

# Microsoft Azure IaaS Defense in Depth Guide

A companion guide to apply defense in depth strategy  
to your Azure IaaS deployment

By Thuan Nguyen

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means – for example, electronic, photocopy, recording – without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

All trademarks, service marks, tradenames, product names and logos appearing in this book are the property of their respective owners.

This book is an independent publication and is not affiliated with, nor has it been authorized or sponsored, by Microsoft Corporation.

“I dedicate this book to my loving dad who sadly passed away 6 years ago.”

- Thuan



# Table of Contents

Preface.....	10
Who This Book Is For.....	11
What This Book Covers.....	11
How This Book Is Organized .....	11
What This Book Does Not Cover.....	12
Chapter 1 Security Thoughts.....	15
CIA Triad .....	16
Security is not a silver bullet.....	17
Security must come firstly from an awareness .....	18
Security by default before security by design .....	19
No Pain No Gain .....	19
Should not we care about security? .....	20
Redefine what is so-called security .....	21
Challenge in cybersecurity today .....	21
Summary .....	26
Additional references .....	26
Chapter 2 Understanding Microsoft Azure IaaS .....	29
Microsoft Azure Compliance .....	29
Microsoft Azure IaaS Model .....	30
Microsoft Azure IaaS Scenarios .....	32
Microsoft Azure IaaS Security Shared Responsibility .....	34
Azure Virtual Network .....	35
Azure Virtual Machine.....	37
Azure Storage .....	38
Summary .....	39
Additional References.....	39

Chapter 3 Defend Your Azure Network .....	41
Overview of Defense in Depth .....	41
Network Defense .....	43
DMZ Implementation .....	44
Network Segmentation .....	47
Stateful Packet Firewall .....	49
Routing to Defense System .....	53
Network Virtual Appliance .....	54
Secure remote connection .....	55
ExpressRoute .....	56
Network Availability .....	56
Sample reference .....	58
Government Cloud Reference .....	60
Summary .....	65
Additional references .....	65
Chapter 4 Protect your Virtual Machine .....	67
Disk Encryption .....	67
Antimalware for Virtual Machine .....	68
Hardened Virtual Machine Deployment .....	71
Virtual Machine Availability .....	72
Summary .....	72
Additional References .....	73
Chapter 5 Manage your identity .....	75
Understanding Azure Identity Access .....	75
Role-based access control .....	76
Multi-factor Authentication .....	78
Brute-force attack mitigation .....	81

Secure RDP .....	82
DMZ Implementation .....	82
Password Complexity.....	82
Enable Multi-Authentication.....	83
Identity Monitoring.....	84
Conditional Access Policy.....	84
Summary .....	85
Additional References.....	85
Chapter 6 Monitoring your Azure resource.....	88
Azure Security Center .....	88
Azure Advisor .....	89
Azure Monitor.....	90
Azure Log Analytics .....	91
Network Monitoring.....	92
Storage Monitoring.....	93
Virtual Machine Monitoring.....	93
Identity Monitoring .....	94
Summary .....	95
Additional References.....	96
Appendix Hands-On Lab .....	98
Lab 1 – Build your base SharePoint Farm .....	98
Lab 1.1 – Creating your Azure resource .....	100
Lab 1.2 – Creating Azure Storage Account.....	104
Lab 1.3 – Creating a virtual network .....	109
Lab 1.4 – Creating Azure subnet .....	111
Lab 1.5 – Creating web front-end availability set.....	114
Lab 1.6 – Creating an Active Directory virtual machine .....	116

Lab 1.7 – Configuring Active Directory Domain Services .....	124
Lab 1.8 – Creating Active Directory accounts .....	135
Lab 1.9 – Creating an SQL Server virtual machine .....	136
Lab 1.10 – Joining SQL Server to the domain controller.....	145
Lab 1.11 – Creating two SharePoint Server 2013 virtual machines .	152
Lab 1.12 – Provisioning and configuring SharePoint Server 2013 farm .....	160
Lab 1.13 – Adding the second web front-end virtual machine.....	166
Lab 1.14 – Creating a SharePoint website.....	170
Lab 2 – Azure Network Security Lab .....	176
Lab 2.1 - Setting up a jump virtual machine .....	177
Lab 2.2 – Setting up Point-to-site VPN gateway.....	183
Lab 2.3 – Connect to private virtual network from your laptop.....	196
Lab 2.4 – Blocking RDP from the Internet with Network Security Group.....	200
Lab 2.5 – Allowing RDP from the Jump virtual machine .....	207
Lab 2.6 – Allowing SQL Service to your database virtual machine .	209
Lab 2.7 – Routing to Defense System .....	213
Lab 2.8 – Deploying Azure Load Balancer.....	226
Lab 2.9 – Deploying Azure Application Gateway.....	234
Lab 3 – Virtual Machine and Storage Protection .....	241
Lab 3.1 – Implementing Disk Encryption .....	241
Lab 3.2 – Installing Microsoft Antimalware Extension.....	246
Lab 3.3 – Automating hardened configuration .....	251
Lab 4 – Manage your Identity .....	261
Lab 4.1 – Configure role-based access control .....	261
Lab 4.2 – Enabling Multi-Factor Authentication for Microsoft Account.....	263

Lab 4.3 – Enabling Multi-Factor Authentication for Azure AD account .....	269
Lab 4.4 – Forcing Multi-Factor Authentication with Conditional Access .....	274
Lab 4.5 – Protecting your Identity with Conditional Access .....	277
Lab 5 – Monitoring your Azure resources .....	280
Lab 5.1 – Overview of Azure resources in Azure Security Center ..	280
Lab 5.2 – Installing Qualys Vulnerability Assessment on your Virtual machine .....	284
Lab 5.3 – Configuring Security policy in Azure Security Center.....	292
Lab 5.4 – Exploring Azure Advisor .....	296
Lab 5.5 – Setting up Azure Log Analytics .....	298
Lab 5.6 – Adding Azure Network Security Group Analytics .....	301
Lab 5.7 – Adding Security Compliance suites to protect your Azure resource .....	306
Lab 5.8 – Exploring Azure AD Identity Protection.....	308

# Preface

Cloud computing offers number of benefits compared with on-premises, including hardware cost savings, hyper-scale advanced workload to fully automation capability to step up to DevOps cultural transformation.

Organizations are looking into transforming their infrastructure to the cloud to take these advantages. Such a transformation is not new today, it's a "shift-and-lift" strategy every organization has been planning for. One of the considerations when moving to cloud is security that people often misunderstand. Your transformation to cloud does not mean everything you have is going to be fully protected. There are a variety of things to be considered, including security strategy, responsibility to security and risk governance. If not carefully planned, impacts shall be huge and damage to organization's sustainability.

Having worked with cloud computing since 2011, primarily focused on Infrastructure-as-a-Service (IaaS) model, my job is not only to help customers transform to the cloud, but also to educate them as to why they still need to coordinate with cloud service provider to protect their environment. The most common misperception is when moving to the cloud, the cloud service provider has fully responsible for customer's tenant security. This leads to unawareness of security that results to business owner a nightmare when security breach happens.

Part of my cloud journey, I have worked with the architect and operational team of a private cloud built for government. For the time being, my responsibilities include planning and designing security architecture, ensuring the technical architectural compliance, and deploying Microsoft Products and Technologies for several government agencies. This drives me to thinking about this book to fulfil your knowledge pocket by my experience with several private cloud providers I have been working with including governmental environment.

# Who This Book Is For

This book is hopefully written for the audience of Azure IT Pros, Solution Architect who work in a daily basis with Microsoft Azure platform, focused on infrastructure architecture and system management to learn more about Cloud IaaS security in Microsoft Azure specifically.

This book is also for IT Manager, C-level or consultants who want to understand how Microsoft Azure can help protect the environment.

The book can also be beneficial to an absolute beginner who needs to quickly adopt Azure IaaS knowledge before taking off to the Microsoft Azure journey. It will explain many Azure concepts and step-by-step guidance to build an experimental lab for security test.

This book assumes you have some familiarity with cloud computing, and you have an understanding of infrastructure and network in particular.

# What This Book Covers

The book will provide you general information of the private government cloud and its security design considerations that are keys to get started with applying defense in depth strategy to your Azure IaaS deployment.

It will also give a comprehensive look at various Azure features you can use to protect your environment.

You will also learn number of different security practices coming along with build-in features that Microsoft Azure is offering to defend from common attacks (e.g. brute-force attack, Distributed Denial-of-Service, Surface attack).

# How This Book Is Organized

This book is organized into the following chapters:

Chapter 1, “Security Thoughts”

The book begins with my introduction of personal security principles I have realized during my time working on the field of cybersecurity.

Followed by these principles, this chapter will present today cybersecurity challenges which would require modern technology to help.

## Chapter 2, “Understanding Microsoft Azure IaaS”

This chapter takes a comprehensive look at Microsoft Azure IaaS (Infrastructure-As-A-Service) including some services you need to know basically before planning for security. We also discuss shared responsibility in security and Microsoft Azure compliance which are helpful when presenting to your manager or customer.

## Chapter 3, “Defend Your Azure Network”

Network is part of your infrastructure on Microsoft Azure, which is also one of the core components. This chapter focuses on number of different practices, including build-in features Microsoft is offering to protect your Azure virtual network.

## Chapter 4, “Protect Your Virtual Machine”

Virtual machine on Microsoft Azure is where you deploy your application and database workloads. This chapter discusses the approaches to protecting Azure virtual machine, and automating hardened on-boarding virtual machine.

## Chapter 5, “Manage Your Identity”

This chapter gives you an overview of what Microsoft is offering to manage your identity. It will also provide practices to not only monitoring the identity but also mitigating brute-force attack.

## Chapter 6, “Monitoring Your Azure Resources”

Protecting your infrastructure includes monitoring effort because it lets you catch up what is badly going on when you receive an attack. This chapter introduces number of different ways to monitor your Azure resources you need protect.

## Appendix, “Hands-On Lab”

Without practice, it is hard to understand completely what is written in this book. The Appendix provides you step-by-step guidance on how to implement a lab for evaluating security features discussed in every chapter. The lab is SharePoint Server 2013 farm deployment on Microsoft Azure.

# What This Book Does Not Cover

Firstly, let's me frankly speak to you. This book is not going to introduce myself as a hacker, neither hacker wannabe. Perhaps I would humbly call myself an advanced script kiddie which is quite good at understanding how

things work, attack flow and can modify variables in payload to exploit something for evaluation or internal investigation purpose.

This book is not also going to share too much about government cloud due to non-disclosure agreement and national security policy. What are written in this book related to the government cloud were already published over the Internet.

I do not focus on web application and database security in this book because each platform may have its own security feature and mechanism to talk about. Moreover, there will not be an introduction to both Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) models in Microsoft Azure.

You will not find scientific security engineering with deep-dive on network protocol, neither complex cryptography in this book.

