1. Go to **Support + troubleshooting**.
2. Then, click on the effective security rules.

It will show which VM NSG has been attached, as well as the rules. You can download those rules, as shown in *Figure 14.24*.

After downloading the rules, you can review all the rules. You will also be able to understand the rules that result in a mismatch, as per your requirements.

**azvm3-nsg | Effective security rules**

Network security group

Search (Ctrl+/) Download Refresh

Showing only top 50 security rules in each grid, click Download above to see all.

Select a network interface below to see the effective security rules and network security groups associated with it.

Scope: Network security group (azvm3-nsg)

Virtual machine: azvm3

Network interface: azvm3272

Click on a rule row to see the expanded list of prefixes.

**azvm3-nsg** azvm3-nsg

**Inbound rules**

| Name                          | Priority | Source                           | Source Ports | Destination                  | Destination Ports |
|-------------------------------|----------|----------------------------------|--------------|------------------------------|-------------------|
| RDP                           | 300      | 0.0.0.0/0,0.0.0.0/0              | 0-65535      | 0.0.0.0/0,0.0.0.0/0          | 3389-3389         |
| AllowVnetInBound              | 65000    | Virtual network (2 prefixes)     | 0-65535      | Virtual network (2 prefixes) | 0-65535           |
| AllowAzureLoadBalancerInBound | 65001    | Azure load balancer (2 prefixes) | 0-65535      | 0.0.0.0/0,0.0.0.0/0          | 0-65535           |
| DenyAllInBound                | 65500    | 0.0.0.0/0,0.0.0.0/0              | 0-65535      | 0.0.0.0/0,0.0.0.0/0          | 0-65535           |

**Outbound rules**

| Name                  | Priority | Source                       | Source Ports | Destination                  | Destination Ports |
|-----------------------|----------|------------------------------|--------------|------------------------------|-------------------|
| AllowVnetOutBound     | 65000    | Virtual network (2 prefixes) | 0-65535      | Virtual network (2 prefixes) | 0-65535           |
| AllowInternetOutBound | 65001    | 0.0.0.0/0,0.0.0.0/0          | 0-65535      | Internet (216 prefixes)      | 0-65535           |
| DenyAllOutBound       | 65500    | 0.0.0.0/0,0.0.0.0/0          | 0-65535      | 0.0.0.0/0,0.0.0.0/0          | 0-65535           |

*Figure 14.24: Effective security rules*

Now, we are able to see how we can evaluate effective security rules.

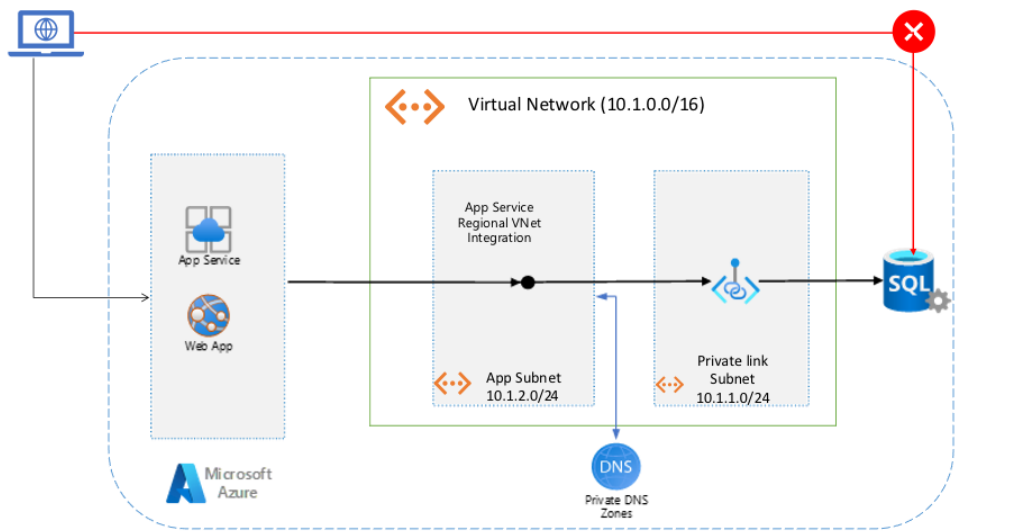
## Azure Private Network

Azure private endpoint is a network interface which provides the private IP address from your virtual network, which helps to connect the services privately and securely. While enabling the private endpoint, you are bringing the Azure services within your virtual network. Private endpoint supports the following services:

- AI+ML services
- Analytics services

- Web services
- Database services
- Compute services
- Containers services
- Integration services
- **Internet of Things (IOT)** services
- Management and governance services
- Security services
- Storage services

Moreover, if you can see, in the following *Figure 14.25*, public connectivity to sql DB (database) is blocked. We need to enable the secure channel through vnet to connect to database from web services. That is how the private endpoint works.



*Figure 14.25: Private endpoint*

Let us see how to enable the private endpoint for one of the services. Follow the steps to create a private endpoint and configure for storage account:

1. Click on **Create a resource**.
2. Search for **Private Endpoint**.
3. Click on **Create** for the option of private endpoint in the drop down menu.

For more information, refer to Figure 14.26:

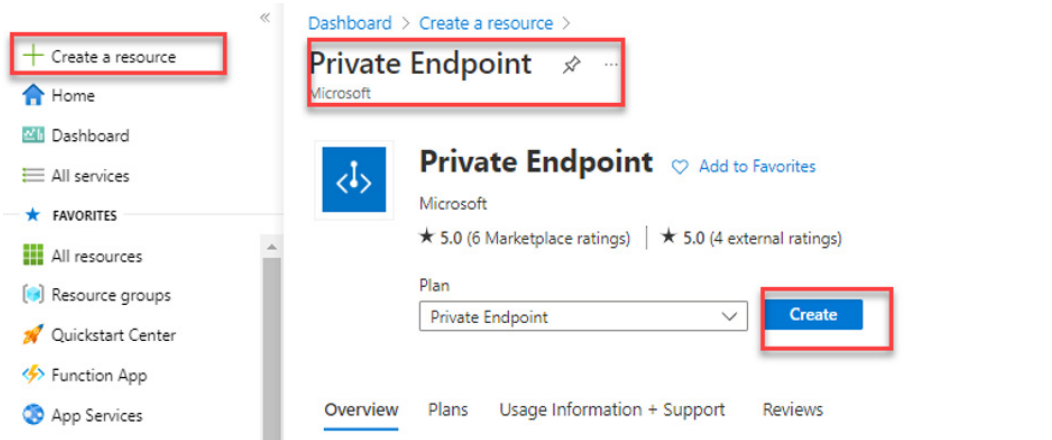


Figure 14.26: Private endpoint creation

4. Provide the Subscription details, resources group name, and name of the private endpoint.
5. Do provide the name of the network interface.
6. Select the region where you want your services to be deployed or where you want to configure the private endpoint.

Refer to Figure 14.27:

**1 Basics** 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

**Project details**

Subscription \* ⓘ

Resource group \* ⓘ

**Instance details**

Name \* bpbstoragepie ✓

Network Interface Name \* bpbstoragepie-nic ✓

Region \* East US ✓

Figure 14.27: Private endpoint resources details

7. Select the resources here. You will get two options; either provide the resources ID or use Azure resources in m directory.
8. Choose the subscription and resources type from the drop down menu.
9. Select the resources and sub resources, such as storage account and blob, file, table, queue, and so on.

Refer to *Figure 14.28*:

✓ Basics **2 Resource** 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Connection method ⓘ

☒ Connect to an Azure resource in my directory.

☐ Connect to an Azure resource by resource ID or alias.

Subscription \* ⓘ

Resource type \* ⓘ

Resource \* ⓘ

Target sub-resource \* ⓘ

*Figure 14.28: Private endpoint storage account*

10. Provide the Vnet details and select the subnet.
11. Select the IP address dynamically or statically. The IP address is based on your organization's need.

Refer to *Figure 14.29* for more details:

✓ Basics ✓ Resource **3 Virtual Network** 4 DNS 5 Tags 6 Review + create

**Networking**

To deploy this private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network \* ⓘ

Subnet \* ⓘ

Network policy for private endpoints Disabled ([edit](#))

**Private IP configuration**

☒ Dynamically allocate IP address

☐ Statically allocate IP address

**Application security group**

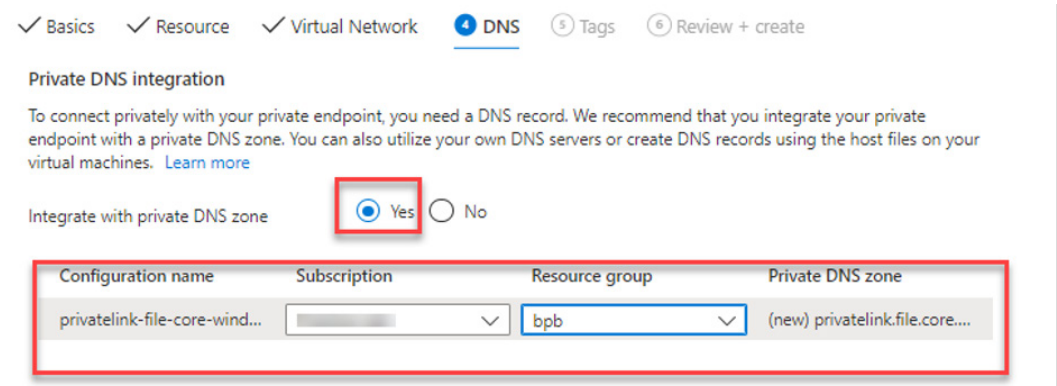
Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)

*Figure 14.29: Private endpoint Vnet configuration*

12. You will have to click on integrate with private DNS to be yes. That is how your private IP address is going to resolved locally or within vnet.

13. Then, select next.

Refer to *Figure 14.30*:



✓ Basics ✓ Resource ✓ Virtual Network **4 DNS** 5 Tags 6 Review + create

**Private DNS integration**

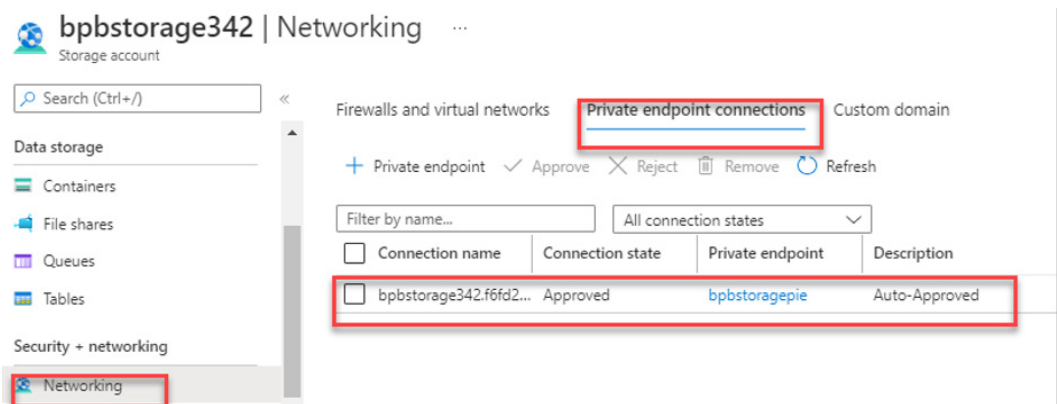
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

| Configuration name            | Subscription         | Resource group | Private DNS zone               |
|-------------------------------|----------------------|----------------|--------------------------------|
| privatelink-file-core-wind... | <input type="text"/> | bpb            | (new) privatelink.file.core... |

*Figure 14.30: Private endpoint DNS configuration*

7. Provide the tags name.
8. Then click on review and create. After some time, private endpoints will be created.
9. You can validate the private endpoint created and approved while going to storage accounts.
10. In the **Networking** section, select the **Private endpoint connections** and you can find the private endpoint connection, as shown in *Figure 14.31*:



bpbstorage342 | Networking ...

Storage account

Search (Ctrl+/)

«

Firewalls and virtual networks **Private endpoint connections** Custom domain

+ Private endpoint ✓ Approve ✗ Reject 🗑 Remove 🔄 Refresh

Filter by name... All connection states

| <input type="checkbox"/> | Connection name        | Connection state | Private endpoint | Description   |
|--------------------------|------------------------|------------------|------------------|---------------|
| <input type="checkbox"/> | bpbstorage342.f6fd2... | Approved         | bpbstoragepie    | Auto-Approved |

*Figure 14.31: Private endpoint validation*

## Conclusion

In this chapter, we discussed the configuration of private and public IP addresses and learned how to change the IP address from dynamic to static. We then discussed the Azure network security group and how to associate with the subnet/VM NIC card. We covered the route table and learned how it can be used to route the traffic.

We will discuss the Azure network monitoring in the next chapter. We will explain the network watcher and on-premises to Azure network connectivity monitoring, and so on. We have also covered private endpoint in this chapter, which will help you learn how to connect azure services more securely and privately.

## Points to remember

- Azure bastion is a fully managed services that provides the secure and seamless **Remote Desktop (RDP)** and **Secure Shell Connection (SSH)** connection to virtual machines without exposing to internet.
- Azure route table allows you to create custom route, so that if required, you can route the traffic to firewall, Vnet, Vnet gateway, and so on.
- Azure Firewall is a cloud based, intelligent, network firewall security service, that provides the best threat protection for cloud workloads that are running in Azure.
- Azure private endpoints enable 1 to 1 communication between the Azure services and provides more security connectivity.

## Multiple choice questions

1. **A customer wants to enable the secure RDP connection. Which solution should they chose?**
  - a. Add the public IP and enable the NSG.
  - b. Azure firewall.
  - c. Azure bastion services.
2. **Which is the cloud based intelligent security service, that helps to manage end to end traffic?**
  - a. NSG.
  - b. Private and public IP.
  - c. Azure firewall.

## Answers

1. c
2. c



# CHAPTER 15

# Monitoring and Troubleshooting of Virtual Networking

## Introduction

In this chapter, we will discuss Azure Network Watcher and its usage. We will also discuss how to troubleshoot the on-premises connectivity using the network watcher.

We will cover network performance monitoring, how to use the IP flow verify, VPN troubleshooting, packet capture, and so on.

## Structure

The following topics will be covered in this chapter:

- Network Watcher
- Monitor on-premises connectivity
- Network performance monitor

## Objectives

In this chapter, you will learn about Azure Network Watcher. If your customer is troubleshooting a network issue from the Azure network to on-premises, then

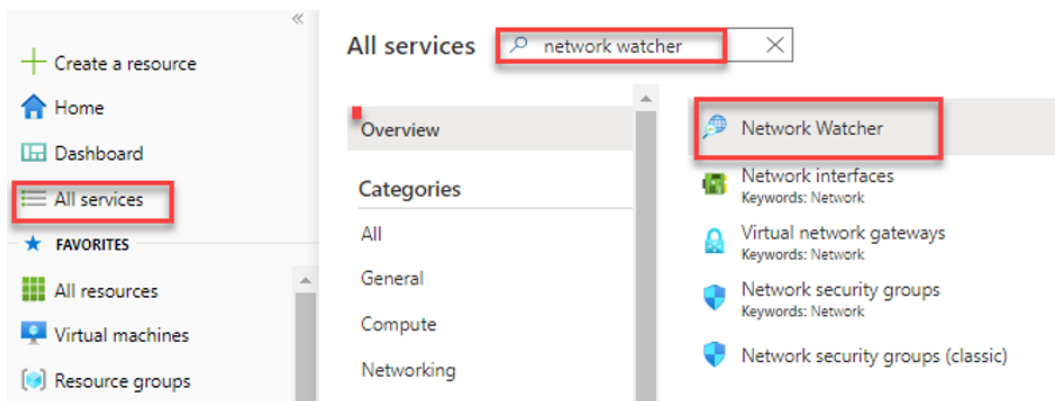
Azure Network Watcher will help your customer trace the traffic at various levels and therefore help you. We will describe the network watcher capabilities in detail, in the further course of this chapter.

## Network watcher

Azure Network Watcher provides the tools to monitor, diagnose, and view the metrics. We can enable or disable the logs in the network watcher. It is designed to monitor and repair the Azure infrastructure services, which includes the Azure virtual machine, virtual network, application gateway, and so on.

Let us see how we can implement the Azure Network Watcher services. Follow the given steps:

1. Go to **All services** and search for **network watcher**. Select the **Network Watcher** option, as shown in *Figure 15.1*:



*Figure 15.1: Network watcher*

2. Once you click on **Network Watcher**, please enable it for the regions you want to select it for. Let us follow the given steps to enable it:
  - a. Click on **Overview**.
  - b. Select the region and click on the **Overview** tab to enable the network watcher.
  - c. It will take some time to enable it.