Lastly, this book is not going to introduce Azure Government which is currently dedicated for U.S. ICT government. You can find useful information about Azure Government at <https://azure.microsoft.com/en-us/overview/clouds/government/>

*This page intentionally left blank*

# Chapter 1

# Security Thoughts

There are many forms of security principles in the field, depending on which of the guide you follow. In this chapter, we are going to explore some common security principles that are broadly applied in many organizations, and my thoughts of today's cybersecurity.

There are many debates in the community to find out differences between two terms: “*information security*” versus “*cybersecurity*”. There are also other terms such as “*computer security*” or generally “*IT security*” that are also brought into the table. The ultimate objective of information security is to protect information and prevent from being stolen from someone who is not authorized to have access to. The ISO/IEC 27000:2013 also defines information security as preservation of confidentiality, integrity and availability of information. “Information” at this point is not really referred digitalized information in your computer. It can be a physical paper of accounting record that is confidential. While cybersecurity is targeted to protecting digital assets in an organization, including computing devices, connected computer, network infrastructure, communication or so on. By that mean, physical paper is not considered a “cyber-asset”. If we bring information security into the computing world, then we would see the overlap between the two terms. You might have yourself the question: which of the thing in this book do we refer to? The answer is the objective of protecting your system and data from the attack. This book is not going to clarify clearly differences between these terms. You should be able to understand the objective of security written in this book. I consider in this book that information is digital or electronic data in computer.

# CIA Triad

At the very first time hearing CIA, you would imagine a civilian foreign intelligence service of the U.S. federal government, named Central Intelligence Agency, with the abbreviation is CIA. Although this department is tasked with gathering, processing and analyzing national security information from around the world, it is not the CIA Triad you are going to learn.

CIA is the combination of Confidentiality, Integrity and Availability when it comes to information security. We do not know exactly who coined this triad. There are some sources indicating the credibility of CIA triad is for Julius Caesar – a Roman politician. CIA triad is the most common key principle to building up security plan. We can see this term in every fundamental information security course, and industrial security certifications such as Certified Information System Security Professional (CISSP).



**Confidentiality** is part of your life obviously. This can be seen in an email containing financial transaction report. This can be seen from an IT email asking you to protect your password. If something is said to be confidential, it is not supposed to be disclosed to unintended people. Compromised confidentiality we have seen in the computing world is password hacking. Password is your own asset, and it needs to be very confidential. Otherwise you have your own personal purpose to share to someone else. If that is not the case, if your password is known by someone you do not expect, the confidentiality is not maintained.

**Integrity** may be hard to be realized in your real life. It is referred to a protection from unauthorized manipulation. A sample case is that your phone's wallpaper is changed without you. Another example is email content sent from your colleague to you. Whatever he sends to you must be exactly the same when you read the message. If not, the integrity is compromised. Integrity in CIA triad is objectively to aim to prevent any change on your data without authorization.

**Availability** might be strange because this sounds irrelevant. In the field of security, availability is very important. It implies that information must be available to authorized people when required. It applies both to data and system services. Consider the case of availability a user for a financial department needs to retrieve financial report but the system does not return due to unavailability. Access denied you may have encountered can be seen as a case of availability breach which may lead to security incident. Availability aims to business user first, then system administrator. If a system is unavailable, the administrator cannot monitor to timely detect suspicious activities in the case of hacking.

No matter what yours is, there must be a principle on something to get started. To me, from the first step, I do not look for a technical and architectural framework for security. Instead, I often start with the following experimental principles I have found for myself. During the past 6 years, these principles have come helping me a lot not only in security design, incident investigation but also in educating my customers and colleagues for an effective security plan and implementation.

- Security is not a silver bullet
- Security must come firstly from an awareness
- Security by default before security by design
- No pain no gain

## **Security is not a silver bullet**

If you do a search over the Internet, you will get to meaning of term “silver bullet”. A silver bullet is metaphorically described as a magical solution that can solve a complicated problem. It sounds like there is only one solution in the world that can be applied to everything. Ask yourself whether an only solution that addresses to every security issue. Such a solution never existed in your life. Every system or software built on it always has a security

breach. It can be found today, or tomorrow or next month depending on how valuable your system is when compromised, which attackers pay attention to. Even some of the historical stories about Snowden you have heard of somewhere, the electronic repository storing top secret-classified document was leaked. Another example is that some systems in NASA (National Aeronautics and Space Administration) were compromised, revealing some high-end technologies that the organization developed. One of the world's most popular movies Fast and Furious 8 recently has shown us the concern of car hacking in the digital transformation. It looks like a magical hacking ever in the history but it will soon become true if security is not being seen a critical factor in autonomous technology development. Such a story tells you one thing: do not expect to see a zero-security-vulnerability system in your life.

Organizations do need to combine all possible security technologies to protect them. They also need to get rid of the silver bullet thought when it comes to security.

## **Security must come firstly from an awareness**

During my time working with many government agencies, I have realized that security awareness is very important to developing a solid security strategy for the country. Information related to computer security and personal privacy are everywhere in the country. You can catch it up when in an elevator. You can happen to see some of the data security posters in a toilet.

The idiom “The leopard cannot change its spots” would address the security awareness concern. It is hard to change who you are, no matter how hard you try. The change requires uncountable duration and time. Even when you try to educate them how big the impact is when security incident happens, and how much they may lose if their data is compromised. Training to improve security awareness is indispensable.

Another perspective in security awareness is the human factor which is the target to attack. An example of lack of security awareness is the use of simple password which allows an attacker to successfully get by using brute-force technique. Low security awareness also can be seen from coding practice when your developers do not have plan for writing a secure code

from the scratch. This results not only software vulnerability, but wasting efforts to remediate in the future. Whatever it can be, without security awareness in mind, your system will never be protected enough. One of the security incidents in my team a couple of months ago, allowed an attacker to successfully remotely connect to a virtual machine hosted on a public cloud after brute-force technique. In a nutshell, security would become useless without security awareness.

## **Security by default before security by design**

Security by default is a common approach to implementing a secure system. It is to make default configuration in the system you are going to build as secure as possible, by default. An example of security by default is password complexity policy. To protect your end user, by default, your end users must set up password as complicated as defined in your policy. It can be a password of minimum eight characters, including one capitalized letter, one number and one special character. Moreover, the password is not allowed to be the last five historical ones. This familiar example can be considered as a security by default.

After security by default is applied, move on to security by design in which you plan to design a practical architecture to prevent your system being attacked, or exploited by an attacker to scan vulnerability. One of an example of security by design is using DMZ (demilitarized zone) we will discuss later in the book. The security by design often includes programming practices to implement extra security features (e.g. token validation, dynamic regression, cryptography algorithm...)

Security by default and security by design are taught in security development lifecycle to educate the project team including developer, project management, quality assurance person, tester to fully understand how security is importantly engaged in the development lifecycle.

## **No Pain No Gain**

Why no pain no gain? This motto inspired us in the life that if you never suffered a pain, you would never feel how painful you would be, and never gain that experience from the pain. I personally believe “No Pain No Gain”

is a true principle to everyone. When you try yourself applying security by default and security by design approaches, you should be optimistic to gain experience if the system is hacked by someone. From such, you would gain experience to improve your system, and make it more stable as possible by the time flying.

“No Pain No Gain” often comes with incident response management in the security context. While you can gain experience from an attack, your incident response to business users are controlled, giving them a feeling like nothing is really happening.

## Should not we care about security?

When we ask ourselves the question “Should we do that?” we would often have a tendency to think of our sake which become the motivation to do so. This is not a practice to come up to the list of problems. Instead, the practice should be the question “Should not we do that?” in order to identify main reasons. When it comes to security, we all see that security is very important. But what if we do not care about security? Think about an impact when your internet-facing e-commerce website is hijacked by an attacker. He may take down to make your services functioning to business users unavailable. When the system is not working, your target online visitors cannot go to the online shop to check out something. This is the loss of potential opportunity in your business. The unavailability does prevent you from operating business. The consequence is that bad as you are going to lose your money.

If that is not unavailability, but a case of compromised intellectual property, what would happen then? Such a data can be sold to your competitor. We are living in a digital transformation era, we see things are going to be digitalized. The big data revolution is raising the concern of lack of data for advanced analysis. Hence, data including intellectual property, business result, financial report, confidential employee information, salary information are valuable and can be sold to your competitor. This will debase your company reputation. When this case happens, your business would be possibly devastated.

---

According to “2016 Cost of Data Breach Study: Global Analysis” research conducted by Ponemon Institute LLC and sponsored by

IBM, the average total cost of a data breach increased from \$3.79 to \$4 million.

---

## **Redefine what is so-called security**

Secure is not going to be defined here again. You all have your own definition. Whatever you think about it, I believe you are correct. I just wanted to have a different extreme in defining security. First, security is a company reputation. The case of Tesco Bank with approximately 40,000 accounts compromised reported in 2016 should be mentioned when it comes to the company reputation. We do not know exactly the number of customers that Tesco Bank may lose in the future. But we should acknowledge the fact that Tesco Bank's reputation since this case has been debased.

If security is considered a company reputation, it will also be a metric of quality for software development. A software without security metric quality assessment is not really a software today. Software companies should focus on security development lifecycle, awareness program or so on to make sure their software delivered to business customers will not affect the reputation.

## **Challenge in cybersecurity today**

In this section, I just wanted to explain just a little bit as to why cybersecurity today is totally challenging. Although this section below does not address to the main content in the book, this is still helpful to see the overview of the new modern security.

According to Wiki, digital transformation is the changes associated with the application of digital technology in all aspects of human society. The transformation means to changes of the business and people action, in resulting to the better outcome. The term is not new. It's been for a quite long time in the world of information technology. Organizations are embracing digital transformation to change the business landscape. The number of buzzwords you have heard every day: BYOD, IoT, Cloud, Big Data & Analytics.

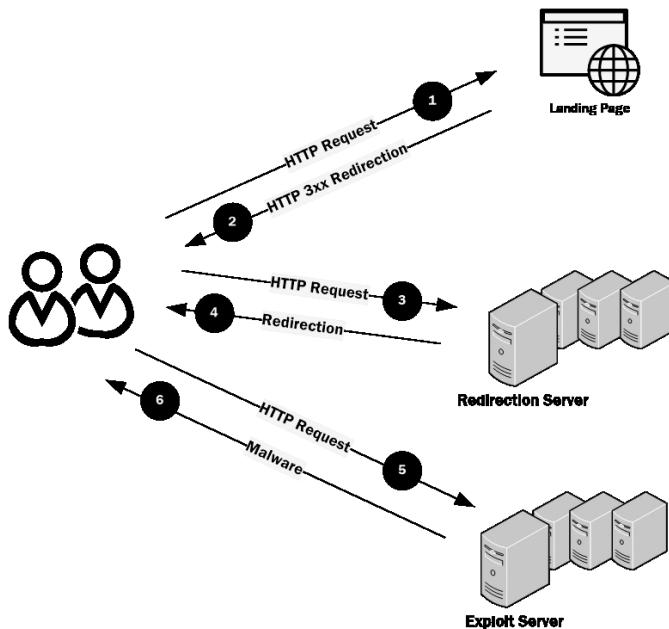
I have worked in Singapore for years, having a chance to realize the explosion of BYOD (Bring Your Own Device) trend. When in a train, don't be surprised by how people bow their heads to mobile devices. They

seem not to know each other. Even they are friends, they still seem. The culture of “Bowing down to the Device” may describe exactly the BYOD trend in Singapore, and in Vietnam as well. One of the world’s most famous slogans is “**Connecting People**” may not be true today because nobody actually looks at each other in a natural conversation.

Internet of Things becomes Things of Internet. Everything is going to be connected to the Internet and becomes much smarter. Imagine in your home, you forget to turn off the air conditioner, a smart device can check and alert you while triggering a process to turn the air conditioner off. Look at a few car manufacturers, they are developing a smart car ever historically that can be autonomous on a zigzag road. A driver now just simply need to keep his hands on steering wheel to concentrate on driving, while most of the other actions he needs such as asking the car to suggest nearest supermarket, or picking up a call can be done by smart devices. When the IoT comes in, data shall exponentially grow, creating a big data revolution. The investment to infrastructure for handling such so-called big data is extremely hard. Hence, people look at cloud adoption. It’s like they borrow the infrastructure of another provider to handle big data in a manner of subscription model.

Talking about the era of digital is not that short within a page or in a day. Even this topic is supposed to creating a big data of information about it. The wave of digital transformation contributes significantly to number of different things. First, it’s Big Data. Every piece of information is considered data. And Data is not just a plain-text file, or just a structured database you do in your IT life. Data can be a video, picture, a document or even a voice recorded during a conference call. Securing such a diversity of data gives you a big challenge. Organizations need to be more open to connect with partner and external systems, surely giving more opening doors to attackers. The working environment is so dynamic and becomes unpredictable. To elaborate how challenging the modern cybersecurity is, I want to give two examples indicating two common problems of cybersecurity today: Malnet and Internet Fraudulence.

Malnet (Malware Distribution Network) is a big and dynamic network of malware circulating over the Internet, designed to deliver massively number of malicious activities to Internet user. The more the Internet user, the more dynamic the malnet.



The illustration below gives you an example of how a typical malnet works. A victim firstly reaches the website via search engine result (e.g. Google, Bing). He clicks on an iFrame which looks informative (e.g. up-to-date stock information, weather prediction, advertisement banner...). The landing page returns back an HTTP 3XX in which the first level referral is executed, redirecting the victim to another URL. A next request from the victim is generated, hitting to a group of servers playing as front-end proxy or redirection server to drive the victim to the malnet. The redirection may be repeated a few times going through a few groups of redirection servers, before getting into the malnet. The malnet finally sends malicious code to the victim which he has successfully executed.

Preventing malnet distribution servers requires the ability to identify the polymorphic model of malware and URL, because the victim gets directed through several times until he reaches the malicious code. Today, identifying if the URL is safe is not easy. There has to be the implementation of URL reputation system to eliminate all the malicious URLs. This sounds easy, doesn't it? Can you imagine how many safe URLs you are going to add into your URL reputation system?

The next example is online payment with digital card (mostly Credit Card). People go shopping online and use their credit card to rapidly

process the payment. The more people go with online payment, the broader the door is open for attackers who do something to grab your card information. The application must have the ability to verify if there is fraudulence. In the past, there was not much of information which is like:

Name	Amount	Fraudulent
Carter	2,650 USD	Yes
Allien	1,890 USD	No
Chris	2,100 USD	Yes
Peter	1,500	No

Look at the table above, the rule seems to be like if the transaction amount is large than 2,000 USD and the name starts with the level “C” then set the fraudulent = TRUE. But if today the information is collected like the one below:

Name	Amount	Where Issued	Where Used	Age	Fraudulent
Carter	2,650 USD	Singapore	U.S.	20	Yes
Allien	1,890 USD	U.S.	U.S.	25	No
Chris	2,100 USD	Hong Kong	Singapore	22	Yes
Peter	1,500 USD	UK	Singapore	28	No
Bethany	2,750 USD	Australia	Hong Kong	23	No
Weller	3,000 USD	U.S.	China	26	Yes

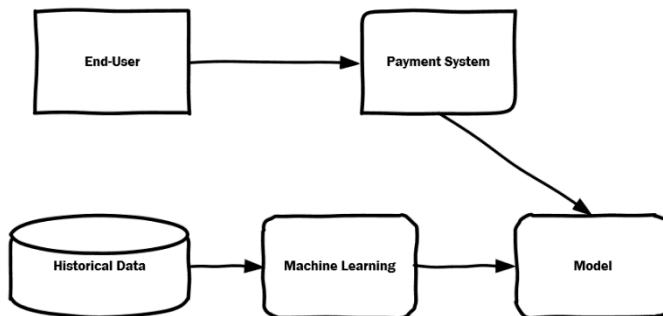
The rule to identify the fraudulence becomes more complicated than the first sample. There should not be the same rule saying that if somebody pays over 2,000 USD with whose name starting by “C” is a case of fraudulence.

By means of two examples, you would realize that the big challenge is to identify and predict pattern (in both malnet and fraudulence) that has never existed. How does your system know if a request send to your web application does not comprise of set of malicious code? Signature-based classification is cool but it not that easy to handle. Another example to help you see the challenge is detecting malicious request sent to your web application from the Internet. Everything is dynamic and polymorphic. Payload has changed the way it works. In a nutshell, the detection and prevention in the modern cybersecurity becomes harder ever!

Look at the first example – malnet, there should be a mechanism to enable your firewall/security system to learn more about the URL whether it is malicious or benign. Yes, it's how machine learning is determined. It

the case of building the URL reputation system the application (let's say it's the one that prevents malware) there is a pre-classified data set to train the system to be smarter to know if a URL is malicious or benign. Features shall be then extracted from the set of pre-defined URLs with specific characteristics of a URL. For example, the number of character and the number of special character (non-alphabetical) in a URL. In theory, it sounds simple. But the fact that it's complicated. There are number of steps to produce and train the detection & rating model with training set and the selection of machine learning algorithm is the key to success.

For the online payment, the fraudulence detection is implemented maturely in most of big online payment system provider such as PayPal, Visa, MasterCard or so on. First, with Machine Learning, there is a selection of data. The more data you have the better result. Selecting right data to process is very important. For example, the time when someone uses credit card, the location he uses, even the age and sex.



The PROS in Machine Learning applied for this case is that it can effectively learn complex fraudulent patterns and can handle large volume of data with big data technology. Moreover, with machine learning technique, the application can predict new types of fraudulence which the traditional expert-driven approach couldn't. However, the CONS are the sample of data and training set which contributes to an effective detection is not enough today, and perhaps results highly rate of false positive.

There are number of recommended machine learning algorithms for such cybersecurity per my research

- Random Forest
- Expectation-Maximization
- Naïve Bayes

- K-Means

Machine Learning often comes with big data & analytics to offer an end-to-end solution. Without big data & analytics, applied machine learning doesn't make so much of sense.

Machine Learning does play a significant role in the modern cybersecurity. In real-world scenario, Machine Learning is used to detect fraudulence, to identify suspicious domain to prevent malware, to classify anomaly requests and activities in SIEM (Security Information Event Management) to model threat, and more ideas you can read here <http://www.mlsecproject.org/#open-source-projects>

Today there are number of big vendors providing Machine Learning and Big Data Analytics that you can experiment, including:

- SAS Analytics Suite
- RapidMinder Studio
- Alteryx Analytics
- IBM SPSS
- SAP Predictive Analysis
- Oracle Advanced Analytics
- Microsoft Azure Cortana Intelligence
- Google Machine Learning

## Summary

In this chapter, you were introduced to the concept of confidentiality, integrity and availability in the CIA triad, with a few examples. You also learned about my personal principles when it comes to security. You also saw a different extreme of what is so-called security and how important it is. Now that you have finished with this chapter. The last section did tell you how challenge security is today. This can help for you to prepare series of approaches for end-to-end security solution.

## Additional references

We always want to learn more things to fuel up our knowledge, here are some additional references that might be useful:

- CIA Triad Introduction: <http://resources.infosecinstitute.com/cia-triad/>

- General information about CISSP – Certified Information Systems Security Professional: <https://www.isc2.org/cissp/default.aspx>
- The Importance of Security Awareness Training: <https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013>
- The Biggest Cybersecurity Incidents of 2016: <http://resources.infosecinstitute.com/the-biggest-cyber-security-incidents-of-2016>
- Why Machine Learning Is Our Last Hope for Cybersecurity: <https://www.datanami.com/2016/04/21/machine-learning-can-applied-cyber-security/>

*This page intentionally left blank*

# Chapter 2

# Understanding Microsoft

# Azure IaaS

Without understanding the Microsoft Azure IaaS model and its offering, you cannot design and build an effective secure system hosted on Microsoft Azure. In this chapter, we are going to explore fundamental Microsoft Azure IaaS, and each service offerings.

## Microsoft Azure Compliance

If you are working with Microsoft Cloud sometimes, you may have heard about Microsoft Trust Center where Microsoft proves to its customers a trustworthy platform. From the center, Microsoft shows not only compliance achievement but also security privacy and its practices. To Microsoft Azure specifically, the Trust Center is <https://www.microsoft.com/en-us/trustcenter/cloudservices/azure>

Industry	United States			Regional		
 ISO 27001	 SOC 1 Type 2	 SOC 2 Type 2	 FedRAMP FedRAMP IAB FATIG	 HIPAA - HITECH	 FIPS 140-2	 Argentina Data Protection Act Ley 27.652
 PCI DSS Level 1	 ISO 27018	 ISO 27001	 FDA 21 CFR Part 11	 FERN	 EISA Level 2	 European Union Model Clauses
 GRCI German Chemistry and Plastics Industry Association	 ISO 27001	 CSA Cloud Security Assessment Protocol Version 1.0.1	 ITAR	 GDS	 ITAR-ready	 GOV.UK United Kingdom G-Cloud
 MPAA	 Shared Assessments	 NIST 800-53 Control Matrix v3.0.1	 FISMA Section 108 VRATs	 NIST 800-171	 China TRUST	 Canadian Privacy Laws
 Gartner	 ISO 27001 (IEC 27001)	 GSA	 GxP	 DIACAP	 iDA Information and Data Assurance Regulation Scheme	 Iraps Australian Signals Direction
 NIST 800-53 Control Matrix v3.0.1	 GSA	 NIST 800-171	 FATIG	 ENISA	 FIEC Financial Institutions Enhanced Compliance Evaluation Committee	 Cloud Security Mark Gold
 NIST 800-53 Control Matrix v3.0.1	 GSA	 NIST 800-171	 FACT	 Privacy Shield EU-US Privacy Shield	 NCCP Framework	 China Multi-Level Protection Scheme
 Gartner	 ISO 27001 (IEC 27001)	 GSA	 DIACAP	 FACT	 Privacy Shield EU-US Privacy Shield	 Japan My Number Act

Microsoft seems to achieve industrial compliance in every big market it targets to. From the compliance offering list, you can filter your country to see if any.