Refer to Figure 15.2:

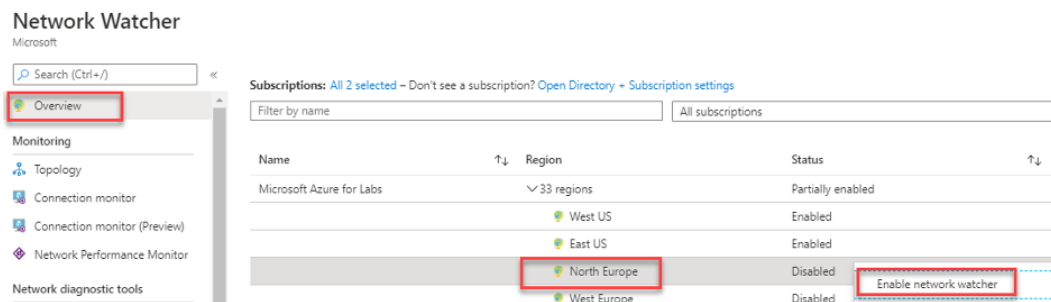


Figure 15.2: Network watcher enable

## Network Watcher topology

Under the **Monitoring** tab, if you click on **Topology**, it will show you the complete architect connectivity of your VNet, which connects to all the resources such as VM, application gateway, and so on. Refer to Figure 15.3:

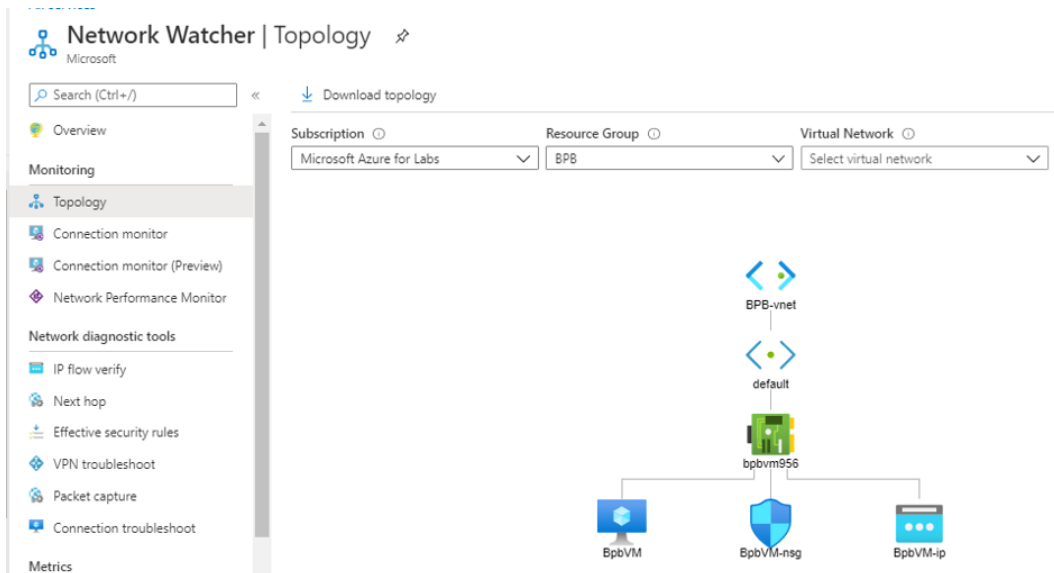


Figure 15.3: Network watcher enable

## Monitor on-premises connectivity

Using **Connection monitor**, we will monitor the traffic between two virtual machines or between the Azure VM and the on-premise server. We can monitor the **Fully Qualified Domain Name (FQDN)** or individual IP address as well. Once you

select the connection monitoring, follow the given instructions to add the monitoring:

1. Provide the name of the monitor.
2. Select the subscription.
3. Select the virtual machine.
4. Select the destination as **Select a virtual machine** or **Specify manually** (URI, FQDN, or IPv4).
5. Select the port number for which you want to monitor the services.
6. Click on **Add**, as shown in *Figure 15.4*:

The screenshot shows the 'Add connection monitor' interface in the Azure Network Watcher portal. The left-hand navigation pane has 'Connection monitor' highlighted. The main form contains the following fields and options:

- Name \***: monitor
- Subscription \***: (Dropdown menu)
- Virtual machine \***: BpbVM
- Destination**:
  - ☐ Select a virtual machine
  - ☒ Specify manually
- URI, FQDN or IPv4 \***: bpb.com
- Port \***: 3389
- Advanced settings**: (Expandable section)
- Add**: (Blue button at the bottom right)

*Figure 15.4: Network watcher connection monitor*

After you click on **Add**, you will be able to see the connectivity of each service when you click on a specific monitor. Take a look at *Figure 15.5* for more details:

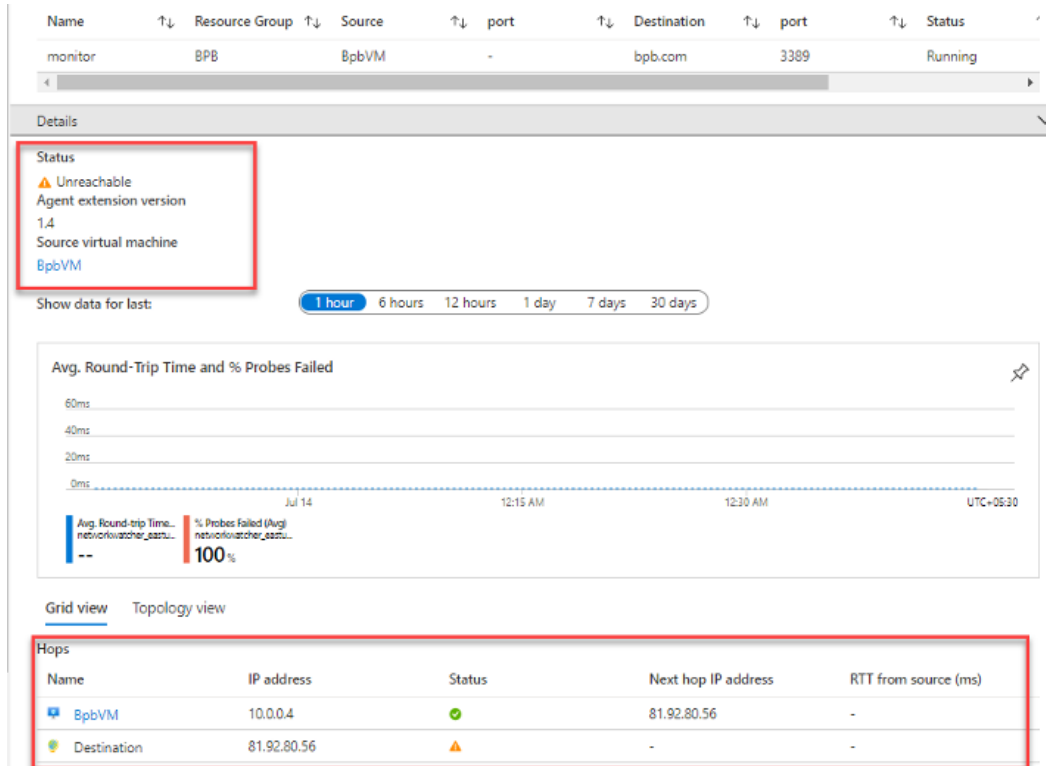


Figure 15.5: Network watcher connection monitor status

## IP flow verify

IP flow verify helps you to track the packets, and checks whether the packets have been allowed or denied. Click on **IP flow verify** under the **Network diagnostic tools** section and provide the following details:

- **Subscription**
- **Resource group**
- **Virtual machine**
- **Direction: Inbound or Outbound**
- Provide the **Local IP address** and **Remote IP address** with the port number to verify.
- Click on the **Check** button.

For more details, take a look at *Figure 15.6*:

**Network Watcher | IP flow verify**  
Microsoft

Search (Ctrl+/)

Connection monitor  
Connection monitor (Preview)  
Network Performance Monitor

**Network diagnostic tools**

IP flow verify  
Next hop  
Effective security rules  
Effective security rules  
Effective security rules  
Effective security rules  
VPN troubleshoot  
Packet capture  
Connection troubleshoot

**Metrics**

Usage + quotas

**Logs**

NSG flow logs  
Diagnostic logs  
Traffic Analytics

Network Watcher IP flow verify checks if a packet is allowed or denied to or from a virtual machine based on 5-tuple information. The security group decision and the name of the rule that denied the packet is returned.  
[Learn more.](#)

Specify a target virtual machine with associated network security groups, then run an inbound or outbound packet to see if access is allowed or denied.

Subscription \*

Resource group \*   
BpB

Virtual machine \*   
BpbVM

Network interface \*  
bpbvm956

**Packet details**

Protocol  
☒ TCP ☐ UDP

Direction  
☒ Inbound ☐ Outbound

Local IP address \*   
10.0.0.4

Local port \*   
80

Remote IP address \*   
192.168.0.0

Remote port \*   
80

**Check**

Access denied

Security rule  
DenyAllInBound

*Figure 15.6: Network watcher IP flow*

## Next hop

Next hop will help you identify the next hop and IP address of the packet, from a specific VM and NIC card. It will help you to determine whether the traffic has been directed to a specific destination or not.

Next hop helps you to identify where your traffic has been routed to, in the virtual network, virtual appliance, or system route, and so on. Take a look at *Figure 15.7*:

**Network Watcher | Next hop**  
Microsoft

Search (Ctrl+/)

- Connection monitor
- Connection monitor (Preview)
- Network Performance Monitor

**Network diagnostic tools**

- IP flow verify
- Next hop**
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

**Metrics**

- Usage + quotas

**Logs**

- NSG flow logs
- Dagnostic logs

Next Hop provides the next hop from the target virtual machine to the destination IP address. [Learn more.](#)

Specify a target virtual machine and destination IP address to view the next hop.

Subscription \* ⓘ

Resource group \* ⓘ  
BPP

Virtual machine \* ⓘ  
BpbVM

Network interface \*  
bpbvm956

Source IP address \* ⓘ  
10.0.0.4

Destination IP address \* ⓘ  
10.0.0.5

**Next hop**

Figure 15.7: Network watcher next hop

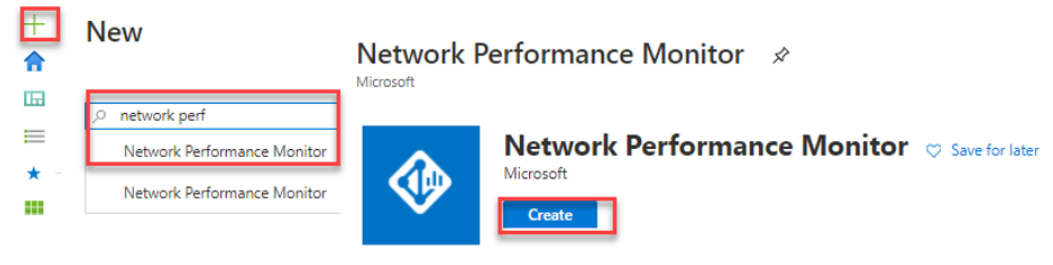
## Network performance monitor

The network performance monitor helps us to monitor the Azure express route traffic. It is a cloud-based hybrid monitoring solution which helps to monitor the various points of the network infrastructure.

Let us take a look at how to configure the Azure network and performance monitor, by following the given steps:

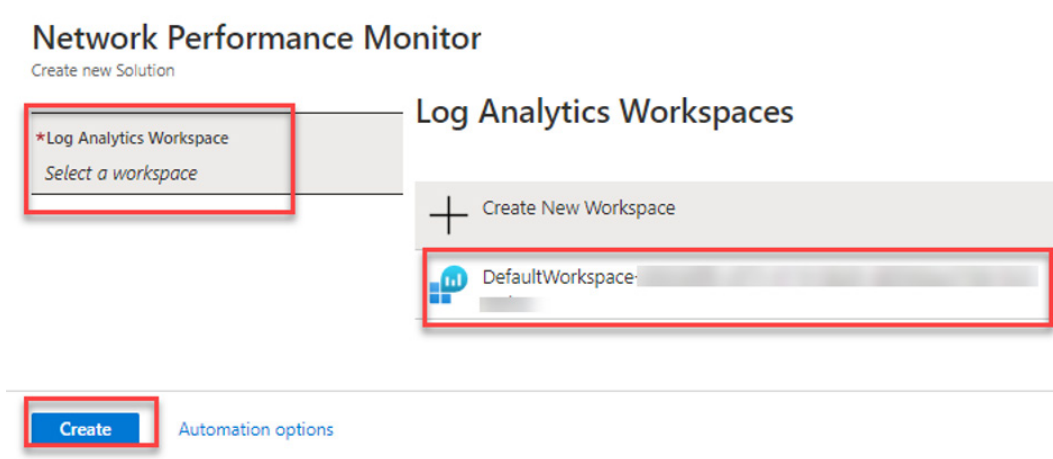
1. Click on the + sign.
2. Search for **Network Performance Monitor**.
3. Click on **Create**.

Look at *Figure 15.8* for more details:



*Figure 15.8: Network performance monitor*

4. Select **Log Analytics Workspace**.
5. Once you select the workspace, click on **Create New Workspace**, as shown in *Figure 15.9*. It will take up to 5 minutes to create the network performance monitor.



*Figure 15.9: Network performance monitor creation*

6. Once the network performance monitor is created, you can check it in log analytics.
7. In log analytics, you will see that one solution has been deployed in the **Overview** tab, which is the network performance monitor. Let us try and configure it. Click on **Solution requires additional configuration** under the **Network Performance Monitor** tab on the right-hand side of the **Overview** section.

Refer to *Figure 15.10*:



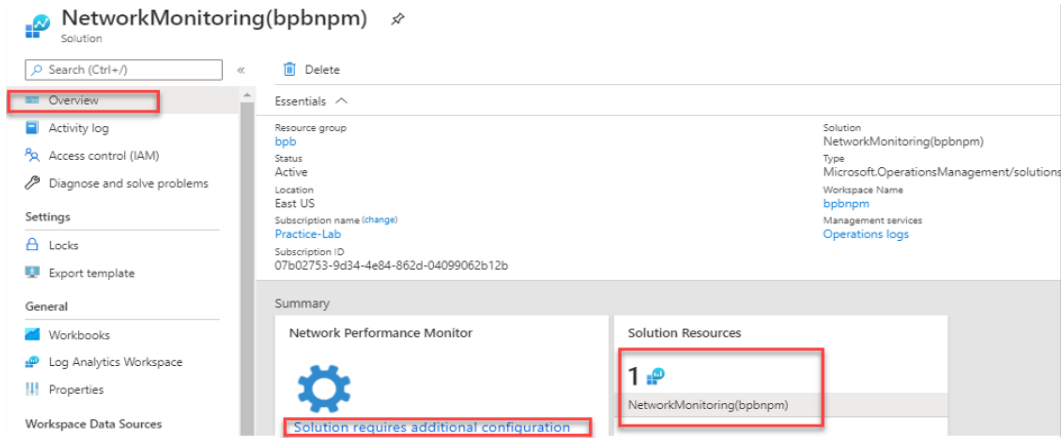


Figure 15.10: Network performance monitor overview

8. When you click on **Solution requires additional configuration**, one window will open up with the network performance monitor configuration, where you need to configure the following services, including the express route:
  - a. You can download the agent and install it on the stand-alone VMs/ devices to configure the monitor.
  - b. You can set up the performance monitor.
  - c. You can configure the services connectivity monitor for network devices.
  - d. You can set up the express route monitor to get the traffic of the express route and fix the issue when it arrives.

Once all the preceding configurations are done, you will start getting the data within 24 hrs in log analytics. We have now successfully configured the network performance monitoring in the Azure environment.

Take a look at Figure 15.11:

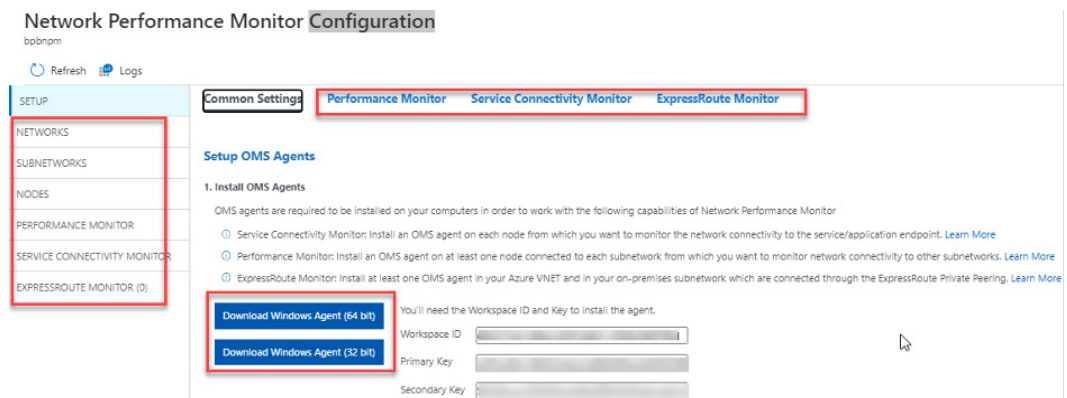


Figure 15.11: Network performance monitor configuration

## Conclusion

In this chapter, we discussed Azure Network Watcher and its usage, how to troubleshoot the network using various tools, how to troubleshoot the on-premises network and Azure connectivity, and how the IP flow verify and next hop will help your on-network troubleshooting. We also discussed the Azure network performance monitor and how to configure it.

In the next chapter, we will discuss the Azure monitor and its subsets, to analyze the utilization and consumption of the Azure services. We will also discuss how to set up alerts in Azure environments.

## Points to remember

- Azure network watcher provides the tools to monitor, diagnose, view metrics for network troubleshooting.
- Network watcher will help you repair and monitor the network health.

## Multiple choice questions

1. **A customer wants to troubleshoot some Azure network related issue. Which tool should they choose?**
  - a) AzMon
  - b) Network watcher
  - c) Log analytics
2. **What is next hop?**
  - a) Where is your traffic
  - b) How your traffic floating
  - c) Where the traffic has been sent

## Answers

1. **b**
2. **c**

# CHAPTER 16

# Analyzing Resource Utilization and Consumption

## Introduction

In the previous chapter, we covered how to create and manage the different types of Azure subscriptions and resources. In this chapter, we will learn about Azure monitor, its utilization of the resources and how to monitor the different services using Azure Log Analytics. We will also learn how to use the log search query functions in the log analytics space.

## Structure

The following topics will be covered in this chapter:

- Azure Monitor
- Setup and configuration of Azure alerts
- Azure Metrics
- Azure Services Health
- Diagnostoc logs
- Azure Log Analytics

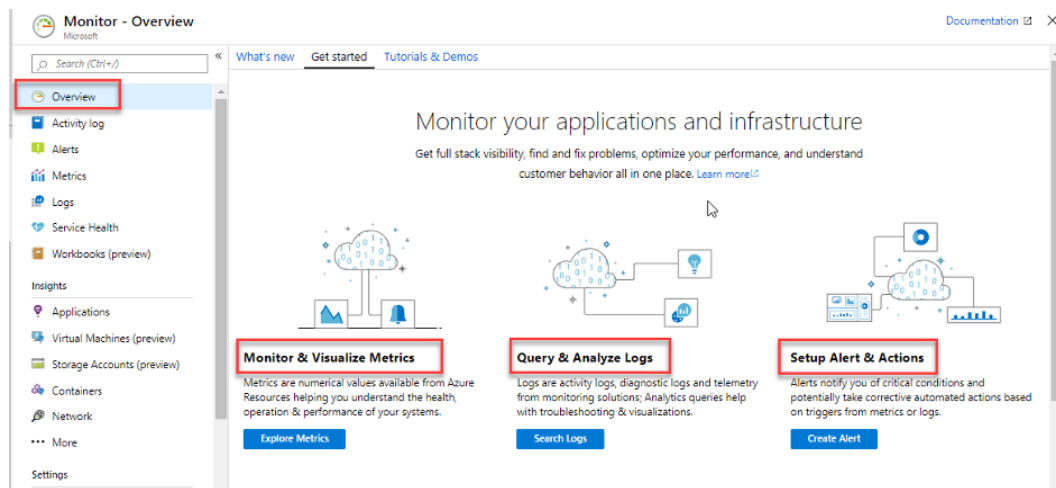
# Objectives

We will cover Azure Monitor in detail, which will help you set up the monitoring alerts for your Azure subscription resources. We will then also discuss how to set up and configure the alerts, which will help you send the notifications.

## Azure Monitor

Azure Monitor is a comprehensive solution for all the Azure services, that reside in the Azure subscription, and it uses various tools to monitor the IaaS, PaaS, and SaaS components. It collects the logs data, application performance data, and so on, to provide the best result for services, and based on them, the customer can get notified.

For more details, take a look at *Figure 16.1*:



*Figure 16.1: Azure Monitor*

Azure Monitor supports a variety of Azure resource collection data, which provides the metrics/alerts on the Azure portal. The types of data provided by Azure monitors are as follows:

- **Application monitoring data:** It collects consistent data of application functionality, performance, and maintenance, with respect to application code-related issues.
- **Guest OS monitoring data:** It collects data of Azure VMs running on the subscription, and also has an application running on it.
- **Resource monitoring data:** It collects the application resource operation data.