Microsoft also has several centers for cybercrime and malware protections, for example Microsoft Cybercrime Center, Microsoft Malware Protection Center. There is a dedicated unit called Microsoft Digital Crimes Unit (DCU) responsible for stopping or interfering with cybercrime and cyber threats. Not too much to explain here, but we all know Microsoft has vastly invested in its cybersecurity to mitigate threats and protect its online services currently being used by hundreds of millions of people across the globe.

If you are asked how secure Microsoft Azure is, make sure to pass over the Microsoft Trust Center link to your customer.

---

With such a long list, do not make your assumption that Microsoft Azure is the most secure platform in the world. Put your head down not to think that everything you are going to deploy on Microsoft Azure is fully protected. This list can help in a few ways. First, it is a selling point to make a decision if security compliance and privacy are raised. Second, this list can be competitive to other cloud service providers such as Amazon AWS, IBM, Google Cloud. The list does not bring a good sleep to you as always, and makes you feel safe without any concern when hosting on Microsoft Azure.

---

## Microsoft Azure IaaS Model

Cloud computing is heterogeneously broad, relating to variety of software services to hardware infrastructure. Nevertheless, people are still following

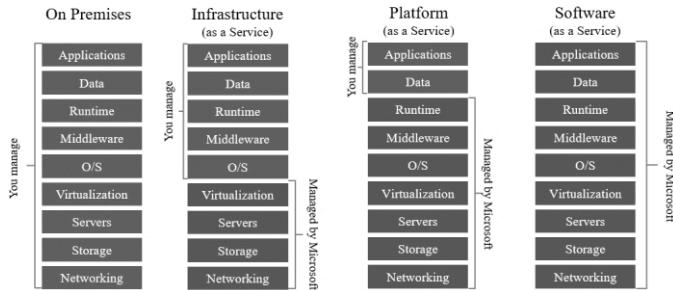
the U.S. National Institute of Standards and Technology (NIST), defining three service models:

- **Software as a Service (SaaS):** this is the model when cloud consumer has access to cloud service provider's software from the Internet. An example of the software is Microsoft Office 365, which offer you set of business productivity services including instant messaging and video conferencing tool (Skype for Business Online), email messaging tool (Exchange Online), collaboration and file sharing (SharePoint Online and OneDrive). The cloud consumer does not manage underlying cloud infrastructure including network, server, operating system, storage. The cloud consumer may have access to limited software configuration settings (e.g. SharePoint Online Central Administration).
- **Platform as a Service (PaaS):** more granular control than the SaaS model, cloud consumer is given to have access to development platform, web server or database instance. The cloud consumer may have access to the cloud service provider's extensibility module, library and tools to develop more robust application hosted on the underlying cloud infrastructure. The cloud consumer still has no control in network, server, storage and operating system.
- **Infrastructure as a Service (IaaS):** the cloud service provider provides infrastructure resources such as network, storage and other fundamental compute resources to allow cloud consumer to fully deploy their system upon specific demands. In this model, the cloud consumer is given to tailor its infrastructure but still cannot manage the underlying infrastructure.

Microsoft Azure IaaS should not be an exception. It still follows NIST definition. Below is the illustration of four models specific to Microsoft - a cloud service provider and you - a cloud consumer. In the on-premises model, you control everything. This includes infrastructure resources such as networking, storage, server, virtualization platform to application and data. Microsoft has nothing to do in this model until you wish Microsoft support if you are using its products e.g. System Center, Hyper-V or so on.

In the IaaS model, Microsoft provides networking, storage, server and virtualization technologies to assist you to build your own virtualized

infrastructure. You have your own decision to choose operating system, data, application. You can pick a virtual machine size you need, deploy it on Microsoft Azure. You can specific the operating system (e.g. Windows Server 2012) you want as well. You can also configure for high availability for your workload deployment (e.g. SharePoint farm deployment).



## Microsoft Azure IaaS Scenarios

When you choose Microsoft Azure IaaS, you must have your own reasons. Below are some of the common scenarios people choose Microsoft Azure IaaS:

- Development and Proof-of-Concept (PoC)
- Disaster Recovery
- Hybrid Deployment
- High-performance Computing

One of the common scenarios is using Microsoft Azure IaaS to do demonstration, development and PoC showcase. Let's see an example of Microsoft SharePoint. Since the version of SharePoint 2013, people are quite afraid of the hardware specification requirement. A single-server farm would be enough for a standalone development environment. However, if you need an advanced evaluation, such as Enterprise Search in a multi-server farm, then the environment need to be large. While this becomes a concern in on-premises, there is still an option on the cloud. With Microsoft Azure IaaS, you can very quickly provision virtual machines with specification you need to create a SharePoint farm. Another advantage is that if you do not need to use your evaluation environment, you can turn your virtual machines off any time to save the cost.

Building development workstation on Microsoft Azure IaaS is a good choice for small company when hardware becomes a consideration. Large organization can be beneficial too, but this requires a security governance and quite complicated setup to establish the hybrid model between Azure hosted development environment and on-premises production environment. Of course, the big advantage is that you do not have to maintain a large development environment to just focus to your production environment only.

In Microsoft Azure IaaS, there is a large image library that Microsoft has prepared for your quick deployment. For example, if you choose to deploy SharePoint Server 2016, there is an image called SharePoint Server 2016 Trial that contains installed pre-perquisites inside.

The next scenario is **Disaster Recovery**. If there are many business-critical applications you are running, then disaster recovery is supposed to be required. You already know that building a disaster recovery (DR) site is not easy, requiring complex infrastructure setup from network, storage, hardware to application and database level. In this scenario, we expect to build a cost-effective DR solution. Microsoft Azure IaaS can be your choice of building a secondary site instead of preparing a costly on-premises datacenter.

Not only a reliable infrastructure and simplified management, Microsoft supports you to deploy your farm on Microsoft Azure by Azure Site Recovery. This kind of service simplify the infrastructure replication to Microsoft Azure.

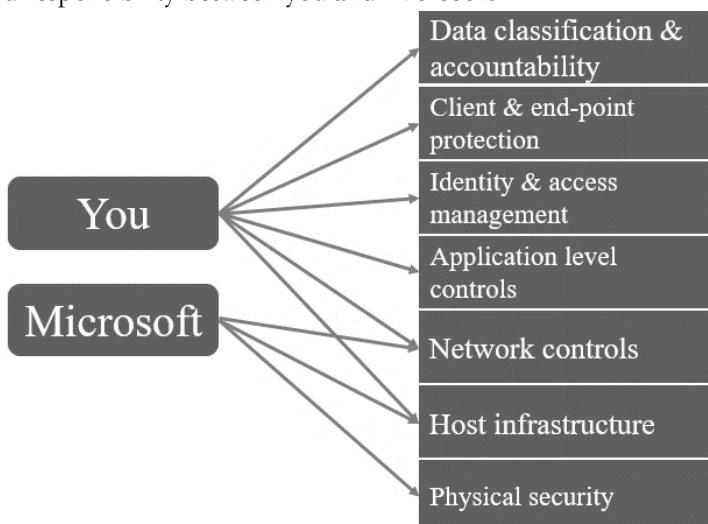
The term **Hybrid** is used in the world of cloud computing these days to describe a scenario in which your on-premises resources communicate with cloud resources. The easily seen scenario is when you have your own Active Directory domain controller in an on-premises environment providing identity service to a system hosted on Microsoft Azure to achieve single sign-on.

Why should you consider Azure hybrid deployment? It is perhaps everyone else is doing it. Cost for hybrid is not going to be discussed here. However, when you do the hybrid, you are going to cut at least operational infrastructure and licensing cost which occupies entirely your cloud budget. In many cases when doing hybrid, you are to outsource data security responsibility which might be a big concern.

**High-performance computing** is another scenario when you need a super-performance computer to solve complex problem, requiring millions of calculations.

## Microsoft Azure IaaS Security Shared Responsibility

Because this book is about Microsoft Azure IaaS security, there must be an understanding of shared responsibility so you will incorporate with Microsoft to build and better harden your system. Below is the illustration of shared responsibility between you and Microsoft.



Data privacy becomes the regulation which is often brought up to discuss about cloud security. Cloud service provider like Microsoft always put in its contract and term agreement that it has no privileges to access to customer data. That said data classification and privacy is your responsibility. The level of confidentiality is defined by yourself. Microsoft can help by offering encryption option for you. But it leaves you the choice whether you like to encrypt your data or not. You are fully accountable for your data even it resides in Microsoft infrastructure somewhere.

Next, client and endpoint protection are part of your responsibility. This often refers to protecting your virtual machines and any client inside your virtual network from virus or malware. Microsoft is offering a built-in

antimalware for your virtual machine called Microsoft Antimalware. We will explore this offering later in this book.

Identity and access management is always your responsibility. Microsoft only provides you a secure identity platform which assists you in managing and protecting identity. You have full responsibility to protect your accounts used to log in to Azure Management Portal to manage Azure resources. Password must be maintained as well.

With the application level in the IaaS model, Microsoft does not know what you are going to deploy on your virtual machine. You have to plan and conduct security checklist to harden your application.

For the network scope, because Microsoft is providing network infrastructure, Microsoft needs to take care of the network portion, of course, with your virtual network. We will see what are given to help build a secure virtual network on Microsoft Azure later in this book.

The last one is physical infrastructure. Have you had access to this scope as a Microsoft's customer? If you say "Yes" I have no guarantee for your life in the jail. Physical infrastructure are often hardware resources, datacenters and other things which are combined to run and monitor Microsoft Azure cloud platform. You are absolutely unauthorized to touch Microsoft infrastructure.

---

You might have a thought that Microsoft can help for Distributed Denial-of-Service (DDos). Well, Microsoft has its own DDos defense system, but is designed for only network-layer high volume attacks to protect Azure customer tenants. It basically means there is no guarantee from Microsoft to prevent from an attack of smaller volume which you may be the target. Microsoft also has no official information regarding how high the network volume attack is. Hence, preventing DDos is still part of your security responsibility

In addition to defense supportability, Microsoft Azure does not provide mitigation or actively block network traffic to customer deployment at application-layer attack.

---

## Azure Virtual Network

An Azure virtual network is a representation of your own network on Microsoft Azure. Virtual network allows virtual machines and other Azure resources to communicate with each other privately. There are essential

network components such as DHCP, DNS setting, security policy that are manageable. These virtual machines can be in the same virtual network or different virtual network on Microsoft Azure. Microsoft Azure also allows organization to extend their on-premises network infrastructure to Azure virtual network.

Azure Virtual Network offers the following capabilities:

- **Isolation:** Azure Virtual Network allows you to create many virtual private networks. It can be seen in a large organization that needs to separate development, test and production environment.
- **Internet connectivity:** You can remotely connect your virtual machine from the Internet through a given public IP address (PIP).
- **Azure resource connectivity:** all Azure resources in the same virtual network can talk with each other. Even they are not the same, the capability of Azure Virtual Network allows you to set up a gateway connectivity to connect two or more virtual networks together.
- **On-premises Connectivity:** when you want to connect from an Azure virtual network to your on-premises network infrastructure, you can use Azure VPN site-to-site which is fully supported.
- **Traffic filtering:** with Azure Network Security Group you can filter inbound and outbound traffic. We will explore more details about Azure Network Security Group later in this book.
- **Routing:** Azure Virtual Network allows you to create a custom route to control your network traffic. This feature will be discussed later in this book.

There are three common deployment models in Azure Virtual Network:

- Single
- Multi-site
- Hybrid

The first deployment model is used when you have everything hosted on Microsoft Azure and you do not need to communicate with another private network. In this case, you only have one virtual network that all Azure resources reside in.

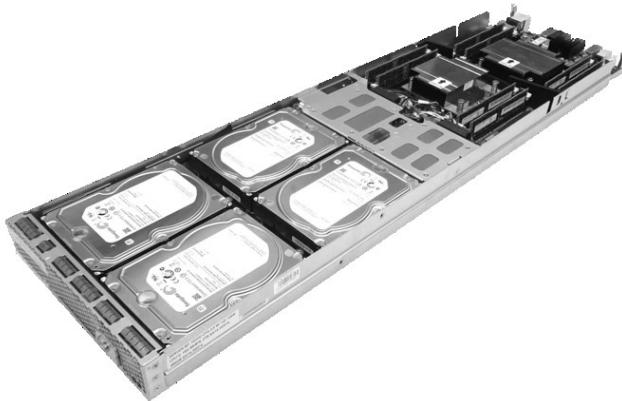
The multi-site model is useful when you need to connect to another virtual network on Microsoft Azure. This would be the case of geographical

deployment in which different offices or sites are connected to a virtual network.

The last one is when you want to connect between your on-premises network and an Azure virtual network. We have seen this case a lot. For example, you deploy a system on Microsoft Azure and want to join it to a corporate identity provider hosted on your on-premises datacenter.

## Azure Virtual Machine

Microsoft Azure is currently generally available in 34 regions around the world. Each region has at least a datacenter, hosting Microsoft Azure platform. The maximum capacity an Azure datacenter can have is approximately 100,000 servers. These servers that run Microsoft Azure platform are custom. They are designed for hyper scale and mostly cable-less design to reduce accidental cable disconnects. Physical servers that host Azure virtual machines are called Open CloudServer V2.



Below is the sample specification of an Open CloudServer system

- 28 CPU cores Intel Xeon E5-2600 v3
- Advanced networking – 40Gbe with ROCE v2
- 8 TB of M.2 PCIe SSDs
- 512GB DRAM
- Accelerator card expansion – GPU, FPGA
- High efficiency 1600W PSU

Previously we discussed briefly about Microsoft Azure IaaS model, giving you more control to design and build your own system with virtual machine you need. As an IT Pro, you should be familiar with the term “virtual machine”. Microsoft does not officially provide any information about the hypervisor technology it is using for Microsoft Azure virtual machine. A rumor is that the hypervisor is similar to Windows Server 2012 Hyper-V and now perhaps Windows Server 2016.

Azure virtual machine is categorized into three things: **Tier**, **Series** and **Size**. There are two tiers: **Basic** and **Standard**. Each tier provides different set of virtual machine sizes serving different purpose. Basic tier is recommended for development, test and application which does not require much memory. While Standard tier provides almost what you need from memory-intensive workload to hyper-scale virtual machine.

There are six series that Microsoft Azure offers: A, D/DS, F/FS, G/GS, NC/NV and H. Each series provides you a specific size including CPU core, Memory, SSD Supportability, Maximum data disk, Maximum IOPS supported. For example, the virtual machine **Standard\_DS2\_v2** provides you 2 CPU core, 7 GiB RAM and allows you add up to four data disks. The maximum IOPS supported is 86.

The list of virtual machine offering can be found as follows:

- For Windows: <https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-sizes>
- For Linux: <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes>

In Microsoft Azure, you cannot say you need X cores with Y GiB of memory. You need to look at the list to pick the size you need, recommended closest match. For example, if you need a virtual machine of 10 GiB RAM, you can choose between a virtual machine supporting 7 GiB or 14 GiB. Pay you attention not only to memory support but also data disk and IOPS.

## Azure Storage

Azure Storage is built with the technology of software-defined storage. Azure Storage can be used to store structured data, unstructured data, event message, backup file, virtual machine disk, video file or so on.

Microsoft offers two types of storage account as follows:

- **Standard storage account:** includes Blob, Table, File and Queue storage
- **Premium storage account:** used for Azure virtual machine disk for on-demand performance.

Note that storage and compute are not the same. You can use Azure storage to store data without any virtual machine.

## Summary

In this chapter, you learned about Microsoft Azure compliance offering list which can be useful when you talk to your customer from the security perspective in the cloud transformation. You also understood the IaaS model and your security responsibility with Microsoft. You explored a little bit to get a view of Azure Virtual Machine, Azure Virtual Network and Azure Storage. The introduction of each offering is not enough to you. You should get more references in the **Additional References** section below. Now you have finished this chapter.

## Additional References

The following additional references you need to read to learn more about Microsoft Azure IaaS service offering:

- Azure Virtual Network: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>
- Introduction to Microsoft Azure Storage: <https://docs.microsoft.com/en-us/azure/storage/storage-introduction>
- Microsoft Cybercrime: <https://www.microsoft.com/en-us/trustcenter/security/cybercrime>

*This page intentionally left blank*

# Chapter 3

# Defend Your Azure

# Network

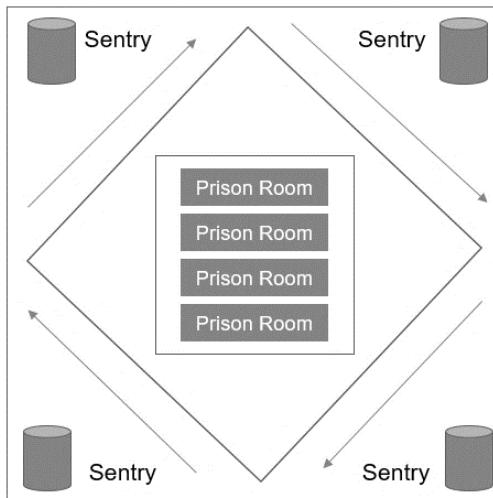
In this chapter, we will learn essential knowledge of defense in depth strategy before we apply it to defend your Azure virtual network.

## Overview of Defense in Depth

Defense in depth is a military defensive strategy to secure a critical position using multiple defensive perimeter. One of the most common things to explain defense in depth is the medieval castle. The king is considered the main target by attackers. In the medieval castle, there are many defensive perimeters. The medieval castle was chosen to be on the hilltop that is always easy to defend. Stone walls and terraces are built around the castle and the hill. Surrounding the hilltop is moat. Rocks are prepared inside the castle to ready to drop from the outer walls to the attack. There are other protective components including warriors to protect the king.



If you are a movie lover of U.S. serial film, you must know *Prison Break* produced by Fox Broadcasting Company. In the movie, we know some of the very popular solid prisons designed with many perimeters to prevent prisoners from escaping. Sentries are positioned in many places to monitor everything coming in and out the prison.



Defense in depth in security is not too different from what we have seen in the two samples above. In a simplest explanation, defense in depth is often referred as a security strategy to implement multiple defensive perimeters. There are two objectives you might not realize:

- **Discourage the attack:** with multi-layer defensive perimeter, you would frustrate the attacker. If the target (e.g. your data) is not worth, the attack would move on. The attacker would see many obstacles to overcome before getting access to his target. It can take a long time and amount of effort he uses. At least we would say this strategy demotivates the attacker.
- **Slow down the attack:** look at medieval castle, to fully overcome the complex architecture to reach to the king, the attacker is supposed to pass every perimeter. For each perimeter, he needs more time for the next one. The defense in depth strategy is to steal more time of an attacker.

Defense in depth, as described, targets to defending in multiple places because an attacker can attack to any single point if possible. With multiple places to be protected, it is practically to resist all possible attack methods. In defense in depth strategy, you need to defend at the minimum perimeters as follows

- Network
- Enclave boundary
- Computing environment
- Identity
- Application

We will explore some defensive solutions for network, computing and identity perimeters later in this book.

## Network Defense

Network is the transmission of packet between your virtual machines and other components to communicate. The OSI (Open Systems Interconnection) would tell exactly why we need to control the network layer. While you cannot do anything with the Physical and Data Link layer in the OSI model, referred to the share responsibility between you and Microsoft, network is the first perimeter to protect. Without network layer, your virtual machine cannot talk to each other. Your application will not be able to receive network packet to identify which protocol and port it needs before further execution. If network is compromised, it is very dangerous to entirely system because at such, attacker can take down your network at a

minimum which would result to business impact we mentioned in **Chapter 1**.

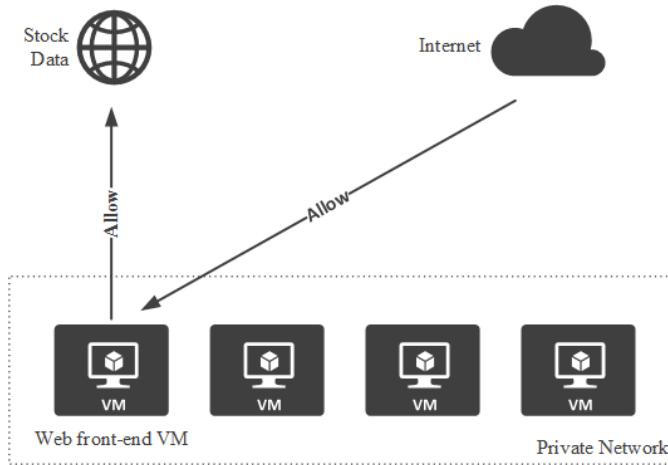
While you cannot do anything with the Physical and Data Link layer in the OSI model, referenced to the shared responsibility, network is the first perimeter to protect from attack.

## DMZ Implementation

When it comes to network defense, demilitarized zone (DMZ) is thought of first. What is so-called demilitarized zone? Is it a very sensitive military zone you should not step into?