- **Subscription monitoring data:** It collects the complete subscription data, including Azure resources health of the Azure services, in terms of the region, and so on.
- **Tenant monitoring data:** It collects the tenant level data such as any operations or any issues that may have occurred on your Azure AD services.
- **Activity logs:** Activity logs are simply the activities that have been performed by the user or owner in terms of all the services. They will be collected and recorded. Refer to *Figure 16.2*:

| OPERATION NAME                         | STATUS    | TIME    | TIME STAMP      | SUBSCRIPTION   | EVENT INITIATED BY          |
|----------------------------------------|-----------|---------|-----------------|----------------|-----------------------------|
| Update linked services under given wor | Succeeded | 4 h ago | Sat Oct 05 2... | MSDN Platforms | Windows Azure Security R... |
| Update linked services under given v   | Started   | 4 h ago | Sat Oct 05 2... | MSDN Platforms | Windows Azure Security R... |

Figure 16.2: Activity logs

## Setup and configuration of Azure alerts

If you would like to configure an alert of your services, follow the given steps:

1. Click on **Alerts**, and then click on **+ New alert rule** under Azure Monitor or resources, as shown in *Figure 16.3*:

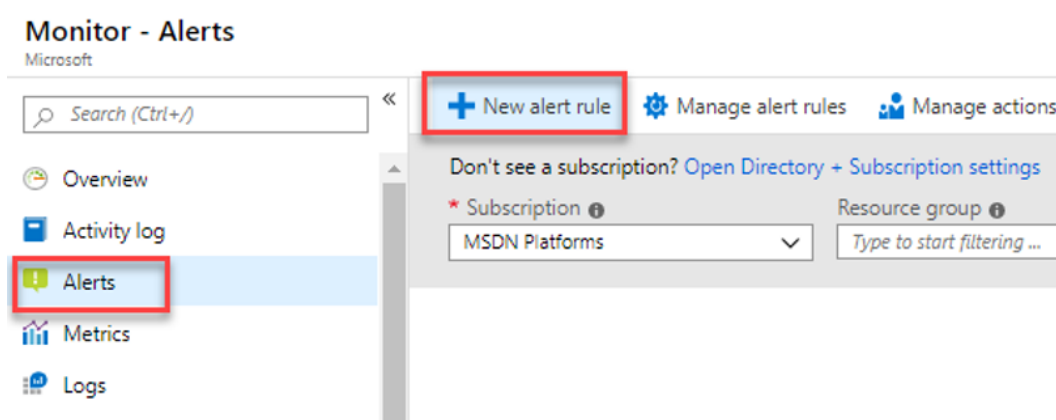


Figure 16.3: New alert

2. Select resources like subscription, VMs, and so on for alert creation, as shown in Figure 16.4:

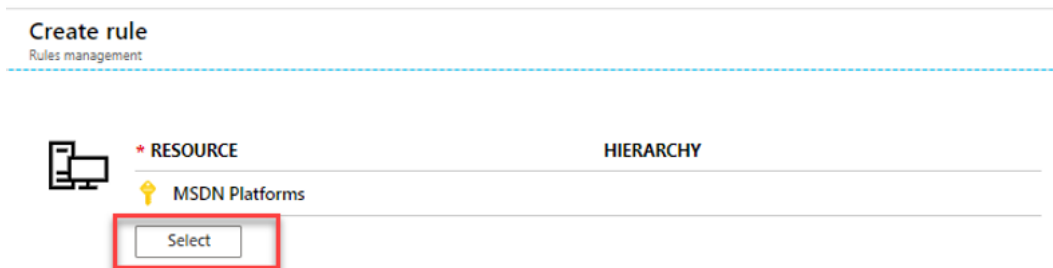


Figure 16.4: Alert creation

3. Select the condition under all administrative logs, specific resources logs, and so on, to add the condition. Refer to Figure 16.5:

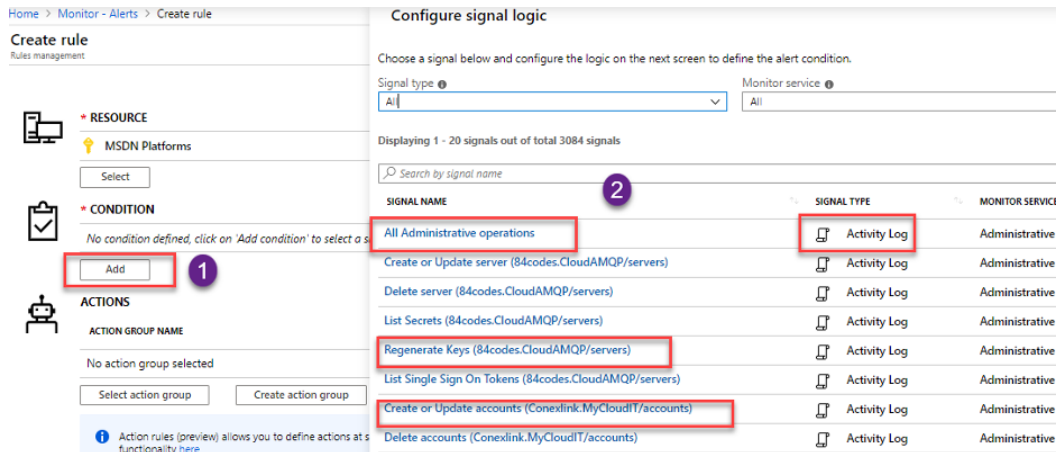


Figure 16.5: Alerts rules

4. Click on the action group and do the following:
  - a. Provide the action group name.
  - b. Short name of maximum 116 characters.
  - c. Subscription name.
  - d. Resource group name.
  - e. Action name like where or how to get an alert:
    - i. **Automation Runbook**
    - ii. **Azure Function**
    - iii. **Email/SMS/Push/Voice**

- iv. **ITSM** like services ticketing tool
- v. **Webhook** and other services

5. Add action group details, as shown in *Figure 16.6*:

**Add action group**

\* Action group name ⓘ

\* Short name ⓘ

\* Subscription ⓘ

\* Resource group ⓘ

**Actions**

| ACTION NAME                                             | ACTION TYPE           |
|---------------------------------------------------------|-----------------------|
| <input type="text" value="Unique name for the action"/> | Select an action type |

Privacy Statement

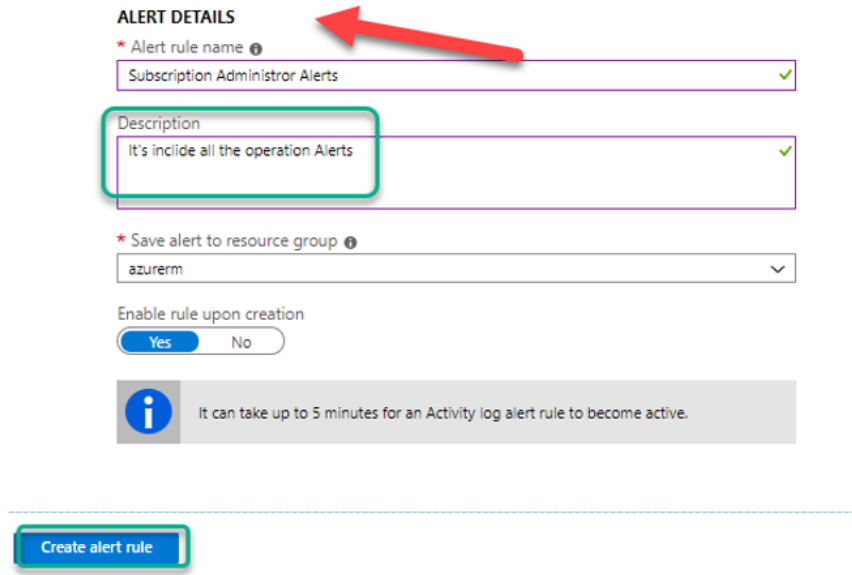
Pricing

Have a consistent format in emails, notifications and other end...

*Figure 16.6: Add action details*

- 6. Click on **OK**.
- 7. Provide the details of the alert:
  - a. Alert rule name.
  - b. Description.
  - c. Save alert to the resource group name.
  - d. Enable or disable rule on creation.
  - e. Click on **Create alerts rule**.

For more details on alerts, take a look at *Figure 16.7*:



**ALERT DETAILS**

\* Alert rule name ⓘ  
Subscription Administrator Alerts ✓

Description  
It's include all the operation Alerts ✓

\* Save alert to resource group ⓘ  
azurerm ▼

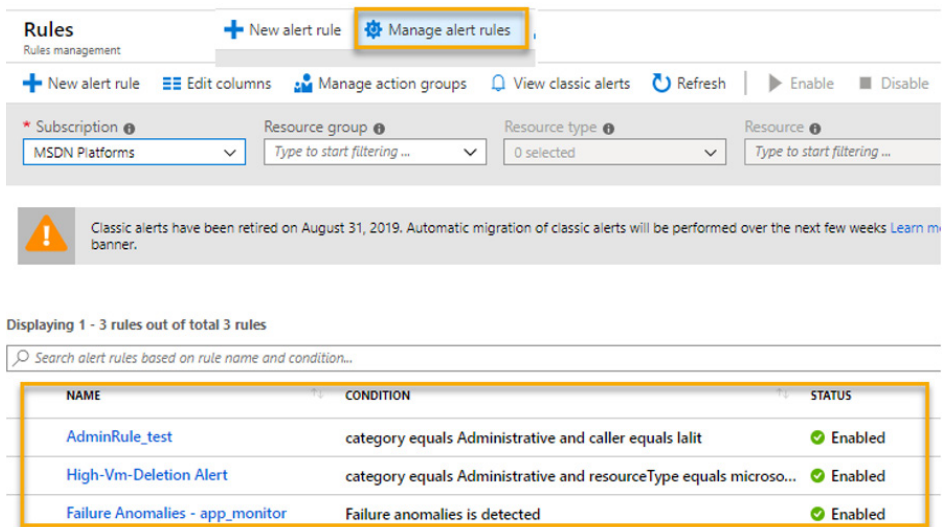
Enable rule upon creation  
☒ Yes ☐ No

*i* It can take up to 5 minutes for an Activity log alert rule to become active.

Create alert rule

*Figure 16.7: Alert details*

Once the alerts are created, you can view all the alerts in the **Manage alert rules** window. For more alert manager details, take a look at *Figure 16.8*:



**Rules** + New alert rule **Manage alert rules**

+ New alert rule Edit columns Manage action groups View classic alerts Refresh Enable Disable

\* Subscription ⓘ MSDN Platforms Resource group ⓘ Type to start filtering ... Resource type ⓘ 0 selected Resource ⓘ Type to start filtering ...

*!* Classic alerts have been retired on August 31, 2019. Automatic migration of classic alerts will be performed over the next few weeks. [Learn more](#)

Displaying 1 - 3 rules out of total 3 rules

Search alert rules based on rule name and condition...

| NAME                            | CONDITION                                                         | STATUS    |
|---------------------------------|-------------------------------------------------------------------|-----------|
| AdminRule_test                  | category equals Administrative and caller equals lalit            | ✓ Enabled |
| High-Vm-Deletion Alert          | category equals Administrative and resourceType equals microso... | ✓ Enabled |
| Failure Anomalies - app_monitor | Failure anomalies is detected                                     | ✓ Enabled |

*Figure 16.8: Manager of the alert rule*

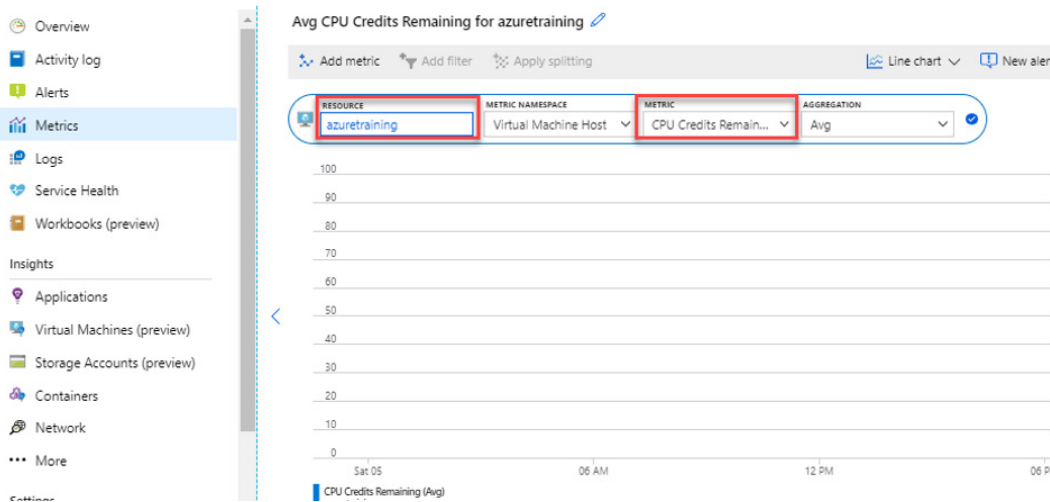
This is how you can create and manage the alerts. You can also modify the Azure resource alerts.



## Azure Metrics

Azure Metrics are numerical values of the resources utilization, which are collected in real-time. Based on the numerical values, it shows the metrics performance of the resources, as shown in *Figure 16.9*. Follow the given steps:

1. You can select the resources.
2. Click on **Metrics**, as shown in *Figure 16.9*:



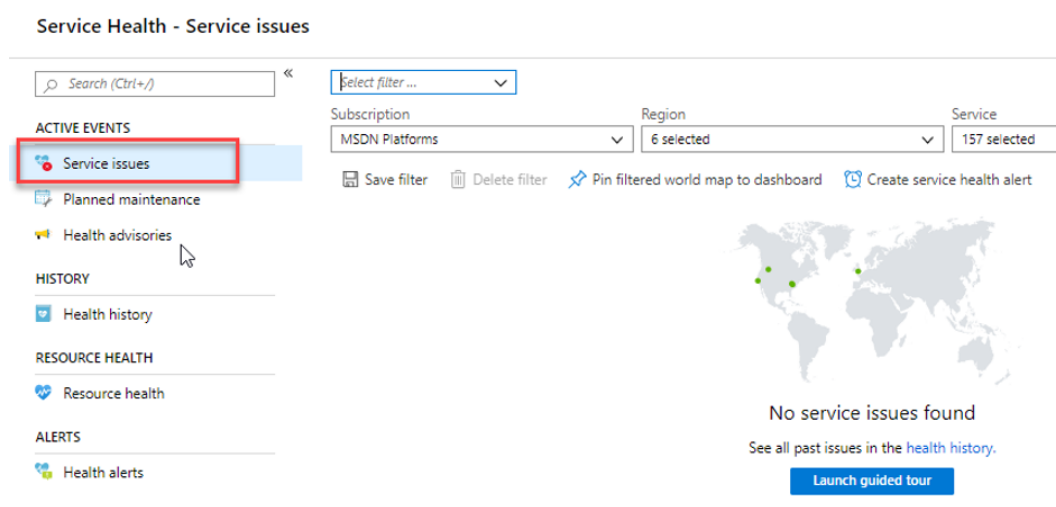
*Figure 16.9: Metrics*

## Azure Services Health

Azure Service Health will help you analyze the resources under the subscription and various region service availability options. Let us understand them:

- **Planned maintenance:** You can see the planned maintenance of the Azure datacenter if there is any global impact. In such a scenario, you can take the primitive action on that.
- **Resource health:** Resources health will help you understand the health of the resources.

- **Health alerts:** We can set up the resource health alerts as well, based on the customers' requirements. For more details, take a look at *Figure 16.10*:



*Figure 16.10: Azure Services Health*

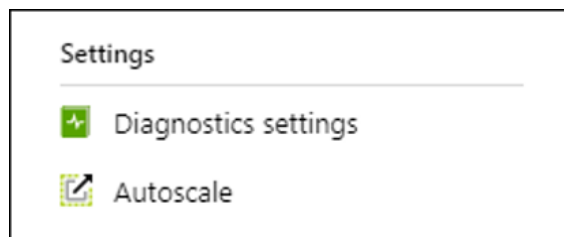
## Diagnostic Logs

Diagnostic Logs provides auditing and diagnostic information about the Azure resources. It also helps to collect the logs and sends the logs to log analytics for further analysis. It can be sent to the event hub to get the notification. It can also store the logs in storage accounts for any further update or archival.

## Enabling the diagnostic settings

To enable the diagnostic settings, perform the following steps:

1. Click on Azure Monitor.
2. Click on **Diagnostic settings** under **Settings** and click on the resource. Refer to *Figure 16.11*:



*Figure 16.11: Diagnostic settings*

3. Click on the resource menu on the Azure portal. Then, click on **Diagnostic settings** under **Monitoring**, as shown in Figure 16.12:

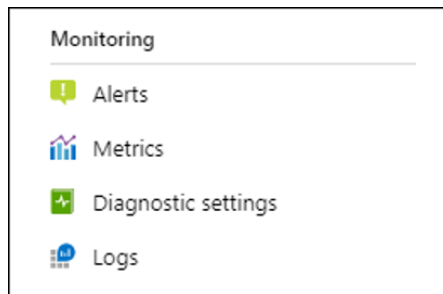


Figure 16.12: Diagnostic settings details

4. If there are no settings that exist on the resource, then click on **Diagnostic settings** and then on **+ Add diagnostic setting** to enable it, as shown in Figure 16.13:

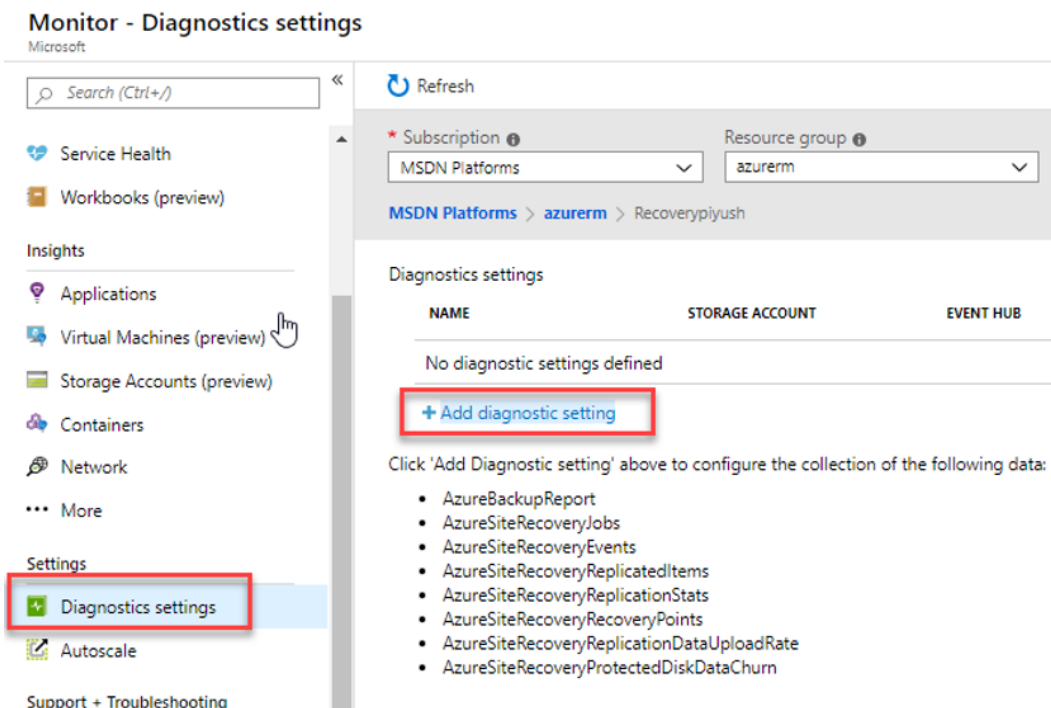


Figure 16.13: Monitor diagnostic settings

5. Once you click on **Diagnostic settings**, follow the given steps:
  - a. Provide the storage account details.

- b. Provide the solution of where to store the logs: **Send to Log Analytics** or **Stream to an event hub**.
- c. Select the storage account and retention period of the logs.
- d. Click on **OK** and save the settings, as shown in *Figure 16.14*:

#### Diagnostics settings

Save Discard Delete

\* Name  
Logs of RecoveryVault ✓

☒ Archive to a storage account

Storage account  
azurermddiag >

☐ Stream to an event hub

☐ Send to Log Analytics

| LOG                                                        |                    |
|------------------------------------------------------------|--------------------|
| <input type="checkbox"/> AzureBackupReport                 | Retention (days) 0 |
| <input type="checkbox"/> AzureSiteRecoveryJobs             | Retention (days) 0 |
| <input type="checkbox"/> AzureSiteRecoveryEvents           | Retention (days) 0 |
| <input type="checkbox"/> AzureSiteRecoveryReplicatedItems  | Retention (days) 0 |
| <input type="checkbox"/> AzureSiteRecoveryReplicationStats | Retention (days) 0 |

*Figure 16.14: Diagnostic settings configuration*

Now, your diagnostic settings have been enabled to recovery services, and it can be done with other services in your Azure subscription resources.