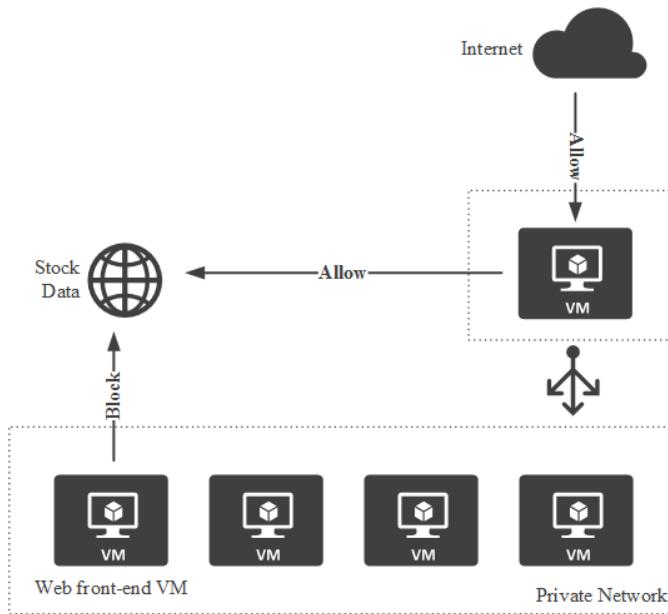
In the field of security, DMZ is a separate zone which is not associated to a private or trusted network. It simply stands alone to isolate from your private network to untrusted network. It is difficult to measure the level of trust. Untrusted network is the one which you have very low trust. Where? The answer is Internet. Why? You do not know exactly who has access to your system because when exposing to the Internet (e.g. internet-facing website), the access is considered anonymously. Internet is not the only untrusted network. DMZ can be used in the case you do not want to expose your private network to any other network.

Let's bring an example in which your web front-end server needs to call to an API to query up-to-date stock data from an internet-facing website. Without defense in depth in mind, the design is straightforward. The web front-end server can directly talk to the Internet to query data and web visitor can send a request directly to the web front-end server.



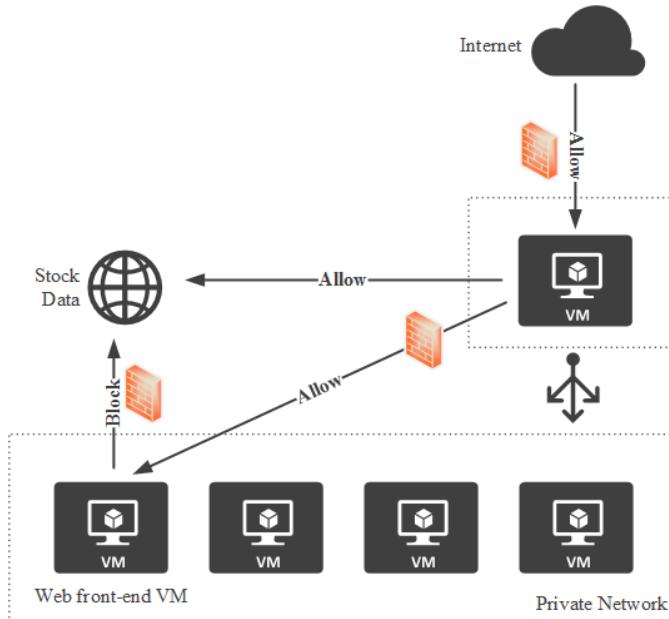
You are not wrong with this design. However, this design has a security breach. An attacker from the Internet has chances to attack to your web front-end server. If he successfully gets in, the other servers would be potentially compromised by his local attack inside the same private network.

When we consider defense in depth, we should not allow private network to directly communicate with the Internet although the web front-end server needs to have Internet-bound traffic to the stock API. A practical approach is to prepare an external network which separates from the private network. In the external network, we place another server whose capability to forward HTTP request or synchronize data to the web front-end server. With this design below, the web front-end server is no longer responsible for querying stock data. Instead, the Internet-facing server is.



Why do we think this design a DMZ practice? Private network should only be private by its name, as always. When considering private, only authorized and monitored access are allowed. If you let your web front-end server go to the Internet, how do you control anonymous access to the server? The internet-facing server in the DMZ design is an extra layer to communicate with the stock API.

The internet-facing server in the above design is often a firewall facing with the Internet. In fundamental security courses, you are taught that DMZ is a network segment between two firewalls. One faces with the Internet and another one faces with the private network.

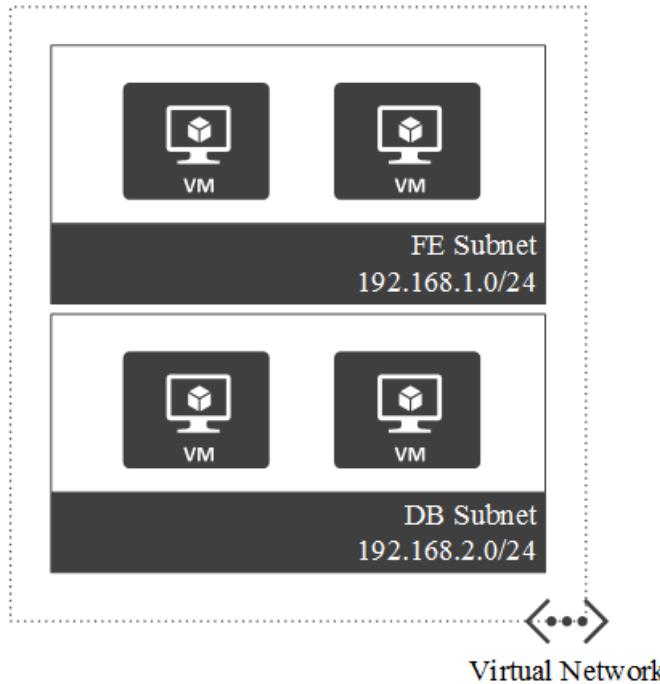


Can Azure Virtual Network provide the ability to build a DMZ architecture? It can absolutely. If not this book would not have happened. We will explore in the book several features to implement a DMZ-like architecture on Microsoft Azure IaaS.

## Network Segmentation

Isolating your private network from untrusted network seems not to be enough in the defense in depth strategy. It is because the isolation is just the external defensive perimeter to anonymous access. Even it is a bad assumption, let's say if the external perimeter is breached and an attacker gets into your web front-end server. From here, he can locally exploit other servers in the same private network. He can get through the database server easier than ever. He also has high chance to control the entirely system in your private network.

Network segmentation is a good practice to mitigate such a threat. It is also an approach to building an internal defensive perimeter. Network segmentation is to segment network into subnet. This approach can help prevent packet sniffing or ARP spoofing technique in your network. Subnet can be based on functional role in your system.



The illustration above shows you an example of network segmentation with two functional roles: front-end and database. In Microsoft Azure, you have to create a virtual network first. The virtual machine will then need to be assigned to this virtual network before the subnet is assigned. There are commonly the following roles you often build on Microsoft Azure:

- Active Directory
- DNS
- Web front-end
- Application
- Database

There may be more depending on what you call. For example, if you are working on SharePoint, you may have Search role, Distributed Cache role or so on.

Creating separate subnet can also help you simplify control network inbound and outbound by using Azure Network Security Group we will explore in the next section.

# Stateful Packet Firewall

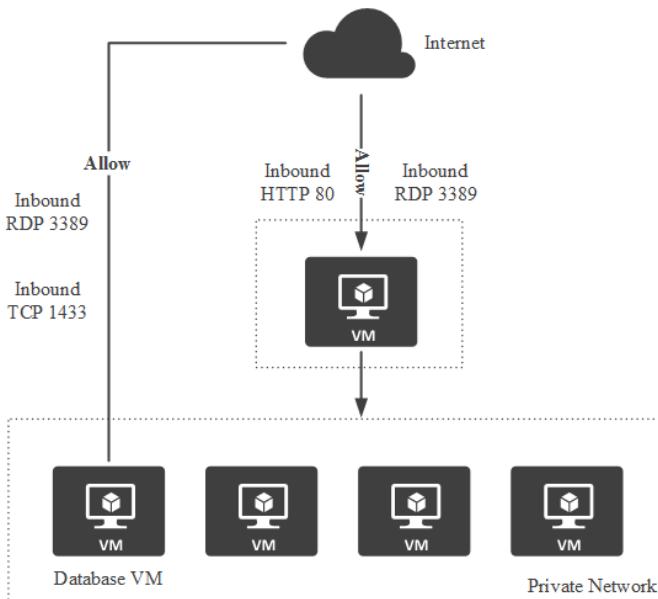
Stateful packet firewall uses the same basic tenets of packet filtering firewall but is more sophisticated. It is working at Layer 4 of the OSI model.

Sometimes it is referred to five-tuple firewall that require five types of information for the execution:

- The source address
- The source port
- The destination address
- The destination port
- The protocol

In Microsoft Azure, Azure Network Security Group works similar to a simple five-tuple stateful packet filtering. Five-tuple firewall might be considered as a backward technology but this is indispensable in implementing DMZ and part of the defense in depth strategy.

The illustration below shows you typical network traffic flow represented by green arrows. From the Internet, inbound network traffic is allowed through port 80. You can also remotely connect to an internet-facing virtual machine using Remote Desktop Connection on port 3389. The problem seen here is the allowed inbound network to the database virtual machine. Do we really need to allow inbound on port 1433 from the Internet? Similar question to the port 3389 is also come out. This design opens the door for attackers to try to listen on both port 1433 and 3389 which are often weak.




---

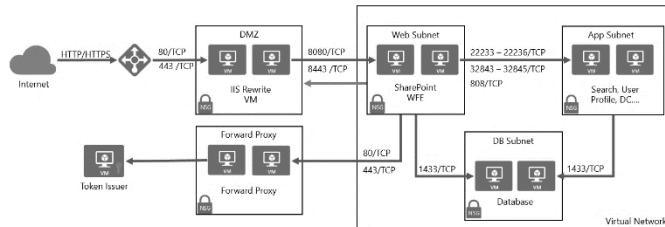
In the Government cloud I worked with, I was not allowed to access to the five-tuple firewall to add rules. Instead, I was asked to provide list of the rules that my system and application used. For example, SQL Server software by default listens on port 1433. Web application commonly uses port 80 or 443 to communicate. Because the Government Cloud applies Deny-All Inbound rule, if we miss any rules in our submission, the application will not work as expected.

---

In Microsoft Azure, you are allowed to create Azure Network Security Group and associate whether to a subnet or a virtual machine's NIC (network interface card).

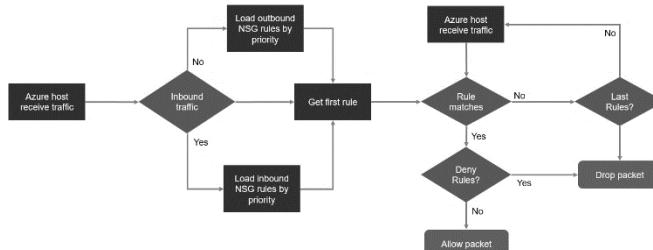
The illustration below shows you the SharePoint reference architecture on Microsoft Azure to simplify your understanding of Azure Network Security. From the Internet, network packet is sent through the load balancer, listening on port 80 (HTTP) and 443 (HTTPS). The Network Security Group of the DMZ subnet allows only port 80 and 443 with TCP. In the DMZ zone, there are two virtual machines running Windows Server 2012 IIS (Internet Information Services) with IIS Rewrite URL module installed to rewrite allowed HTTP/HTTPS request from load balancer to

the actual web front-end virtual machines in the Web Subnet. If the request is Search query for example, then SharePoint web services calls Search service application proxy to trigger to call to the Search service application connection on virtual machines in App Subnet. If there is a database request, network packet is sent to database virtual machine through port 1433 (SQL Server by default) to process the request before returning to the requestor from the Internet.