## Azure Log Analytics

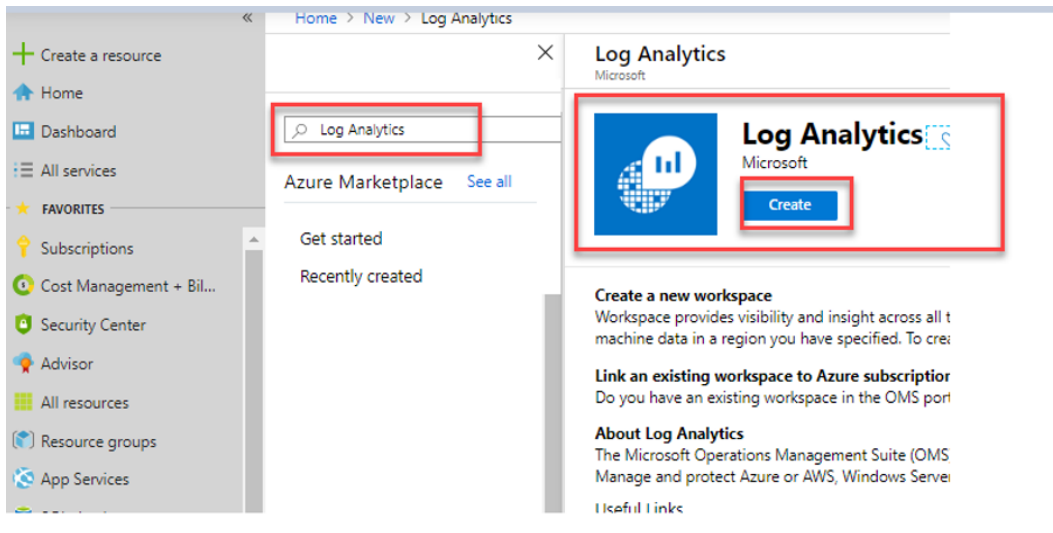
Azure Log Analytics is a service that collects the data from various Azure resources and on-premises devices, and sends it to your log analytics.

The collected data is stored in the log analytics workspace, which can be used for a query language, alerting, and so on. Log analytics analyses the metric data and provides the result based on that.

# Creating the Azure workspace

Follow the given steps to create the Azure workspace:

1. Click on **+ Create a resource**.
2. Search for **Log Analytics** and then click on **Log Analytics**.
3. Click on the **Create** button to create the log analytics workspace, as shown in *Figure 16.15*:



*Figure 16.15: Log analytics workspace*

4. Once the preceding steps are complete, perform the following steps:
  - a. Provide the log analytics name.
  - b. Provide the subscription name.
  - c. Provide the resource group name.
  - d. Provide the location based on your customer or project.
  - e. Provide the pricing tier.

5. Click on **Create**, as shown in Figure 16.16:

**Log Analytics workspace** □ ×  
Create new or link existing workspace

☒ Create New ☐ Link Existing

\* Log Analytics Workspace ⓘ  
azure4you ✓

\* Subscription  
MSDN Platforms ▼

\* Resource group  
azurem ▼  
[Create new](#)

\* Location  
East US ▼

\* Pricing tier  
Per GB (2018) >

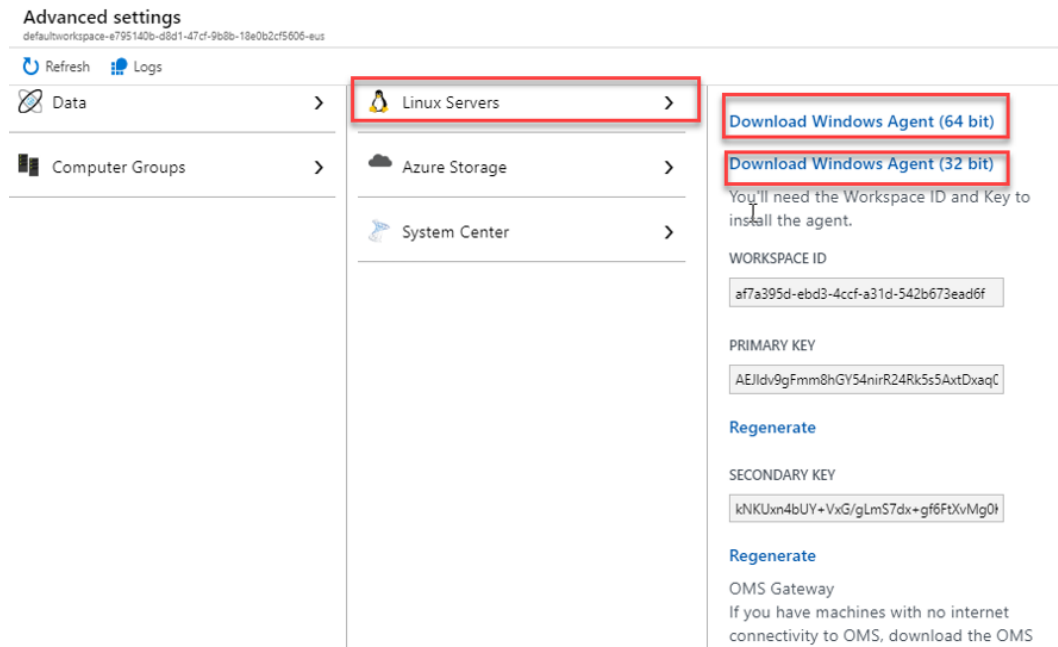
OK

*Figure 16.16: Log analytics details*

Now, your log analytics workspace has been created. You can start connecting your devices or using them.

If you would like to install or connect the VMs to the workspace manually, click on the **Advanced settings** option under Log Analytics and click on the Windows or Linux agent to download it.

Take a look at *Figure 16.17* for more details:



*Figure 16.17: Log analytics agent download*

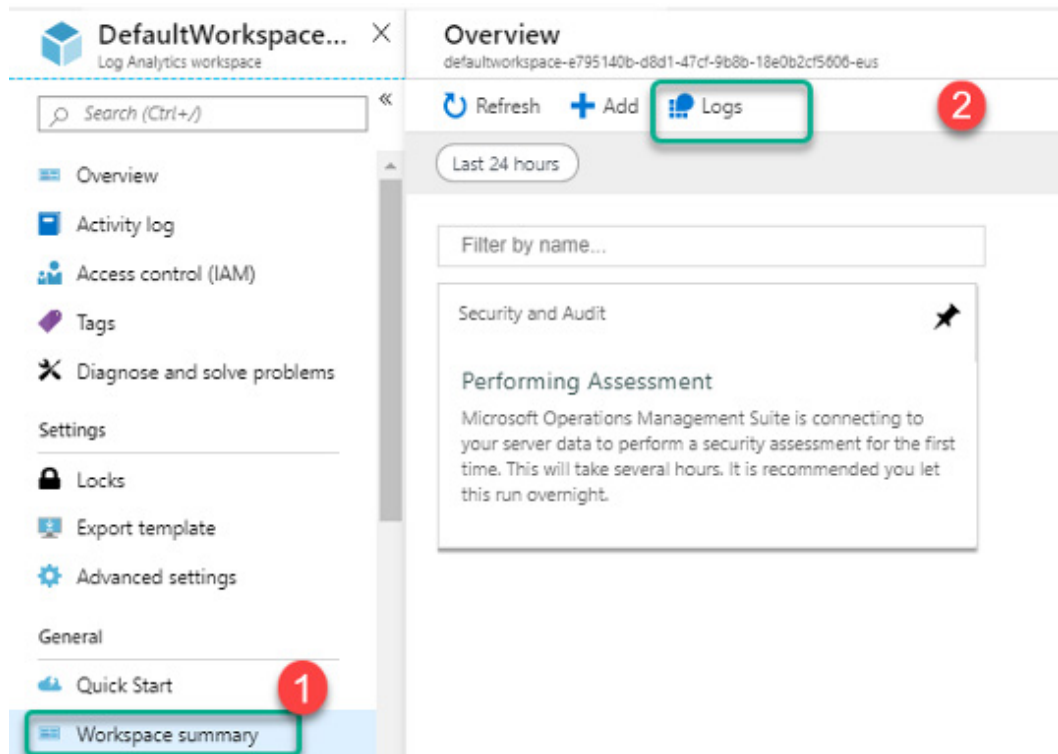
## Utilize Log Search Query Functions

The log query function will provide you with the values from the data collected from log analytics or Azure monitor. The query is a powerful language that allows you to combine the data from the multiple tables, aggregate the larger data, and provide a complex operation with minimal code.

You can query the data using the following steps:

1. Click on the log analytics which you have created.
2. Go to **Workspace summary**.
3. Click on **Logs**.

- Once you click on **Logs**, you will be able to see the dashboard of the log analytics. Take a look at *Figure 16.18*:



*Figure 16.18: Log analytics logs*

Here, you can run the query search for your port, dashboard or alert, and so on.

A query can be used to create the custom dashboard of Azure monitoring based on your customers' requirements. Follow the given steps to run a query:

- Click on **Sample queries**.
- Type the query.
- Click on **Run**.
- You will get a result.
- You can use the same query and create an alert as well, as shown in *Figure 16.19*:



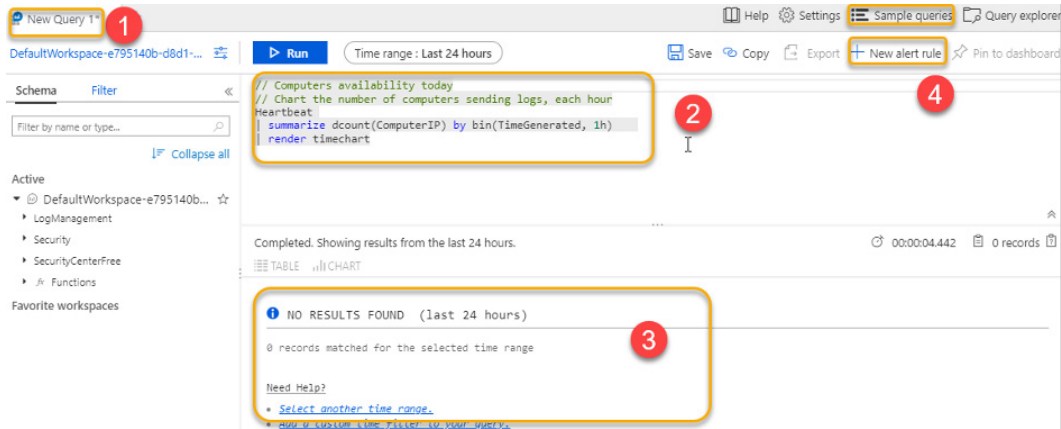


Figure 16.19: Log analytics search query

This is how we can use the query search to get the result of Azure resources and use it to monitor and query the result of the services. We can enable the alert based on the query.

## Conclusion

In this chapter, we covered analyzing the resources and explaining the Azure monitor. We discussed how to create the alerts and how to use those alerts. We covered how to create the Azure log analytics workspace and query search of Azure data based on the query. Using the query, we can then create the alerts.

We will discuss Azure backup and disaster recovery in the next chapter. We will also cover how to enable the backup of your Azure virtual machine and migrate the VM or set up disaster recovery in Azure.

## Points to remember

- Azure matrix collects numeric data from monitored resources into a time-series database.
- Azure Monitor metrics are lightweight and supports near-real-time scenarios.
- Diagnostic logs provides auditing and diagnostic information about the Azure resources. It also helps to collect the logs and sends the logs to log analytics for further analysis.

- Log analytics helps to edit and run log queries against data in the Azure Monitor Logs.
- Azure Service Health notifies you of Azure service incidents and planned maintenance, so that you can take action to mitigate downtime. We can also configure customizable alert.

## Multiple choice questions

1. **Which services help to run the query against the monitor logs?**
  - a. Azure monitor
  - b. Azure Metrics
  - c. Log analytics
2. **What are diagnostics logs?**
  - a. Provides Azure monitor data
  - b. Provides log analytics data
  - c. Provides auditing and diagnostic information

## Answers

1. c
2. c

# CHAPTER 17

# Implementation of Azure Backup and Disaster Recovery

## Introduction

In this chapter, we will discuss the Azure backup services, Azure backup recovery vault, and usage of the Azure backup policy. We will also discuss how to create the backup reports and see how the restoration process works in Azure. We will cover the various types of backup operations, and so on.

## Structure

The following topics will be covered in this chapter:

- Azure backup
- Azure backup vault creation
- Azure VM Backup Configuration
- Azure Backup Policy
- Azure Backup Report
- Azure Restoration of VMs
- Azure Backup Operation Details

- Using Soft Delete to Recover Azure VMs
- Site-to-Site Recovery Using Azure Site Recovery

## Objectives

In this chapter, you will learn about Azure backup and disaster recovery services. You will also learn how to configure the backup to protect the Virtual Machines (VMs) from accidental deletion and ensure faster restoration process in detail.

## Azure backup

Azure backup services come under the Azure site recovery vault. Azure backup services are used to take the backup of your virtual machines, Azure storage file share, as well as SQL servers, which are all hosted in Azure VMs. It provides the files and folder-level backup as well.

We can take the on-premise servers backup to Azure using Azure backup. The Azure backup vault supports Windows as well as Linux VMs to take the backup. It enhances the backup capability and provides a secure way to backup your infrastructure. It provides centralized monitoring and protects all the Azure VMs. We can control the access using the Role-Based Access Control (RBAC) roles to meet the compliance level.

## Azure backup vault creation

Let us see how to create the Azure backup vault and how to backup the services. Follow the given steps:

1. Log in to the portal.
2. Go to All services, or you can go to the marketplace and search for the **Backup and Site Recovery** service.
3. Click on the **Backup and Site Recovery** service. For more details, take a look at *Figure 17.1*:

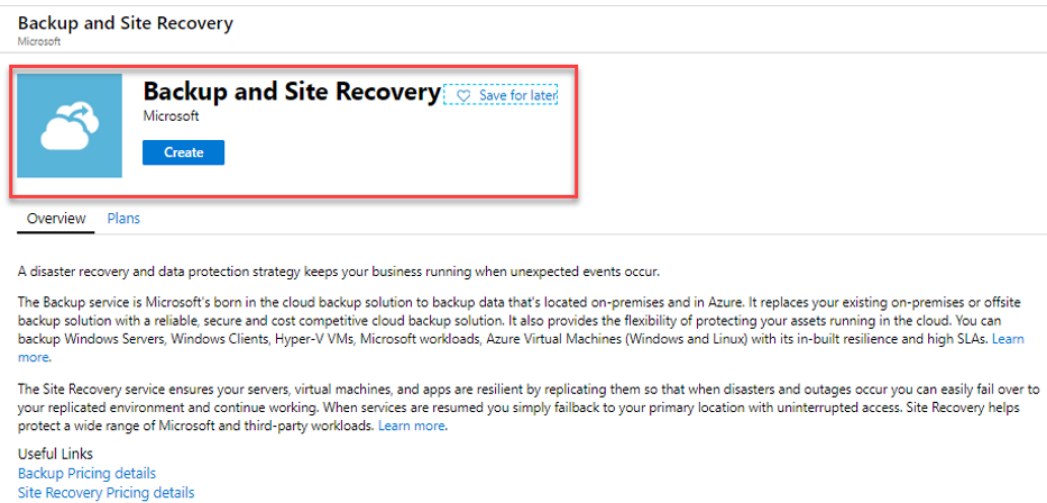


Figure 17.1: Azure backup vault marketplace

4. Provide the backup vault name.
5. Provide the **Resource group** name and other subscription details.
6. Click on **Review + create**. For more details, take a look at Figure 17.2:

[Basics \\*](#) [Tags](#) [Review + create](#)

**Project Details**

Select the subscription and the resource group in which you want to create the vault.

Subscription \* ⓘ

Resource group \* ⓘ  **1** [Create new](#)

**Instance Details**

Vault name \* ⓘ  **2** ✓

Region \* ⓘ  **3**

[Review + create](#) **4** [Next: Tags](#)

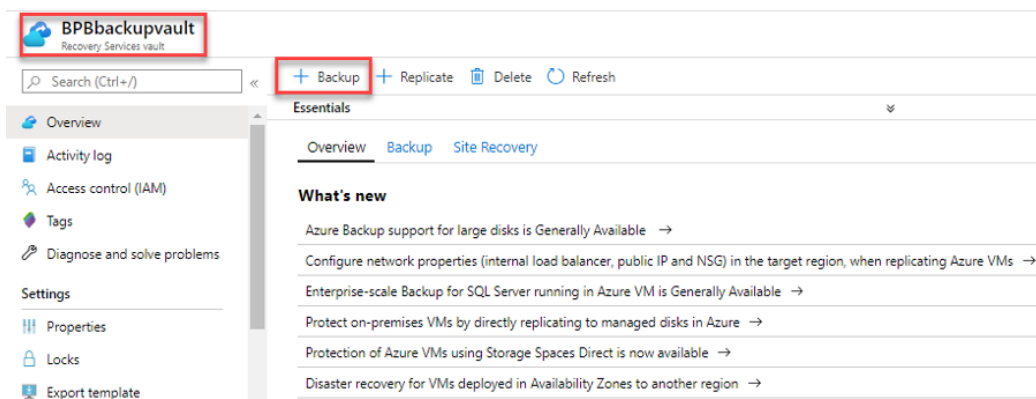
Figure 17.2: Azure backup creation

Now, you will be able to create the Azure backup vault. The backup vault has been created, and we will start the backup using the same recovery vault.

## Azure VMs backup configuration

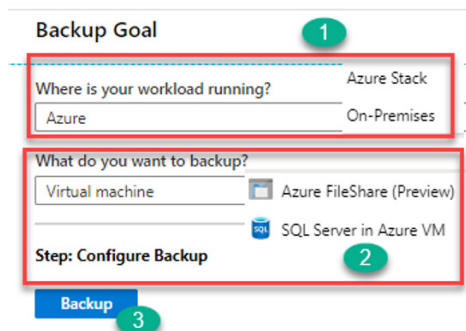
To configure the backup of your VMs, follow the given steps:

1. Click on **Recovery Services vault**.
2. Click on the **+ Backup** button.
3. Set up the quota limit as per customers' requirements.
4. Click on **Create**. Refer to *Figure 17.3*:



*Figure 17.3: Azure backup configuration*

5. You can select the Azure environment, and you can get two or more options to backup the Azure stack and on-premise servers.
6. Select **Azure** and the Azure VMs. However, you can also backup **Azure FileShare (Preview)** and **SQL Server in Azure VM**. Refer to *Figure 17.4*:



*Figure 17.4: Azure backup configuration setup*

7. Once you click on **Backup**, it will ask you for the Azure policy.

Let us now understand how the Azure backup policy will help schedule the backup for daily purpose.

## Azure backup policy

The Azure backup policy helps you set the rules for your backup infrastructure like VMs. You can have the retention policy, which will help you to retain the data in the Azure backup vault for up to 99 years. A retention policy can be set based on a daily, weekly, monthly, and yearly basis. Refer to *Figure 17.5*:

**Backup policy**

Choose backup policy

Create New

Policy name \*

BPBBBackuppolicy

Backup schedule

Frequency \* Time \* Timezone \*

Daily 6:00 AM (UTC) Coordinated Universal Time

Instant Restore

Retain instant recovery snapshot(s) for

2 Day(s)

Retention range

☒ Retention of daily backup point.

At For

6:00 AM 180 Day(s)

☒ Retention of weekly backup point.

On \* At For

Sunday 6:00 AM 12 Week(s)

☒ Retention of monthly backup point.

**Week Based** Day Based

On \* Day \* At For

First Sunday 6:00 AM 60 Month(s)

☒ Retention of yearly backup point.

**Week Based** Day Based

In \* On \* Day \* At For

January First Sunday 6:00 AM 10 Year(s)

Azure Backup service creates a separate resource group to store the instant recovery points of managed virtual machines. The default naming format of resource group created by Azure Backup service is AzureBackupRG\_{Geo}\_{n}. It is optional to custom the name as per your requirement. [Learn More](#)

Azure Backup Resource Group (Optional)

Enter the name Suffix (Optional)

*Figure 17.5: Azure backup policy*

Follow the given steps to create the backup policy:

1. Click on **OK** to create the backup policy. Once your backup policy is created, the backup vault will allow you to choose the VMs.
2. Click on **Items to backup** and select the virtual machine.
3. Click on **Enable backup**.
4. Once you click on **Enable backup**, it will trigger a job that installs the recovery agent. It will start taking the backup of your services. Refer to *Figure 17.6*:

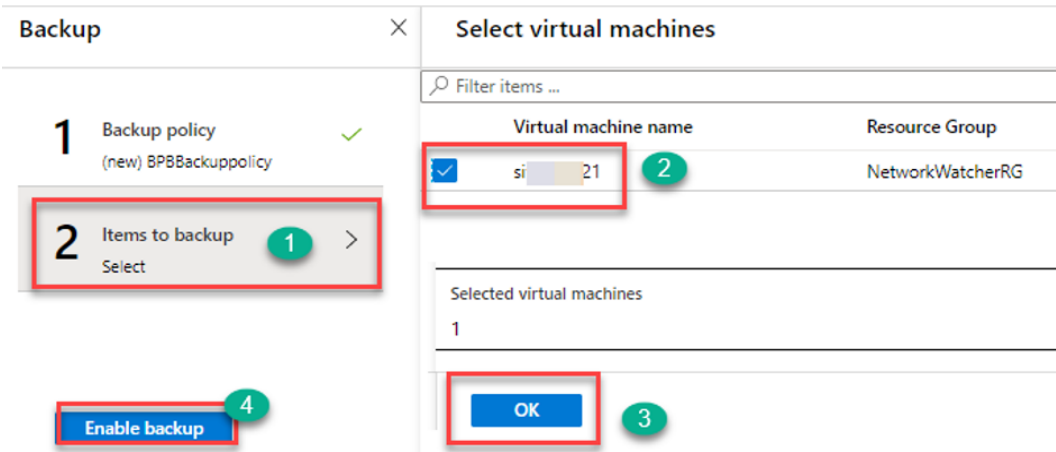


Figure 17.6: Azure backup enable

5. Once done, it will start the deployments. It will take some time to enable the backup, as shown in *Figure 17.7*:

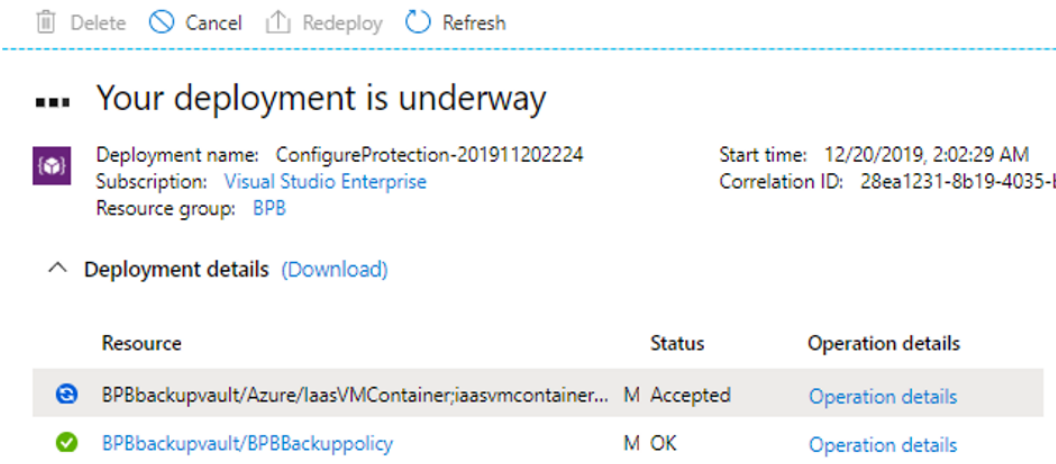


Figure 17.7: Azure backup deployment



- Once the backup is enabled, you can see that the VMs will be added to your backup services vault. You can see the numbers of the VMs in your VM backup vault, as shown in *Figure 17.8*:

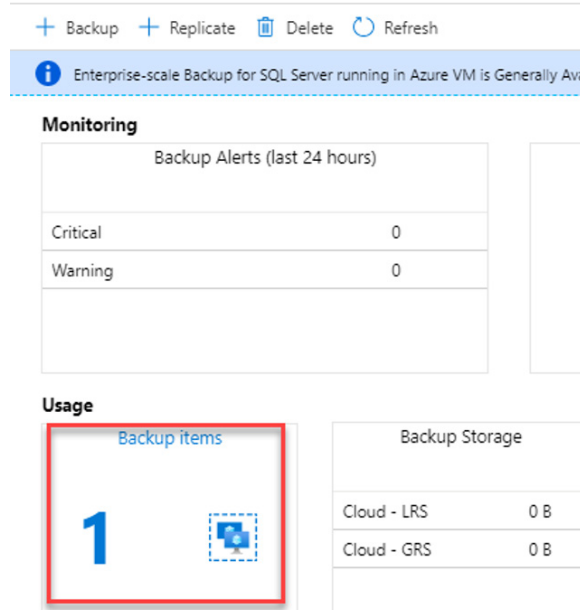


Figure 17.8: Azure backup verification

- Click on **Backup items** (as seen in *Figure 17.8*) and select the Azure VMs tab and then select the Azure VM.
- Click on the **Backup now** button to enable the backup.
- When you click on **Backup now**, the backup will get triggered, or it will start based on the Azure backup policy as per your schedule. Refer to *Figure 17.9*:

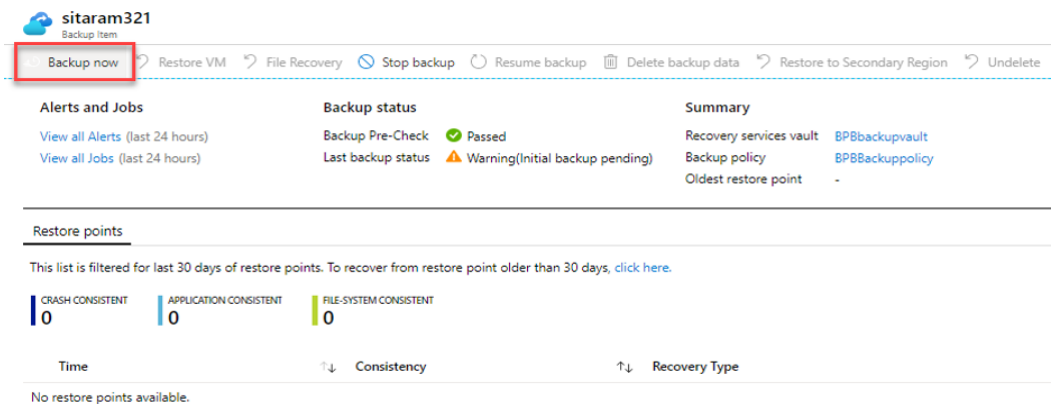


Figure 17.9: Enabling Azure backup for VM

## Azure backup report

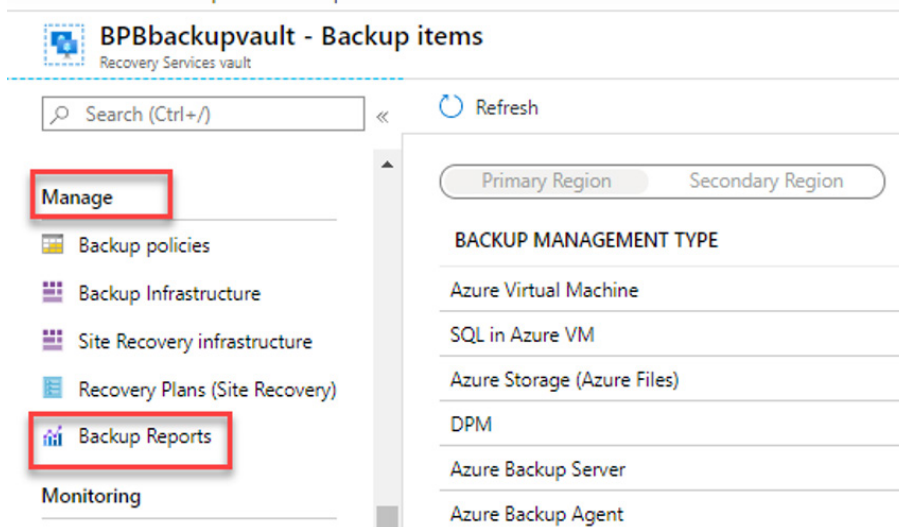
Azure backup reports will help you identify the backup of your VMs. Furthermore, its storage provides the transaction and backup failure. It also provides restoration and size of the backup size of your backup vault.

Before we create the backup report, we need the following:

- Azure storage account.
- Log restoration time 30 days to a maximum of 1 year.
- An important part is to have the Power BI licensed version, to configure the Azure backup report.

Let us see how to set up the Azure backup report from the Azure backup vault. Follow the given steps:

1. Go to the Azure backup vault for which you want to configure the backup report.
2. In that backup vault, go to **Manage** and select **Backup Reports**, as shown in *Figure 17.10*:



*Figure 17.10: Azure backup report*

Now, you need to follow the step-by-step instructions to enable the backup report, as shown in *Figure 17.11*:

**Backup Reports (Preview)**

You can use [Power BI](#) to view report dashboard, download reports and create custom reports 1

**Step 1. Add Diagnostics Setting**

Add Diagnostics Setting by going to Properties > Diagnostics Settings > Update and select storage account to get Azure Backup Reports

[Link to Diagnostics Settings](#) 2

 Backup Reports data will be fully available in the storage account after 24 hours from configuration. Wait until that time before connecting to the Azure Backup Content Pack.

**Step 2. Sign in to Power BI and connect to Azure Backup Template App**

Navigate to Apps > Get More Apps from Microsoft Appsource and install the 'Azure Backup' app

Use storage account details configured in Step 1 to connect to Template App

[Learn more](#) about how to connect to Content Pack 3

Figure 17.11: Backup report configuration

- When you click on the Azure backup diagnostic settings, it will ask you to store the log. You can select the Azure storage account, stream logs to an event hub, or send the logs to log analytics. In this case, we have selected the Azure storage to configure the backup report. Refer to Figure 17.12:

**Diagnostics settings**

Save Discard Delete

Name \* 1

☒ Archive to a storage account

Storage account 2  
Configure

☐ Stream to an event hub

☐ Send to Log Analytics

**log** 4

|                                                          |                                                        |
|----------------------------------------------------------|--------------------------------------------------------|
| <input checked="" type="checkbox"/> AzureBackupReport    | Retention (days) <span style="float: right;">30</span> |
| <input checked="" type="checkbox"/> CoreAzureBackup      | Retention (days) <span style="float: right;">30</span> |
| <input checked="" type="checkbox"/> AddonAzureBackupJobs | Retention (days) <span style="float: right;">30</span> |
| <input type="checkbox"/> AddonAzureBackupAlerts          | Retention (days) <span style="float: right;">30</span> |

 Showing all storage accounts including classic storage accounts

Location  
East US

Subscription 3

Storage account \*  
Select a storage account

OK

Figure 17.12: Backup report diagnostic configuration

4. Once this process is complete, please log in to the Power BI report tool and add backup apps from the storage, to configure the backup report. Refer to Figure 17.13:

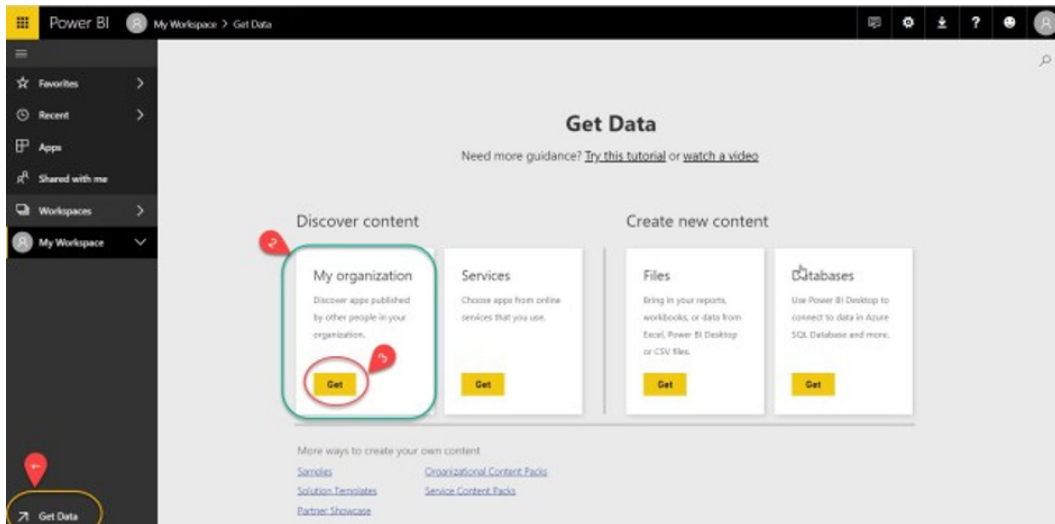


Figure 17.13: Backup report Power BI configuration

5. Now, you can create the Azure file sync. We will create the Azure file sync group, as shown in Figure 17.14:

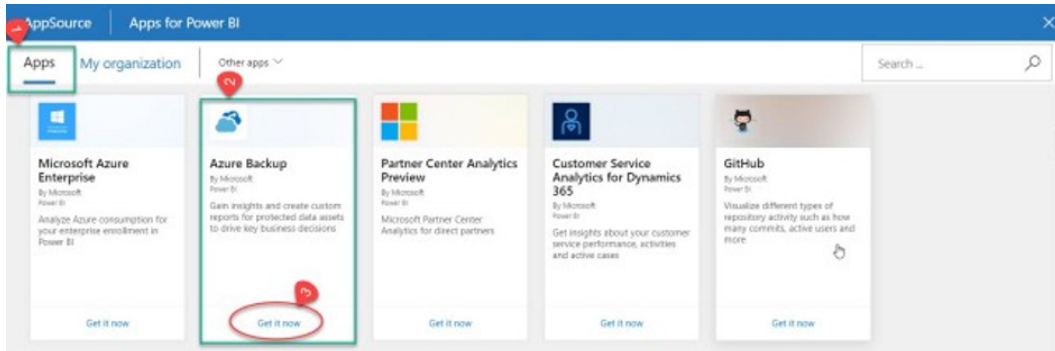
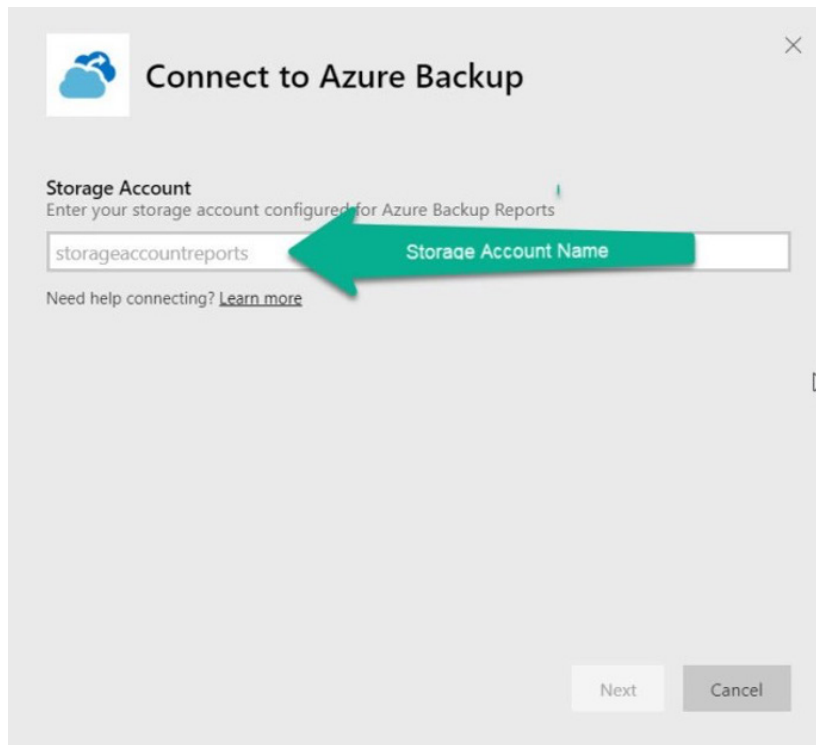


Figure 17.14: Azure backup from Power BI

6. Provide the storage account name to configure the diagnostic setting from the Azure backup vault.
7. Provide the Azure storage account and Azure storage account key.
8. Once you are done with the setup, it will take some time to add the report.
9. It might take 24 to 48 hours to store the logs and generate the reports.