The illustration also shows the outbound call to the Forward Proxy virtual machines for multi-factor authentication that will be mentioned in the **Government cloud reference** section.

Azure Network Security Group ordering for inbound is different from outbound. For inbound, network packet is evaluated in subnet first before virtual machine's NIC. Unlike inbound, outbound network packet is evaluated in virtual machine's NIC first before subnet. Below is illustration of how rules in Azure Network Security Group is processed.



In Azure Network Security Group, there are two special rules Microsoft recommends you not to block:

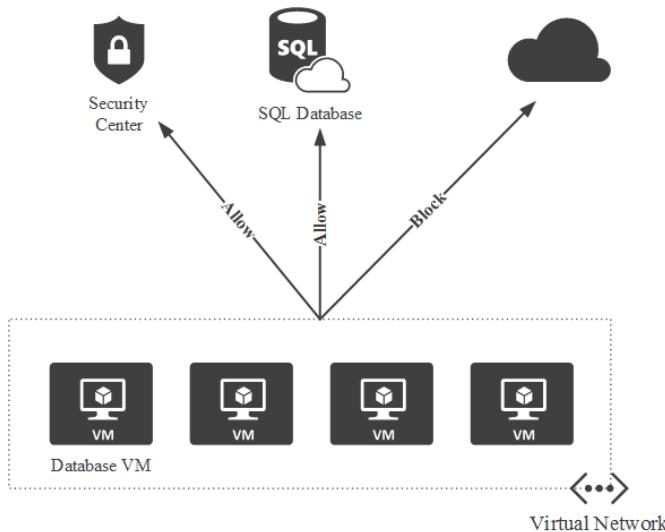
- **Virtual IP of the host node:** The virtualized host IP address 168.63.129.16 must not be blocked because this IP address maps to the physical IP address of the server machine (host node) hosting your virtual machine.

- **Licensing (Key Management Service):** Windows images running on virtual machines must be licensed. The outbound request through port 1688 must not be blocked because it is sent to the Key Management Service host servers to process license activation.

One of the other things to note down is Deny-All Outbound rule. You may need to harden your system by applying this rule. However, be considerate using this rule because this will block your outbound request to public Microsoft Azure services. For example, if your virtual machine is installed Microsoft Antimalware extension, it needs to connect to Microsoft Antimalware system and engine to pull new updates to the virtual machine.

When applying Deny-All Outbound rule, the request to Microsoft Antimalware is blocked. Fortunately, there is a PowerShell script to automatically add all Microsoft Azure public IP addresses. This PowerShell script can be found here

<https://blogs.technet.microsoft.com/keithmayer/2016/01/12/step-by-step-automate-building-outbound-network-security-groups-rules-via-azure-resource-manager-arm-and-powershell/>



If your environment is large, you need to plan carefully and know some limitations and constraints. Azure Network Security Group default limit per subscription is 100. You can request up to 200. The number of rules per

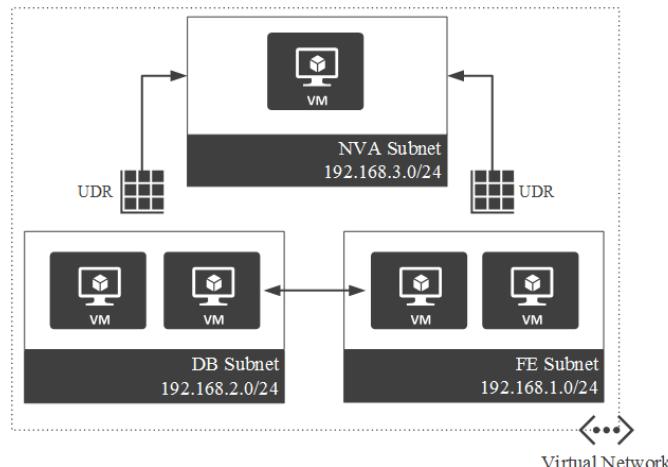
Network Security Group is 200 and can be up to 400. Diagnostic logs are only available for NSGs deployed through the ARM.

If your environment is large, you need to plan carefully and know some limitations and constraints. Azure Network Security Group default limit per subscription is 100. You can request up to 200. The number of rules per Network Security Group is 200 and can be up to 400. Diagnostic logs are only available for NSGs deployed through the ARM.

## Routing to Defense System

Virtual machines in the same virtual network by default can communicate with each other, even they are in different subnets. This can be done by number of system routes used by Microsoft Azure to define how IP traffic flows.

In the security context, you often need to force traffic to a network virtual appliance in which the forced traffic can be filtered, monitor, captured or inspected. In the illustration below, you can see all outbound network traffic from virtual machines in both Front-End Subnet and Back-End Subnet are routed to a Barracuda Next-generation firewall. Another real-world example is to route your outbound network traffic to a DLP (Data Loss Prevention) system for investigation. If outbound packet matching pre-defined sensitive data, the DLP system shall filter and block it.



When creating custom routes, make sure the IP Forwarding is enabled so your traffic can be forwarded to the destination successfully. You can use packet tracert command in Windows to compare before and after you implement User-Defined Routing.

---

Note that limitation of Azure User-Defined Routing is 265 routes per subnet.

---

User-Defined Routing contributes to your DDoS mitigation if configured correctly. That said, if you have a strong next-generation firewall or your own one with machine learning and advanced analytics applied, route all traffics from the Internet to that intelligent firewall for inspection before traffics are forwarded to the destination.

## Network Virtual Appliance

Azure Network Security and User-Defined Routing should not be enough because these features provide basic level of network security. In some cases, you will need higher level that these built-in features cannot meet. For example, you need intrusion detection and prevention (as known as IDPS) or network-based anomaly detection using machine learning algorithm. Instead of implementing your own high-end firewall which is costly, you can pick a virtual network appliance from the Azure Marketplace.

 <b>A10 vThunder ADC for Microsoft Azure</b> By A10 Networks A10 vThunder Application Delivery Controller for Microsoft Azure	 <b>Barasuda NextGen Firewall F-Series</b> By Barasuda Networks, Inc. Next Generation Firewall for Distributed Enterprises	 <b>Check Point vSEC (Image)</b> By Check Point Check Point vSEC for Microsoft Azure delivers a next generation firewall and security gateway.	 <b>Cisco Adaptive Security Appliance virtual (ASAv)</b> By Cisco Systems, Inc. ASAv is the virtualized version of Cisco's best-selling Adaptive Security Appliance (ASA).	 <b>Cisco Cloud Services Router (CSR) 1000V</b> By Cisco Systems, Inc. Deploy and manage enterprise-class networking services and VPN services in the Azure cloud.
Software plans start at \$0.43 per hour  Free software trial	Software plans start at \$0.60 per hour  Free software trial	Software plans start at \$0.95 per hour  Get it now	Get it now	Get it now

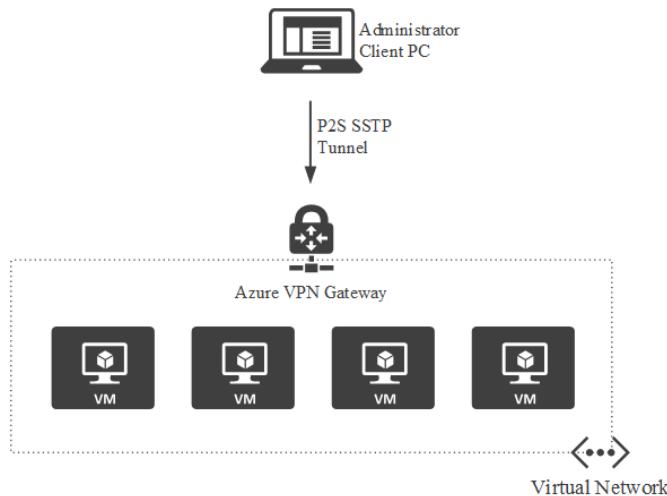
 <b>Citrix XenApp 7.13 Trial</b> By Citrix Deploy a fully functional Citrix XenApp environment in Azure.	 <b>F5 WAF Solution for ASC</b> By F5 Networks F5 web application firewall security for Microsoft Azure-based applications	 <b>FortiGateNGFW High Availability (HA)</b> By Fortinet High Availability Acute Resource Manager Template for Fortigate Next Generation Firewall	 <b>FortiGate Next Generation Firewall - Single VM</b> By Fortinet Single Acute Resource Manager Template for Fortigate Next Generation Firewall	 <b>Fortinet Web Application Firewall - FortiWeb</b> By Fortinet FortiWeb Web Application Firewall delivers multi-layered application threat protection
Get it now	Get it now	Test Drive	Test Drive	Get it now

# Secure remote connection

Normally when managing a virtual machine, an administrator uses Remote Desktop Protocol (for Windows) or SSH (for Linux) to remotely connect. The problem we have seen with these types of protocols is that attackers can use brute-force techniques to try to guess the password. As mentioned in my principle of security awareness, if password does not meet complexity level, it can be easily guessed. And you have heard of millions of pawned passwords, haven't you? To establish a secure remote connection more than just direct remote desktop protocol, you should consider disabling public IP address (if you do not need it), then using one of the following ways:

- Point-to-site VPN
- Site-to-site VPN
- ExpressRoute

Point-to-site VPN and Site-to-site VPN are Azure VPN Gateway options typically for hybrid deployment. Point-to-site VPN requires a client certificate before you can connect to your private virtual network. It is considered a multi-authentication from network layer.



The illustration above shows you the Point-to-site VPN setup to secure the remote from the administration PC to Microsoft Azure hosted system. After the administration keys in his password, he can use RDP to connect to the virtual machines. Twice authentication does strengthen your security.

There can be a jump server which adds an extra hop before you have access to your virtual machines in the virtual network. The administrator must remotely connect to the jump server first. From this jump server, he must remotely connect to virtual machines with RDP.

---

In many cases, people are unaware of securing this jump server. They consider it just a jump server without hardening. Thus, this server is easily compromised. Make sure the jump server is always included in your hardening plan. More on this stuff, read later in the Virtual Machine and Storage Protection section.

---

## ExpressRoute

You may wonder if there is a secure and direct connection from your on-premises datacenter to Microsoft Azure. In many cases, when security and performance are your top priorities, you would consider such a connection. Azure ExpressRoute provides you a private, high-speed and dedicated connection from your facility to Microsoft Azure datacenter. The industrial standard dynamic routing protocol (BGP) is used behind the scenes.

ExpressRoute has three connectivity models:

- CloudExchange Co-location
- Point-to-point Ethernet Connection
- Any-to-any (IPVPN) Connection

The reason why you should consider to choose ExpressRoute is not only because of performance, but the connection does not travel over the public Internet. In other words, there is no public IP address associated with ExpressRoute Gateway.