10. Once the report is published, take a look at the Power BI backup report, as shown in *Figure 17.15*:



*Figure 17.15: Azure backup storage configuration Power BI*

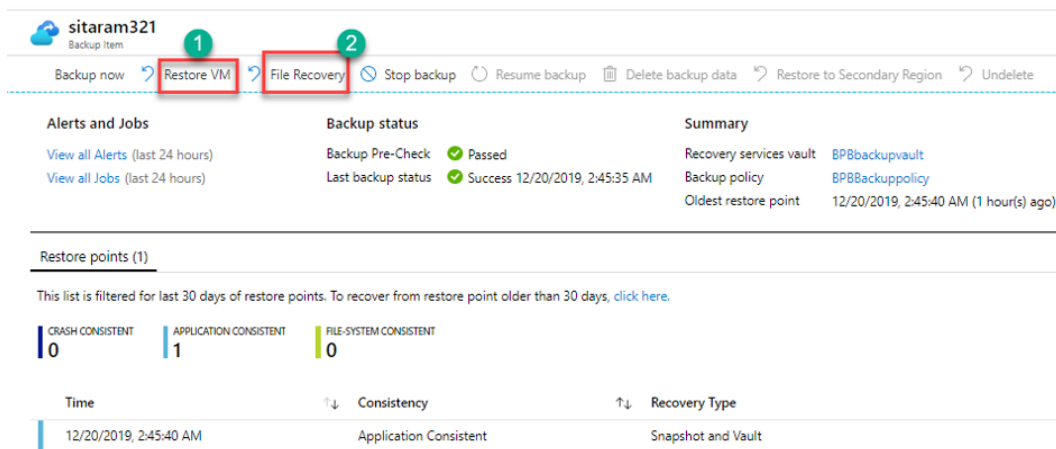
11. After the storage configuration backup report is published, you can customize the Azure backup dashboard.

## Azure restoration of VMs

The Azure backup restoration is processed to restore the VMs, files, and so on, in case of corruption of images, interruption to services, or for restoring to the previous version. To restore the VM using the recovery vault, follow these steps:

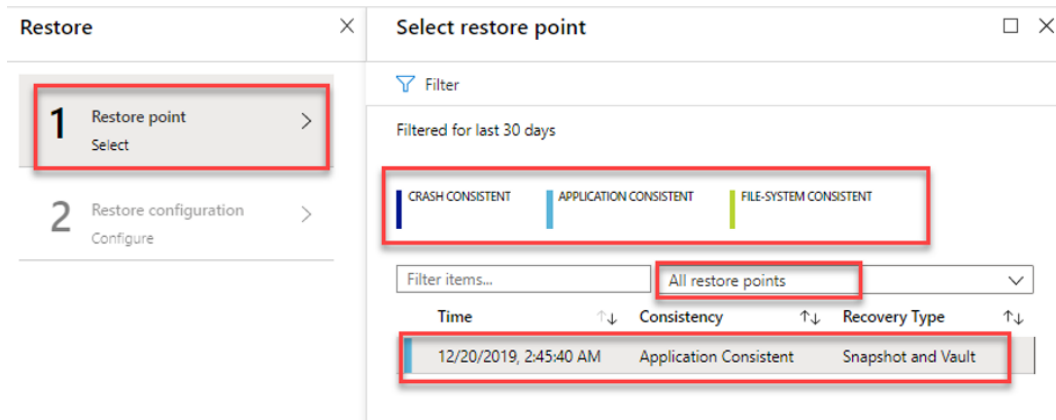
1. Select the recovery vault where you have taken the backup.
2. Then click on the **Backup** tab from **Protected** items.
3. Select the virtual machine for which you want to restore the VM.

- When you click on **Restore VM** or **File Recovery**, you will see the restore option. Take a look at *Figure 17.16*:



*Figure 17.16: VM backup restoration*

- Click on the **Restore point** option.
- When you click on it, it will show you the restoration time.
- You can restore the backup in terms of application, crash, and file consistency as well. Take a look at *Figure 17.17*:



*Figure 17.17: VM backup restoration point*

- Once you select the restore configuration, you can select whether you want to create a new VM or replace the existing setup which will replace the disk.
- Let us select the new VM creation.

10. Now, you need to provide the name of the VMs. VNet will select the default, or you can change it within the same region.
11. Please select the storage account and click on the **Restore** button.
12. After 10 to 15 minutes, your VM will be created. Based on the data, it might take a longer time. Take a look at *Figure 17.18*:

The image shows the Azure portal interface for restoring a virtual machine. It is divided into two main sections: 'Restore' and 'Restore configuration'.

**Restore Section:**

- 1** Restore point: 12/20/2019, 2:45:40 AM (marked with a green checkmark and callout 1).
- 2** Restore configuration: Configure (marked with callout 6).
- 7** Restore button (marked with callout 7).

**Restore configuration Section:**

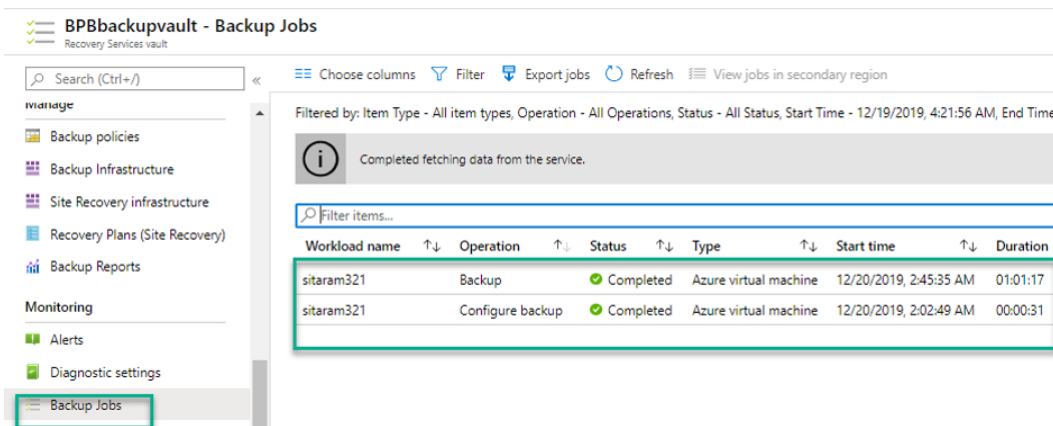
- 2** Create new button (marked with callout 2).
- 3** Replace existing button (marked with callout 3).
- Information box: To create an alternate configuration when restoring your VM (from the following menus), use PowerShell cmdlets.
- 4** Restore Type: Create virtual machine (marked with callout 4).
- Virtual machine name \* (marked with callout 5).
- Resource group \* (NetworkWatcherRG).
- Virtual network \* (NetworkWatcherRG-vnet (Networ...)).
- Subnet \* (default).
- 5** Staging Location \* (Select an option) (marked with callout 5).
- Link: [Can't find your storage account?](#)

*Figure 17.18: New VM creation using restoration*

## Azure backup operation details

Azure backup operations help you understand whether your backup job has been successful or unsuccessful. It provides the end-to-end Azure operation errors to

understand and troubleshoot the issue. Activity logs will also help in the Azure backup operation. Take a look at *Figure 17.19*:



The screenshot shows the 'BPBbackupvault - Backup Jobs' page in the Azure portal. The left sidebar contains navigation links for 'Backup policies', 'Backup Infrastructure', 'Site Recovery infrastructure', 'Recovery Plans (Site Recovery)', 'Backup Reports', 'Alerts', 'Diagnostic settings', and 'Backup Jobs' (which is highlighted). The main area displays a table of backup jobs. A message at the top states 'Completed fetching data from the service.' The table has columns for Workload name, Operation, Status, Type, Start time, and Duration. Two rows are visible, both for workload 'sitaram321'.

| Workload name | Operation        | Status    | Type                  | Start time             | Duration |
|---------------|------------------|-----------|-----------------------|------------------------|----------|
| sitaram321    | Backup           | Completed | Azure virtual machine | 12/20/2019, 2:45:35 AM | 01:01:17 |
| sitaram321    | Configure backup | Completed | Azure virtual machine | 12/20/2019, 2:02:49 AM | 00:00:31 |

*Figure 17.19: Azure backup operations*

## Using soft delete to recover Azure VMs

The Azure soft delete backup will help you recover the VM even after you delete it from the backup vault. You can recover the VM from the backup vault within 14 days only. This is helpful in case you might have deleted the file accidentally or if the file got deleted due to malicious activity. Whenever you create the backup vault, soft delete will be enabled by default.

Let us now see how we can enable or disable the soft delete Azure VM using the site recovery:

1. Select the Azure backup vault.
2. Go to **Properties**.
3. Select **Security Settings** and click on **Update**.
4. Enable Soft Delete.
5. Click on **Save** to enable it. Take a look at *Figure 17.20*:



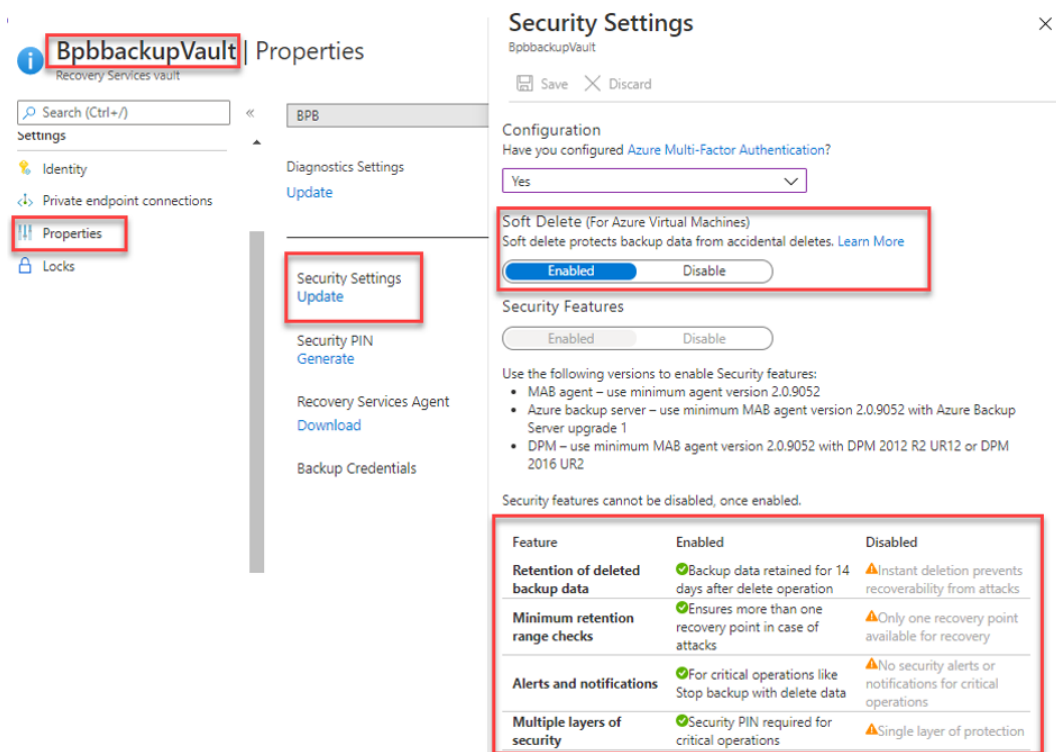


Figure 17.20: Azure backup soft delete

6. When you delete the backup, you will get the following message. It informs you that if you have enabled the soft backup to delete, then you will be able to recover the data within 14 days. Refer to Figure 17.21:

### A delete Backup data alert has been activated

You're receiving this email because a delete Backup data alert has been activated for BpbVM.

|                       |                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Severity              | Critical                                                                                                                                          |
| Alert                 | Delete Backup data                                                                                                                                |
| Backup item(s)        | BpbVM                                                                                                                                             |
| Description           | Your data for this Backup item has been deleted. This data will be temporarily available for 14 days, after which it will be permanently deleted. |
| Recommended action(s) | Undelete the Backup item within 14 days to recover your data.                                                                                     |
| Time                  | July 12, 2020 18:32 UTC                                                                                                                           |
| Vault                 | BpbbackupVault                                                                                                                                    |

Figure 17.21: Azure backup soft delete

- If you want to recover the data, then go the backup vault and select the deleted VMs backup and click on **Undelete**, as shown in Figure 17.22:

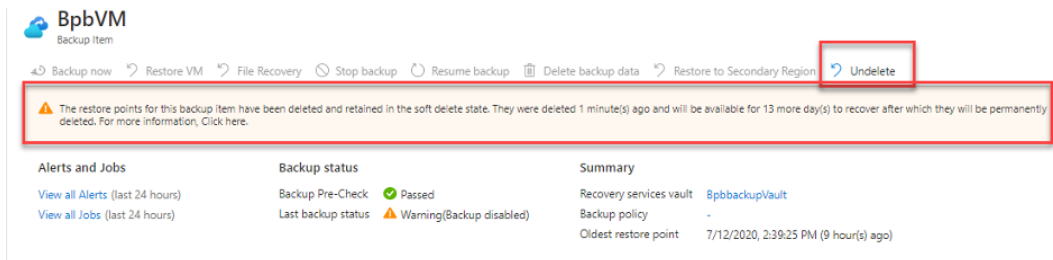


Figure 17.22: Azure backup soft undelete

## Site-to-site recovery using Azure Site Recovery

Azure site recovery helps you ensure your business continuity by running due to unplanned or planned outage. Azure site recovery services will help you to replicate the on-premise and Azure workload from the primary site to the secondary site, whenever there is an outage on primary sites. Once the primary sites are up and running, you can failback to primary sites.

The site recovery manages the following replications:

- Azure VMs can replicate between Azure regions.
- On-premises VMs, Azure stack VM, physical server, Hyper-V, and VMware servers.

Let us see how to enable the Azure site recovery:

- Go to site recovery and click on **+ Replicate**, as shown in Figure 17.23:

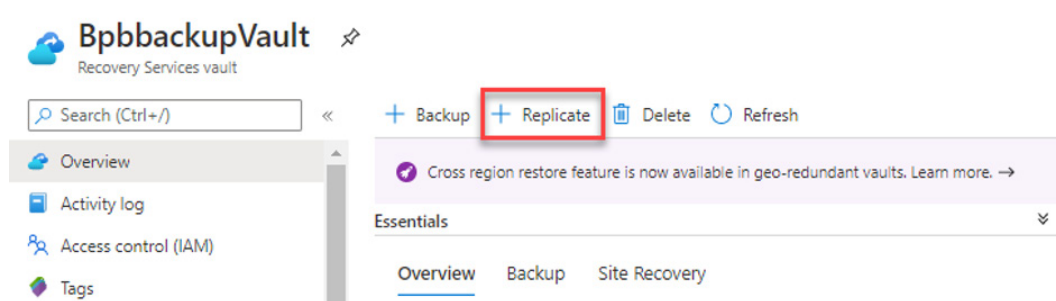


Figure 17.23: Azure site recovery replicate

2. Once you click on **+ Replicate**, select the source and provide the details as follows:
  - a. Provide **Source** as **Azure**.
  - b. **Source location** is your Azure VM location.
  - c. Provide the **Source resource group** and **Source subscription**.
  - d. Select the **Availability zones** and click on **OK**. Take a look at *Figure 17.24*:

**Enable replication**  
BpbbbackupVault

1 Source Configure

2 Virtual machines Select

3 Replication settings Configure replication settings

Enable replication

**Source**  
BpbbbackupVault

Select your source environment

Source  
Azure

Source location \* ⓘ  
East US

Azure virtual machine deployment model \* ⓘ  
Resource Manager

Source subscription \*  
[Redacted]

Source resource group \*  
BPPB

Disaster Recovery between Availability Zones? \* ⓘ  
Yes

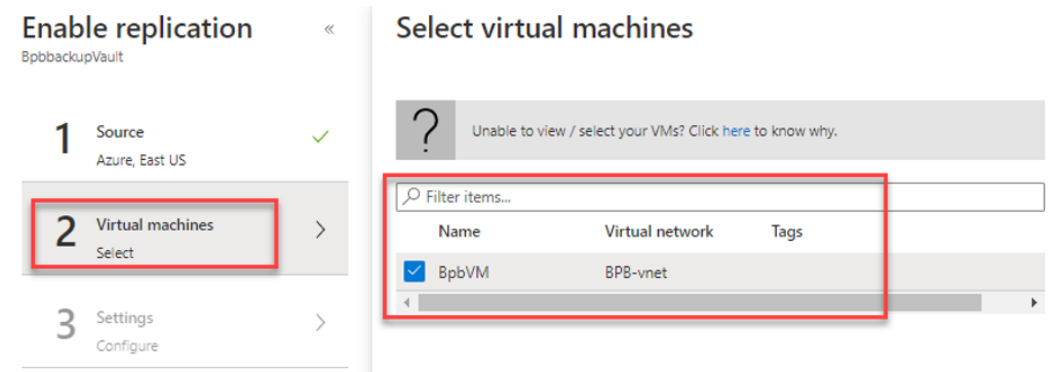
⚠ Disaster Recovery between Availability Zones is not supported in all regions. Please check the list of supported regions [here](#) before proceeding.

Availability Zones \* ⓘ  
1

OK

*Figure 17.24: Azure site recovery source*

3. Click on **OK** and select the Azure virtual machine, as shown in *Figure 17.25*:



*Figure 17.25: Azure site recovery virtual machine*

4. When you click **OK**, it will be directed to the **Settings** tab. Please define the settings as follows:
- Select the target location.
  - Select the **Disaster Recovery (DR)** subscription you want to configure in Azure.
  - Select the **Target resource group**, **Target virtual network**, **Cache storage accounts** and **Replica managed disks**.
  - Target the AV set if you want to configure.
  - Replication policy has the following settings under it:
    - 24-hour retention policy
    - Recovery point retention
    - Application consistent settings
    - Replication group
5. Click on **Create target resources**, as shown in *Figure 17.26*:

Enable replication

BpbbbackupVault

1 Source

Azure, East US

✓

2 Virtual machines

1 Selected

✓

3 Settings

Configure

>

Enable replication

Configure settings

Target location \*

West US

▼

Target subscription

Customize

Microsoft Azure for Labs

⚠

If you are choosing General Purpose v2 storage accounts, ensure that operations and data transfer prices are understood clearly before you proceed. [Learn more](#)

Resource group, Network, Storage and Availability

Customize

By default Site Recovery will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network and availability sets as below. Click 'Customize' above to change the configuration. The resources created are appended with 'asr' suffix.

Target resource group

(new) BPB-asr

Target virtual network

(new) BPB-vnet-asr

Cache storage accounts

(new) rp2vpwbpbbbackupvrasr-cache

Replica managed disks

(new) 1 premium disks(s), 0 standard disk(s)

Target availability sets

Not Applicable

Replication Policy

Customize

Name: 24-hour-retention-policy

Recovery point retention: 24 hour(s)

App consistent snapshot frequency: 4 hour(s)

Replication group: None

Extension settings

[+] Show details

Site Recovery manages site recovery extension updates for all your replicated items. 1 new automation account will be created.

Create target resources

Figure 17.26: Azure site recovery target resource

6. Once the target resource is created, click on **Enable replication**, as shown in Figure 17.27:

Enable replication

BpbbbackupVault

1 Source

Azure, East US

✓

2 Virtual machines

1 Selected

✓

3 Settings

Configured

✓

Enable replication

Figure 17.27: Azure site recovery replication enables

7. Once the replication is enabled, you will be able to successfully set up the DR using the site recovery. It will start the replication, and once the replication is complete, you can do the failover.

Now, we can successfully create the DR site.

## Conclusion

In this chapter, we discussed the Azure backup and its usage. We learned how to create a backup report and its usage, discussed how to set up the Azure site recovery for Azure VMs and explained the Azure backup reports.

In the next chapter, we will discuss the exam guidelines and assessments. We will provide the details on how to register for the exam and provide 75 questions to prepare for the exam.

## Points to remember

- Azure backup services are used to take the backup of your virtual machines, Azure storage file share, as well as SQL servers, which are hosted in Azure VMs.
- Azure backup policy helps you set the rules for your backup infrastructure.
- Azure soft delete backup will help you recover the VM even after you delete it from the backup vault. You can recover the VM from the backup vault within 14 days only.
- Azure backup restoration is processed to restore the VMs, files, and so on, in case of corruption of images, interruption to services.
- Azure site recovery helps you to ensure your business continuity by running due to unplanned or planned outage.

## Multiple choice questions

1. **How many day's backup retention period can be configure for azure backup ?**
  - a. 99 years
  - b. 999 Years
  - c. 100 years

2. **By mistake you have deleted the backup from backup vault, and the customer wants to recover the data. Which option you will select?**
  - a. Azure VM restore
  - b. Data disk restore
  - c. Soft delete

## **Answers**

1. a
2. c





# CHAPTER 18

# Exam Preparation Guidelines and Assessment Based on Live Questions

## Introduction

In this chapter, we will discuss the AZ-104 live scenario-based questions and answers, which will help you understand the exam pattern. These are dummy questions which have been created by the author and will help you in your exam practice. It is not related to your exam, but will nonetheless help you to understand the topics. It will give clarity on what types of questions will be asked in the exam so that you can prepare well for your exam. We will try to cover all the topic questions which have been written in this book and also try to cover the questions as much as we can.

**Note: Certified authors will create all the questions but if there is any match to your exam question, then it is just a coincidence and neither the author or publisher will be responsible for those questions.**

The following topics will be covered in your exam as per the Microsoft exam center official site <https://docs.microsoft.com/en-us/learn/certifications/azure-administrator>.

Please follow the given topics to start preparing for the exam:

- Manage Azure identities and governance (15-20%)
- Implement and manage storage (15-20%)

- Deploy and manage Azure compute resources ) (20-25%)
- Configure and manage virtual networks (20-25%)
- Monitor and Maintain Azure Resources (10-25%)

# Exam preparation guidelines

*AZ-104 Microsoft Azure administrator certification* validates your expertise in the Azure administrator role. In this exam, your administrator skills and knowledge will be tested.

If you want to be certified on the AZ-104 exam, you should be aware of the Azure compute, storage, networking, Azure AD, monitoring, subscription management, and so on, which we have covered in this course. In this exam, you will have to perform the labs as well. Hence, you will have hands-on practice. You can create the free subscription (<https://azure.microsoft.com/en-in/free/>), which will provide the 12K credit for 1 month and 25 most used applications which you can use for 12 months. *Table 18.1* provides some basic subscription for AZ-104:

| Exam AZ-104 Basic Information |                                                                        |
|-------------------------------|------------------------------------------------------------------------|
| Name of the exam              | Exam AZ-104: Microsoft Azure Administrator                             |
| Technology                    | Microsoft Azure                                                        |
| Prerequisites                 | Hands-on practice for Azure Admin labs and Azure concept understanding |
| Number of questions           | 40-60                                                                  |
| Exam fee                      | USD 165 and INR 4800                                                   |
| Exam language                 | English                                                                |

*Table 18.1: Basic information for AZ-104*

# AZ-104 Exam tips

Here are a few AZ-104 Exam tips:

- The Azure exam duration will be of 180 minutes, and in those 180 minutes, 30 minutes will be given for instructions, comments, score reporting, and others. In the remaining 150 minutes, you must answer all the questions and complete the labs.
- You will get two labs, which have 14 tasks to be completed and there will 3-5 case study-based questions.
- In the case study-based questions, you need to read and understand the questions very carefully to provide the correct answers. It is a time consuming

section because in these study cases, you might have to answer about 10 to 15 questions. In each case study, there will be approximate 2 to 5 questions which you need to answer.

- You will get multiple-choice questions as well, in the following format:
  - **Single-correct answer:** You have to say Yes/No.
  - **Fill in the blanks:** You have understood the scenarios and you need to choose the right answer and do the drag and drop job.
  - **Order statements:** In the exam, you need to create a site-to-site VPN by putting the preceding steps in order. Hence, you should be aware of the correct order and able to perform the steps.
- Exams will be divided into sections, and you can go back and correct the answers within the section. However, once you have moved on to the next section, you will not be able to change the section. Please make sure you will be able to verify or review the question before going to the next section.
- Please read the question properly and understand the format of the question. It can be a scenario-based question. If it is a scenario-based question, understand the question that is being asked, and fill in the requirements to give the correct answer. Once you do this, it will take a few minutes to provide the correct answer.
- Try to complete single answer questions as early as you can, so that you can save some time for scenarios-based questions and labs.
- Try to attempt and answer all questions which come in the exam because there is no harm in guessing the answers.
- A few of the questions will be from PowerShell and ARM. To answer with the given PowerShell command, let us prepare the new module AZ PowerShell which will help.
- A few of the questions will come from cost management. Please prepare the topics and answer them.
- Practice the labs, as there will be around 14 tasks. You can get the free subscription and prepare well, which will help you clear the exam.
- Azure exam labs will be slow and you may face some issues. If you are running out of time and stuck in labs or any other technical issues arises during the exam, you can talk to the center person to reschedule the exam or the concerned person will help you. Pearson VUE supports emails to reschedule your exam.

- You will not be allowed to go out during the exam time, so please make sure to finish other activities before sitting for the exam.
- You will not be allowed to take any of your other stuff into the exam hall. The exam center requires two ID proofs to let you sit for the exam and the exam center team will help you with that.
- You can mark questions to be reviewed during the exam if you are not sure about the answers. Once you are done with the section, review the answer and proceed further.
- You might get the performance-based question about the Azure services, and you have to answer that as well.
- In the case study question, you will need to give the business requirements and technical requirements of the existing environments and other information, to answer the question.
- Case study questions might require you to look at your question back and forth, which might require information to be integrated with multiple sources in the question. Please make sure to read the case study properly, understand the requirements, and then answer the question.

## Exam registration

If you are planning to register for the exam, and if you are a first time user, please make sure you have a valid email ID like Outlook, Hotmail, and so on. Once you are ready with your email ID, follow the given steps to register for the exam:

1. Click on the link-AZ-104 exam registration link to register for the exam.
2. Provide your name, job title, and address, as shown in *Figure 18.1*:

**Microsoft Certification Profile**

Exam AZ-103 | Exam AZ-103: Microsoft Azure Administrator [Change](#)

\*Required fields

Legal name

**Important:** Please enter your name as it appears on the acceptable legal identification you will present at the testing center

Title  
Mr ▼

First Name \*  
Lalit

Middle Initial

Last Name \*  
Rawat

Job Title \*  
▼

Address 1 \*

Figure 18.1: Exam schedule-1

3. Select the city and country for which you want to register for the exam.
4. Provide the state postal code.
5. Provide the country code and phone number.
6. Provide the preferred email ID and language, as shown in Figure 18.2:

City \*  
▼

Country \*  
▼

State \*  
▼

Postal code

Country code \*  
▼

Area code \*

Phone number \*

Ext

Email \*  
lalit01.rawat@outlook.com

Preferred language \*  
English ▼

☒ I would like to hear from the Microsoft about products, services, and events, including the latest solutions, tips, and exclusive offers.

☒ I would like to hear from the Microsoft Partners, or Microsoft on their behalf, about their products, services, and events. Share or use my details with Microsoft partners.

☒ I have read and agree to the [Terms of Use](#) and [Privacy & Cookies](#) statement. \*

Figure 18.2: Exam schedule-2

7. Click on **Save & continue**.
8. Once you click on **Save & continue**, it will ask you to go the Pearson VUE site to register for the exam.
9. Select the local center, home address, and the other options. Select the center option and click on the **Next** button.
10. Select the language.
11. Click on **Schedule the Exam**.
12. Select the exam center or search for the center name.
13. Select the date and time.
14. Proceed to check out and proceed for payment.
15. Once you click on checkout, your exam will be scheduled. You will get an email from Pearson VUE.

## Dummy objective exam questions

1. What kind of users can be invited using the guest user invite?
  - 1) B2C
  - 2) B2B
  - 3) Both

**Ans: 3) Both**

2. How can we create multiple users in Azure AD?
  - 1) Using bulk user creation
  - 2) Guest user invitation
  - 3) Group management

**Ans: 1) Using bulk user creation**

3. Which types of groups can we create in Azure AD?
  - 1) Security group
  - 2) O365 group
  - 3) Both

**Ans: 3) Both**

**4. What is the use of Azure AD connect?**

- 1) Hybrid connectivity
- 2) On-premises AD connect to Azure AD integration
- 3) MFA

**Ans: 2) On-premises AD connect to Azure AD integration**

**5. What is the permission requested to install the Azure AD Connect?**

- 1) Enterprise admin
- 2) Global administrator
- 3) Both

**Ans: 3) Both**

**6. What is the use of password writeback?**

- 1) It is used to sync the users.
- 2) On-premises sync services
- 3) To sync the password if it is changed through the Azure portal

**Ans: 3) To sync the password if it is changed through the Azure portal**

**7. Which is the PowerShell command to get the role definition?**

- 1) Get-azRoledefinition "Contributor"
- 2) Get-azRoledefinition "Contributor" | convertto-json | out-file D:\ABPGroup
- 3) Connect-azsubscription

**Ans: 1) Get-azRoledefinition "Contributor"**

**8. How many types of role back Access are available in Azure?**

- 1) Read and write
- 2) Viewer and editor
- 3) Owner, contributor, and reader

**Ans: 3) Owner, contributor, and reader**

**9. How many custom roles can be created in one tenant?**

- 1) 1000
- 2) 2000
- 3) 5000

**Ans: 3) 5000**

**10. If your company wants to buy a subscription directly from MS, which subscription would you chose?**

- 1) Free subscription
- 2) Enterprise subscription
- 3) CSP subscription

**Ans: 2) Enterprise subscription**

**11. What is a subscription in Microsoft Azure?**

- 1) It is a billing container which contains the Azure services
- 2) It just a container
- 3) It is Azure cloud services provider

**Ans: 1) It is a billing container which contains the Azure services**

**12. A customer asks you to provide the IT admin access role, that can manage the subscription and provide access. Which RBAC role access would you provide to the user?**

- 1) Owner
- 2) Contributor
- 3) Reader

**Ans: 1) Owner**

**13. What is the use of the Azure policy?**

- 1) To meet the compliance
- 2) To meet the cloud security
- 3) To restrict the access

**Ans: 1) To meet the compliance**

**14. A customer wants to allow only a few locations, based on his presence in the Azure subscription. How would you do that?**

- 1) Using the Azure policy
- 2) Using the Resources group
- 3) Using the RBAC access

**Ans: 1) Using the Azure policy**



**15. Which types of storage accounts does Azure have?**

- 1) Blob storage account
- 2) GPv1
- 3) GPv2
- 4) All of the above

**Ans: 4) All of the above**

**16. What is storage account replication recommended by MS Azure?**

- 1) RA-GRS
- 2) GRS
- 3) ZRS
- 4) LRS

**Ans: 1) RA-GRS**

**17. How many IOPS are provided by 1 TB premium storage account?**

- 1) 1000
- 2) 2000
- 3) 5000
- 4) 7500

**Ans: 4) 7500 IOPS**

**18. How to connect the Azure storage explorer? Please select two methods.**

- 1) SAS key
- 2) Storage account key
- 3) Through Azure portal

**Ans: 1) SAS key, and 2) Storage account key**

**19. What is the storage account contributor role?**

- 1) Provide access to read/write/delete access
- 2) Provide read access
- 3) Provide write access

**Ans: 1) Provide access to read/write/delete access**

**20. Why do we use the Azure import and export utility?**

- 1) To migrate the petabytes of data
- 2) To migrate 1 TB data
- 3) To migrate 50 GB data

**Ans: 1) To migrate the petabytes of data**

**21. Which OSes are supported by Azure fileshare?**

- 1) Windows and Linux
- 2) MAC
- 3) Linux

**Ans: 1) Windows and Linux, and 2) MAC**

**22. What is the limit of Azure fileshare?**

- 1) 2 TB
- 2) 5 TB
- 3) 4 GB

**Ans: 2) 5 TB**

**23. What is the use of Azure file sync?**

- 1) Centralized management for your files and folders
- 2) Used to sync docs Azure to Azure
- 3) Used for file sharing, which is in cloud

**Ans: 1) Centralized management for your files and folders**

**24. What is Azure VMs size?**

- 1) Configuration of Azure VMs instance
- 2) VM image
- 3) None

**Ans: 1) Configuration of Azure VMs instance**

**25. Can we set the auto-scaling while creating the scale set?**

- 1) Yes
- 2) No
- 3) None of the above

**Ans: 1) Yes**

**26. Azure VMs size support GUP and SAP sizes as well?**

- 1) Yes
- 2) No
- 3) None

**Ans: 1) Yes**

**27. In which format does the ARM template save the documents?**

- 1) JSON
- 2) PowerShell
- 3) CLI

**Ans: 1) JSON**

**28. What are ways to deploy the ARM template?**

- 1) PowerShell
- 2) CLI
- 3) All of the above

**Ans: 3) All of the above**

**29. How to deploy the ARM template from the portal?**

- 1) Using a custom template
- 2) PowerShell
- 3) None

**Ans: 1) Using a custom template**

**30. What is the way to connect to the on-premises network?**

- 1) A site-to-site connection
- 2) Express route
- 3) Vnet-to-VNet connection
- 4) Options 1 and 2

**Ans: 4) Options 1 and 2**

**31. How do you configure the Vnet-to-VNet connectivity?**

- 1) VNet peering
- 2) Site-to-site connection
- 3) ExpressRoute configuration

**Ans: 1) VNet peering**

**32. What is the use of a local area network?**

- 1) It has on-premises VPN device configuration
- 2) ExpressRoute configuration
- 3) None

**Ans: 1) It has on-premises VPN device configuration**

**33. Which are the types of Azure DNS zones?**

- 1) Private zone
- 2) Public zone
- 3) Both

**Ans: 3) Both**

**34. What are the different types of the Azure load balancer?**

- 1) Internal
- 2) External
- 3) All of the above

**Ans: 3) All of the above**

**35. Which are the types of rules available in Azure NSG?**

- 1) Inbound
- 2) Outbound
- 3) Both

**Ans: 3) Both**

**36. What is the use of a route table?**

- 1) Route the traffic to the firewall
- 2) Route the traffic within Azure
- 3) All of the above

**Ans: 3) All of the above**

**37. Can we apply the NSG in web apps?**

- 1) Yes
- 2) No

**Ans: 2) No**

**38. What is the use of the Azure resource's health monitoring?**

- 1) Azure Resources Health Check
- 2) Subscription monitoring
- 3) PaaS service monitoring
- 4) None

**Ans: 1) Azure Resource Health Check**

**39. What is the use of log analytics?**

- 1) Resource monitoring
- 2) Analyzing the metrics and alerting
- 3) Data collection
- 4) All the above

**Ans: 4) All of the above**

**40. How to query the monitoring data?**

- 1) Using the log search query
- 2) Azure monitor
- 3) Log analytics
- 4) None

**Ans: 1) Using the log search query**

**41. What is use of the action group in an alert?**

- 1) Used to send the notification to tools/email ID
- 2) Used to configure the Azure monitor
- 3) Used to connect to log analytics
- 4) None of the above

**Ans: 1) Used to send the notification to tools/email ID**

**42. What is the use of activity logs?**

- 1) It tracks all the operation activities within the subscription
- 2) It collects the data from the Azure monitor
- 3) It is used to connect to log analytics and analyze the logs

**Ans:** 1) It tracks all the operation activities within the subscription

## Dummy Scenario-Based Exam Questions

1. A BPB customer has more than 150 VMs, and now the customer wants to delete few of the VMs from his subscription. The customer wants to find out the unused disk which has been created during the VMs creation and deletion process. How can you identify the unused disk?

1. You can use the Azure portal.
2. You can use Azure storage explorer.
3. You can use the cost management report.
4. You can use the Cloudyn optimization report.

**Ans:** 4: You can use the Cloudyn optimization report which will provide the report of an unused disk.

2. A BPB customer asked to create 10 Azure virtual machines with Linux OS that was required for the production workload. The customer needs to monitor the metrics. What are the options the customer can use to monitor the Linux metrics from the portal?

1. Log analytics
2. Application insight
3. Azure performance diagnostic extension
4. Azure monitor

**Ans:** 3. Azure performance diagnostic extension will help the customer to collect the additional metric data and monitor the Linux metrics.

3. A BPB customer has two different subscriptions: call subscriptions BPBDev and BPBProd and both the subscriptions need to communicate with each other. We have already configured the VNetDev for the subscriptions BPBDev and VNetProd with the BPBProd subscription. Now, you want to set up a communication between both the subscriptions. How can you configure it?

1. We will move the VNetDev to the BPBProd subscription.

2. Configure the VNet peering.
3. Configure Vnet-to-VNet connection between both the subscriptions.
4. Site-to-site connectivity between the subscriptions.

**Ans: 3. Configure Vnet-to-VNet connection between both the subscriptions.** Creating the vent-to-vent connectivity is a more time-consuming process than site-to-site VP connectivity, and moreover, the required local area connection needs to be created.

4. Your customer wants to create an Azure storage account called bpbstorage, and under that, he wants to create an Azure fileshare. Once you create the Azure fileshare, you need to map it to an Azure fileshare supported port. Which port number will you choose to configure the Azure fileshare?
  1. Port-443
  2. Port-445
  3. Port-80
  4. Port-8080

**Ans: 2. Port-445, because port 445 supports Azure fileshare.** If the port 445 is blocked by your organization, then you will not be able to connect to fileshare.

5. You are the administrator of your subscription which contains 30 virtual machines, and in your team, members want to create a couple more VMs with the NSG group. Now, your manager wants to block port 80 whenever any new NSG is created. What is your approach on this?
  1. Use a custom Azure policy
  2. Create lock on NSG
  3. Block using the RBAC role
  4. Provide limited access

**Ans: 1. We will use a custom Azure policy which will help to define the policy.** Whenever an engineer creates an NSG automatically, the deny rule will be created with port 80.

6. You are the administrator of your subscription and you have 50K users. You want to create 10 more users in the Azure AD and assign the user administrator role to those users. What options will you choose to provide access to those users?
  1. Only create the users.
  2. Create the users and modify the directory role.

3. You can use the group policy to provide the access.
4. Use an active directory license to provide the access.

**Ans: 2. We will create the user from Azure AD and use the directory role to modify and assign the user administrator role to those users.**

7. You have 20K users, and now your organization IT head wants to buy 20 additional P2 licenses for higher management as they want to use the additional feature of premium AD. You have bought the 20 licenses. How will you configure them so that higher management can use the premium feature?
  1. You will assign the admin role to those users.
  2. You will create a user group that allows you to use the premium feature.
  3. You will assign the P2 licenses to each user using the license blade.
  4. You will use the RBAC role.

**Ans: 3. We will assign the P2 licenses to each user using the license blade because unless the license has been not configured, higher management cannot access the premium feature as those features will be available only if they have a valid license.**

8. You have created a storage account in the resource group BPBRG32, and now you have applied a read-only lock to BPBRG32. Which operation will you perform?
  1. You will delete the resource group.
  2. You can copy the storage key.
  3. You can upload the data to the blob storage account.
  4. You can change the replication settings.

**Ans: 2. You can copy the storage key because the read-only lock allows you to copy the data, but it will not allow you to modify or delete anything from the resources group.**

9. You have two Azure active directories `bpb.com` and `azure4you.com`. Now, you want to set up a default directory tenant to sign in to both the tenants. How can you configure it?
  1. Change the portal configuration settings.
  2. Use the PowerShell command.
  3. Change the directory from the portal.



4. You can change the subscription.

**Ans: 3: We will change the directory from the portal to set up sign in.**

10. **Your customer wants to enable the backup solution on Azure web apps name called bpbapp1. How will you process this request?**

1. Set up the third-party backup solution.
2. Use the backup policy to implement.
3. Configure the backup using the recovery vault.
4. You can use the Azure backup server for app services.

**Ans: 3: We will configure the backup using the recovery vault, which will help to take the backup of web apps.**

11. **A customer wants to transfer the data from the on-premises system to Azure. Which tool will you use to process it?**

1. Use the upload option directly to the blob storage.
2. Use the import and export option.
3. Create fileshare and map to on-premises.
4. Use the storage explorer to move the data.

**Ans: 4: We will use the storage explorer to move the data, as it is simple to use and tightly integrate with the Azure storage account. Then we will move the data to the storage account.**

12. **You are the global administrator of your Azure AD, and now you want to enforce the multifactor authentication. How will you process it?**

1. Configure the playbook for MFA.
2. Use the custom policy.
3. Configure the Azure AD Connect.
4. Use the Azure AD conditional access policy.

**Ans: 4: We will use the Azure AD conditional access policy which will help the MFA implementation organization. We can create a conditional access policy and apply it.**

13. **Your customer wants to configure the VNet name BPBVnetprod, which supports the VNet gateway configuration to configure the site-to-site VPN. What will you do?**

1. Create a Vnet.
2. Create subnet.

3. Create a VNet with the subnet gateway.
4. Create VNet with the subnet.

**Ans: 3: We will create the VNet with the subnet gateway, which will help to configure the VNet gateway and the site-to-site VPN.**

**14. Your Azure tenant has enabled the privileged identity management, and you want to see how many users have been assigned the security admin role. You need to review the security admin access role. How can you process it?**

1. In identity protection manager, you will configure the risk policy.
2. You will configure the weekly ad report.
3. You will configure the access review from the privileged identify management.
4. You will enable the AD audit logs.

**Ans: 3: We will configure the access review from the privileged identity management, which helps us to understand the details about access to that security admin and based on the report, we can decide it.**

**15. You have configured the multifactor authentication to all the users in your Azure tenant. A few of the users are having an issue logging in to mobile devices and are unable to reset the password. What is the solution you will apply?**

1. Self-service password reset.
2. Configure the mobile devices.
3. Create the password for those users.
4. Reinstall the app services.

**Ans: 1: We will enable the self-services password reset which will help the users to reset their password whenever it is required. Then, they will be able to configure the apps in mobiles.**

**16. You have a couple of storage accounts and your customer wants to restrict the access to the internet in the production storage accounts. Which is the solution you will apply?**

1. In the storage account, enable encryption.
2. Create the SAS key.
3. Enable the VNet integration from the firewall settings.
4. Enable the replications.

**Ans: 3:** We will enable the VNet integration from the firewall settings, from the Azure storage account, which will help to restrict the storage access to the internet.

**17.** Your clients have an on-premises network which contains multiple OS versions of servers. The client wants to migrate all the servers to Azure. You need to provide a solution to ensure that some of the servers which are available in single Azure data center and might go offline during planned and unplanned maintenance. What should be your recommendation to the client?

1. Fault tolerance
2. Low latency
3. Scalability
4. Replication to Azure

**Ans: 1:** We will suggest having fault tolerance in the workload, which will help during planned and unplanned maintenance.

**18.** You have 100 VMs in the Azure subscription, and now your customer wants to configure the backup. You have successfully created the backup. The client manager wants to enable the backup retention to 20 years? What is the solution you will propose to your customer?

1. Backup reports
2. Azure backup policy
3. Manually take the backup
4. Enable the replication for 20 year

**Ans: 2:** We will enable the retention period in the Azure backup policy, which will help to retain the backup for upto 20 years.

**19.** You have 50 storage accounts in the Azure subscription, and now your customer wants to create a container in 20 storage accounts. What are the tools you will use to create the container in the storage account?

1. From the portal.
2. You go to fileshare and create the container.
3. Manually create the container.
4. Azure storage explorer.

**Ans: 4:** We will be using the Azure storage explorer to configure the Azure storage containers.

**20. Your customer plans to map a network drive from several computers that run Windows 10 and Linux to Azure Storage. You need to create a storage solution in Azure for the planned mapped drive. What will be the solutions you will provide to the mapped drive?**

1. Enable the port 80.
2. Using fileshare, connect and enable the port 445.
3. Use the blob storage account.
4. Use the Azure containers.

**Ans: 2: We will use fileshare connect and enable the port 445, which provides the command to connect to Windows and Linux fileshare.**

**21. Your company plans to deploy web servers and SQL database servers to the Azure subscription. Now, you need to recommend a solution to restrict the connection between Azure web servers and SQL BD servers. What is the solution you will provide?**

1. You will restrict from the firewall.
2. You will use the route table.
3. Configure site-to-site connection.
4. Configure the NSG.

**Ans: 4: We will configure the NSG, which will help to allow or deny the traffic. It will help to restrict the outgoing traffic and it can only send the traffic to web servers to DB servers.**

**22. Your customer plans to migrate to Azure and the company has several departments. All the Azure resources have been used by each department and managed by an IT administrator. Now, the customer wants to provide the solution which will minimize the administrative effect and will be easy to manage by each IT administrator. Please provide the solutions.**

1. Multiple tenants with multiple subscriptions
2. Multiple region deployment
3. One tenant with multiple subscriptions
4. Multiple resource groups

**Ans: 3: We will choose one tenant with multiple subscriptions, which helps to separate the resources and its billing and also the administrative task to reduce the administrative workloads.**

**23. Your organization has multiple offices, and every month, you plan to generate several billing reports from the Azure portal. Every report contains the resources of each subscription. What is the feature you will use before generating the report?**

1. Azure policy
2. Tags
3. Cost management
4. Cloudyn

**Ans: 2: We will use the tags before generating the reports, which will help us to provide the expected reports, department wise.**

**24. You have multiple virtual machines, and now your customer wants to move the virtual machine from one subscription to another subscription. How can you process this request?**

1. Go to resources group, and click on **Move**.
2. From the virtual machine, we can go to **Move**.
3. Using PowerShell, we can do that.
4. Will use third-party tools.

**Ans:1: We will go to resources group, and click on Move and select the subscription to move the resources to another subscription.**

**25. You have multiple virtual machines and the backup has been configured in all the virtual machines. Now, your customer wants to understand the backup process and wants to show the report to higher management. What is the solution you will propose?**

1. Go to backup report.
2. From the virtual machine, we can go to move.
3. Using PowerShell, we can do that.
4. Will use third-party tools.

**Ans: 1. We will go to backup report and configure it, which will help us to provide the data and we can extract it in the PPT format for presentation.**

**26. You are the network administrator of your subscription and the customer has more than 50 VNet. Now, the customer wants to enable the VNet peering between VNetProd-to-VNetDev to enable the communication between both the VNet resources. What is the solution you will propose?**

1. Enable Vnet-to-VNet connection
2. Configure the VNet peering
3. Site-to-site VPN
4. Point to site VPN

**Ans: 2: We will configure the Vnet-to-VNet peering between both the VNets, which allows the communication between both the VNets.**

**27. You are the network administrator of your subscription and the customer wants to configure the Azure EXPRESSROUTE connectivity on-premises to Azure. The customer has decided the ISP, and the ISP has configured the on-premises connectivity. Now, you want to configure it. What is the service you can create to configure the EXPRESSROUTE?**

1. VNet
2. VNet gateway
3. Site-to-site VPN
4. Expressroute circuit

**Ans: 4: We will create the Expressroute circuit to configure the Expressroute connectivity. Then, we need to configure the VNet gateway for connectivity.**

**28. You have 100 virtual machines in your subscription, and there are 20 virtual machines in production environments. Now, your manager wants to enable the alerts and whenever your VMs reboots, deallocates, you should get an alert. What is the solution you will propose?**

1. We will create the rule.
2. We will configure with the Azure policy.
3. We will create two rules and one action group from monitoring.
4. We will set up alerts.

**Ans: 3. We will create two rules and one action group from monitoring. One rule to stop deallocation and another rule to reboot the VM. We will be associated with one action group to configure the alerts.**

**29. You have 20 virtual machines in your subscription and the customer has reported that few of the virtual machines are not connecting to the application, and the customer wants to fix the issue on priority. Which tool will you use to fix the issue?**

1. Network performance monitor
2. Application insight
3. Weblog analytics
4. Network watcher

**Ans: 4. We will use the network watcher tool, which will help to identify the issue of the servers and help to fix the issue quickly. It will also provide the input on traffic flow within Azure.**





# Index

## A

- Access control (IAM) 38
- Active Directory Domain Services (ADDS) 102
- Active Directory Federation Services (ADFS) 16
- AKS Cluster
  - network configuring 174
  - upgrading 173, 174
- App Container
  - creating 158, 159
- application gateway 240
  - backend configuration 244, 245
  - backend target, configuring 246
  - creating 242, 243
  - features 240-242
  - front-end configuration 244
  - HTTP/HTTPS listener, configuring 245
  - HTTP setting 247

- app services 178
  - backup 191, 192
  - configuring 182-184
  - creating 181, 182
  - dedicated compute 179
  - deployment slots, configuring 197-199
  - isolated compute 179
  - network setting, configuring 186-188
  - plan 180, 181
  - plan, creating 178, 179
  - private endpoint, enabling 188-190
  - shared compute 179
  - VNet Integration 190, 191
- app services plan
  - scaling setting, configuring 193-196
- app services security
  - authentication 185
  - TLS/SSL configuration 186
- ARM API 144
- AZ-104 Exam tips 326-328

**AzCopy**

- data copying with 103, 104

**Azure Active Directory (Azure AD) 2****Azure AD authentication**

- configuring, for storage account 101-103

**Azure AD Connect 16**

- features 16
- federation integration 16
- health monitoring 16
- installation prerequisites 17
- installing 17-22
- managing 23, 24
- pass-through authentication 16
- password hash synchronization 16
- synchronization 16

**Azure AD join 12****Azure alerts**

- configuring 289-292

**Azure ARM template 144**

- deploying 149
- modifying 144-149

**Azure backend pool 238****Azure backup 304**

- operations 315, 316
- policy, creating 307-309
- restoration 313-315
- vault creation 304, 305

**Azure backup reports**

- creating 310
- setting up 310-313

**Azure Bastion 266**

- creating 267-269
- features 266

**Azure Blob Storage**

- configuring 94-96

**Azure Data Box 100**

- authentication, configuring 101, 102
- data, copying with AzCopy 103, 104
- initial bulk transfer 101

- one-time migration 100

- periodic uploads 101

**Azure Data Lake Storage Gen2 101****Azure disk encryption**

- configuring 138-140

**Azure DNS 230**

- creating 231, 232
- DNS zone 231
- domain registrar 231
- records, creating 233, 234
- zone delegation 230
- zones 230

**Azure File share 110**

- configuring 110-113
- creating 110-112

**Azure File sync**

- configuration 114, 115
- group, creating 115-117
- troubleshooting 118

**Azure firewalls**

- configuring 262-266
- deploying 262

**Azure internal load balancer 235, 236**

- front-end IP configuration 237

**Azure Load Balancer 234**

- external load balancer 234
- health probes, creating 238-240
- internal load balancer 234

**Azure Log Analytics 296****Azure Metrics 293****Azure Monitor 288**

- activity logs 289
- application monitoring data 288
- Guest OS monitoring data 288
- resource monitoring data 288
- subscription monitoring data 289
- tenant monitoring data 289

**Azure Private Network 270, 271**

- private endpoint, enabling 271-274

**Azure quota 63**

- hard limit 64
- soft limit 63
- Azure resource group 55
- Azure Resource Group Manager 55, 56
- Azure Resource Manager (ARM) template 40
- Azure Service Health 293
  - health alerts 294
  - planned maintenance 293
  - resources health 293
- Azure site recovery 318
  - enabling 318-321
- Azure storage account 76
  - Blob storage account 77
  - configuring 80-82
  - creating 79, 80
  - GPv1 storage account 78
  - GPv2 storage account 78
  - network access, configuring 86-88
  - premium storage account 78
  - types 77
- Azure storage replication 82
  - Geo Redundant Storage (GRS) account 83
  - implementing 82-84
  - Locally Redundant Storage (LRS) account 82
  - Read-only Geo-Redundant Storage (GRS) account 83
  - Zone Redundant Storage (ZRS) 83
- Azure subscription policy 59
  - assignments 61-63
  - configuring 60, 61
  - creating 60
- Azure subscriptions 46
  - Azure Germany Customers 47
  - Azure Government Customer 46
  - free subscription 46
  - Microsoft resellers 46
  - open subscription 46
  - pay-as-you-go subscription 46
- Azure Subscription Support Plan 48
  - Azure Developer Support 48
  - Azure tenant 49
  - Professional Direct Support 48
  - Standard Support 49
- Azure tenant 49
- Azure Traffic Manager 248
  - configuring 248, 249
  - creating 248
  - features 248
- Azure Virtual Network 203, 204
  - address space 204
  - Azure VNet peering 206-209
  - creating 204-206
  - site-to-site VPN 213-215
  - site-to-site VPN connection, creating 215-218
  - subnet 204
  - virtual network gateway 209-213
  - VNet-to-VNet connectivity 218-220
- Azure virtual WAN
  - configuring 222
  - creating 223-227
  - features 222, 223
- Azure VMs 124
  - administrator account 126
  - auto shutdown configuration 128
  - availability set 125
  - availability zone 125
  - boot diagnostics 128
  - components 124
  - dedicated host 128
  - diagnostics account 128
  - disk type 126
  - images 126
  - Linux VMs, creating 134
  - network components 127
  - NSG 127
  - OS guest diagnostics 128

- pre-requisites 124
- proximity placement group 128
- public IP 127
- redeploying 140, 141
- resource group tag 128
- review and create 128
- scale set creation 134-137
- size 127
- Windows VM, creating 128-134
- Azure VMs backup
  - configuring 306
- Azure workspace
  - creating 297-299
- B**
- blob life cycle management
  - configuring 118-121
- Blob object replication
  - configuring 105
  - configuring, for block blobs 105-107
  - prerequisites 105
- Blob storage account 77
  - Access tiers 77
  - archive storage 77
  - cold storage 77
  - hot storage 77
- bulk user creation 2-4
- C**
- Cloud Solution Provider (CSP)
  - subscription 46
- Container 153, 154
  - App Container, creating 158
  - creating 154-157
  - scaling, configuring 158
  - sizing, configuring 158
  - uses 154
- Container App Instance
  - scaling, configuring 160-162
  - sizing, configuring 162-164

- cosmos database (DB) tables 76
- cost management 56
  - budget alerts, configuring 58, 59
  - exploring 56, 57
- custom domain 184
  - configuring 184, 185
- custom RBAC role 40
  - creating 40-42

## **D**

- Diagnostic Logs 294
- diagnostic settings
  - enabling 294-296
- disk type, Azure VM
  - HDD 126
  - SSD 127
  - standard SSD 127
- dummy objective exam
  - questions 330-338
- dummy scenario-based exam
  - questions 338-347

## **E**

- effective rules
  - evaluating 269, 270
- Enterprise Agreement (EA)
  - subscription 47
- accounts 47
- departments 47
- Enterprise agreement 47
- subscriptions 47, 48
- European Free Trade Association (EFTA) 47
- Exam preparation guidelines 326
- exam registration 328-330
- export job
  - creating 98-100
  - creating, in Azure 94
- ExpressRoute 220, 221
  - configuring 221, 222

**F**

free Azure subscription  
     creating 50-52

Fully Qualified Domain Name  
     (FQDN) 279

**G**

global administrator permission 54, 55  
 Global VNet peering 206  
 GPv1 storage account 78  
 GPv2 storage account 78  
 group creation 5-7  
     O365 Group 6  
     security group 6  
 group management 7, 8  
 guest user management 8, 9  
 GZRS-zone redundant storage 78

**H**

health probes 238  
     creating, for load balancer 239, 240  
 hybrid connectivity 16

**I**

import job  
     creating 94-98  
 IP addresses  
     modifying 253, 254

**K**

Kubernetes 165  
     creating 165-171  
     scaling, configuring for 171, 172

**L**

Linux VMs  
     creating 134  
 log search query functions  
     utilizing 299-301

**M**

management group 70  
     configuring 72, 73

creating 70-72

**N**

network access  
     configuring, to storage account 86-88  
 network performance monitor 283  
     configuring 283-285  
 Network Security Group  
     (NSG) 127, 251, 254  
     association 257-259  
     creating 254-256  
     inbound port 127  
     inbound rule 254  
     inbound rules, creating 256, 257  
     outbound port 128  
     outbound rule 254  
 Network Watcher 278  
     topology 279

**O**

Office 365 16  
 on-premises connectivity  
     IP flow verify 281, 282  
     monitoring 279, 280  
     next hop 282

**P**

password sync 30  
 password writeback 24  
     enabling, from Azure AD 25-28  
     enabling, from portal 28, 29  
     features 24  
 premium storage account 78  
 private IP address  
     configuration 252  
 public IP address  
     configuration 252

**R**

RBAC access configuration 35  
     resource access 38, 39  
     resource group access 37, 38

- subscription access 35, 36
- RBAC policy 34
- RBAC roles
  - contributor 34
  - owner 34
  - reader role 35
  - user access administrator 35
- Remote Desktop Protocol (RDP) 126
- resource group 55
- resource tag 64
  - resource lock configuration 65-67
  - resources group, removing 68-70
  - resources movement 67, 68
  - usage 65
- Role-based access control (RBAC) 34
- route table 259
  - configuring 261, 262
  - creating 260

## **S**

- Secure Shell (SSH) 126
- Secure Socket Layer (SSL) 186
- self-service password reset 10, 11
- shared access signature 84
  - generating 84
- SharePoint Online 16
- single sign-on (SSO) 16
- site-to-site VPN 213
  - configuring 215-218
  - creating 214, 215
- soft delete backup
  - using 316-318
- static IP 252
- Stock-keeping-Unit (SKU) 234
  - basic SKU 234
  - standard SKU 235
- storage account access key
  - managing 85, 86
- storage account data structure
  - storage, for VMs data 76

- structured data 76
- unstructured data 77
- Storage Blob Data Contributor 101
- Storage Blob Data Owner 101
- Storage Blob Data Reader 102
- storage explorer 88
  - implementing 90, 91
  - installing 88-90
- Storage Queue Data Contributor 102
- Storage Queue Data Message Processor 102
- Storage Queue Data Message Sender 102
- Storage Queue Data Reader 102

## **T**

- Transmission Control Protocol (TCP) 234
- Transport Layer Security (TLS) 186

## **U**

- user creation 4, 5
- User Datagram Protocol (UDP) 234

## **V**

- Virtual Hard Disk (VHD) 110
- Virtual Machine (VM) 59, 76
- VNet peering 206
  - creating 207
- VNet-to-VNet connectivity
  - creating 218-220
- VPN type
  - policy-based 211
  - route-based 211

## **W**

- Wide Area Network (WAN) 220
- Windows VM
  - creating 128-134