ExpressRoute is under the agreement between you and Microsoft connectivity partners. It is not available in all Azure regions. The availability depends on Microsoft's target market and service providers.

## Network Availability

Availability is part of the CIA (Confidentiality – Integrity – Availability) triad for decades in the IT security field. CIA triad is kind of knowledge required in industrial security certifications such as CISSP (Certified Information System Security Professional). We also discussed this characteristic in **Chapter 1**. Availability becomes a critical factor in security

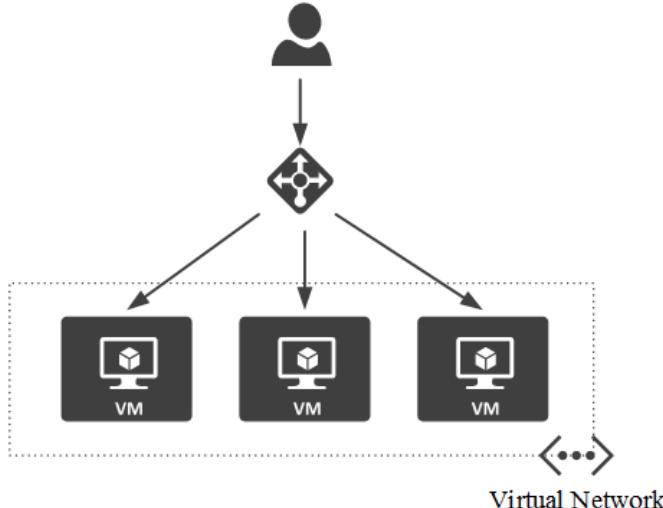
because if your system goes down then you do not know exactly whether it is being accessed by a bad guy. The unavailability would stop monitoring and prevention engine which allows an attacker to have more time to do something. Distributed Denial-Of-Service is the most common types of attack to take down your system.

Implementing fully available system on Microsoft Azure requires the use of many features and an approach we would call Availability-In-Depth to cover every layer we can do to make it as available as possible. These layers may include network, virtual machine, web front-end, application to database layer. Each layer has different mechanism to function, requiring different approach to availability.

In this section, we are not going to discuss fully availability solution in Microsoft Azure. Instead we will focus on availability in network layer, and little bit of Azure Application Gateway which is a web application firewall plus HTTP-based load balancing.

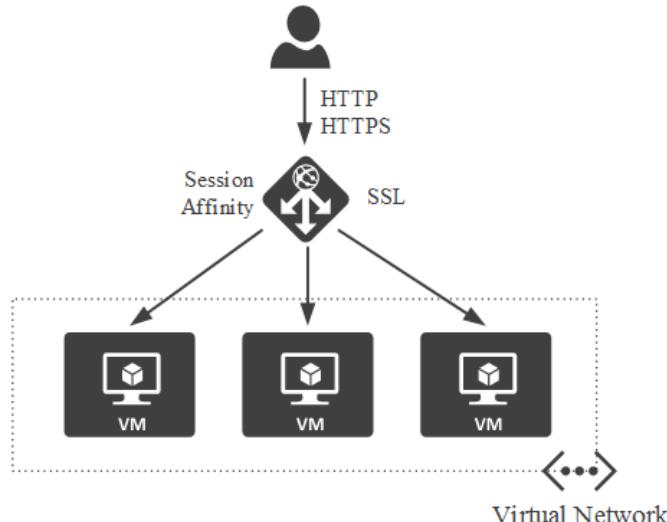
Load balancing is a common solution to distributing network traffic among your virtual machine. Microsoft Azure provides you primarily two type of load balancing services:

- Azure Application Gateway
- Azure Load Balancer



Each load balancer has its own characteristics to perform. Azure Application Gateway is an HTTP-based load balancer which relies on

HTTP protocol to distribute HTTP request to different virtual machine. Azure Application Gateway works on the layer 7 in OSI model. It's not only an HTTP-based load balancer but also a web application firewall that provides the ability to inspect requests based on OWASP (Open Web Application Security Project) core rule set 3.0.



Azure Load Balancer works on network layer in OSI model. It can be set up in two scenarios: Internal and External. External Azure Load Balancer receives incoming request from Internet while Internal Azure Load Balancer works internally among virtual machines in the virtual network. External Azure Load Balancer is often used to distributed traffic from Internet to group of web front-end virtual machines. Internal Load Balancer is recommended mostly with your database virtual machines internally.

## Sample reference

Practice does make perfect in almost case. If you learn something but do not practice you hardly gain practical experience. To apply what we have discussed so far in the Azure Network Security Group, I recommend you to implement multi-server SharePoint farm deployment. If that is your expectation, the deployment will have at least one virtual network and four subnets as follows:

- Active Directory subnet
- Web Front-End subnet
- Application subnet
- Database subnet

Active Directory subnet is where Active Directory domain controller virtual machines are in. Web Front-end subnet includes internet-facing web front-end virtual machines. Application virtual machines running SharePoint services such as Search are in Application subnet. Finally, database virtual machines running SQL Server are in Database subnet.

To make the deployment more practical, you should create a Deny-All Inbound rule and apply to every subnet. After that, try to create individual rules for different network security group to allow inbound network traffic properly. For example, from a network security group associated to the database subnet, inbound TCP on port 1433 from web front-end subnet and application subnet should be allowed.

---

If you want to learn more about ports required for SharePoint Server farm, read here <https://technet.microsoft.com/en-us/library/aa262849.aspx>

---

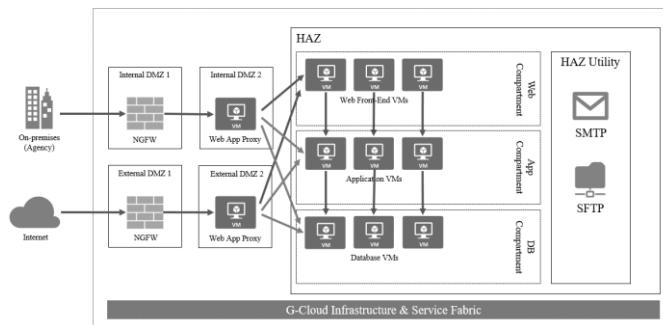
There will be two internal Azure Load Balancers in this practical scenario. One is for SQL Server connection distributed to database virtual machines in the database subnet. Another one for web front-end virtual machines network load balancing.

From the Internet, set up **Azure Application Gateway** then add the internal Azure Load Balancer's IP address to the backend pool. With this, incoming request from the Internet will hit to Azure Application Gateway then the internal Azure load balancer before it is distributed among web front-end virtual machines.

You can add a network virtual appliance and test outbound routing. Let's say if I do not allow outbound through the internal load balancer but the network virtual appliance for better protection.

# Government Cloud Reference

To help you understand more about the network defense, let's see the illustrated architecture below in the Government Cloud. There are two separate connection line to a system hosted inside High Assurance Zone (HAZ): Government agency network and Internet. The request to High Assurance Zone must go through an internet-facing NGFW (as known as next-generation firewall) owned by the Government cloud, before hitting to the web application proxy controlled by the government agency. If the request is qualified by firewall rules, these defense systems will permit network traffic to the system inside High Assurance Zone.



The Government cloud calls “compartment” to distinguish functional server role in the system. There are three basic compartments the Government cloud defines:

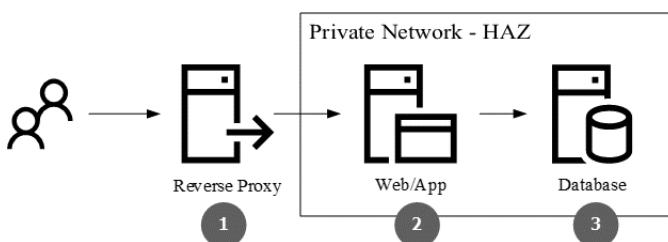
1. Web compartment is the logical network segment of all virtual machines playing as web front-end role.
2. App compartment is the logical network segment of all virtual machines playing as application business processing logic role.
3. Database compartment is the logical network segment of all virtual machines playing as database role.

The compartment design is followed by the Government security policy and compliance. In HAZ Utility zone, there are two services as far as I know: SMTP and SFTP. A government agency must subscribe to any of these services if needed, and specific ports are allowed accordingly.

To explain a little more from the illustration, the network flow is controlled by the five-tuple firewall. The green arrows represent inbound network traffic rule while the red ones represent blocked network traffic. Look again at the illustration, you can see that there is no inbound network traffic from Web App Proxy in external DMZ 2 going directly to the virtual machines in the App compartment network segment. Similarly, inbound network traffic from internal DMZ 2 directly to the App compartment segment is not permitted. At the bottom is the physical host running virtualization technology and some core service fabrics to monitor and orchestrate the entirely Government Cloud.

In the Government cloud, there is also a technical requirement of three-layer architecture I should mention here to clarify more about the network isolation. This requirement is one of the time-consuming challenges to debate to the architect team at the Government cloud.

Three-layer architecture does not mean to the application level. It is not an MVP (Model – View – Presenter) nor MVVC (Model – View – View – Model). It means to the physical level, in which web front-end virtual machine is responsible for receiving incoming request; application virtual machine is responsible for processing the request; and database virtual machine is responsible for processing data before returning to the requestor.

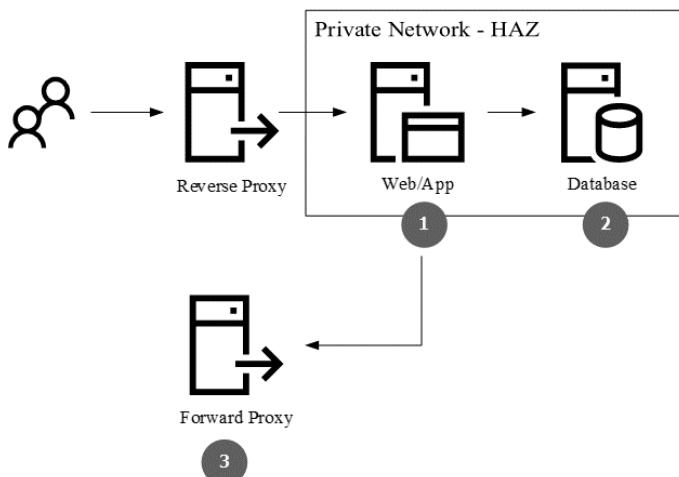


In the first hop, there is commonly a reverse proxy software based running on a virtual machine required by the Government cloud. This reverse proxy interfaces with another firewall to receive forwarded incoming request. The reverse proxy then reverses the request and sends it to the internet web front-end virtual machine on port 80 (HTTP) or 443 (HTTPs) before database virtual machine starts processing data upon the request and get back to the Internet requestor.

This requirement has the following advantages though:

- Easy to audit and troubleshoot on each layer (web, application, database).
- Easy to scale out to meet the demand.
- Meet the Government cloud compliance in particular, and the national security policy in general.

The three-layer architecture requirement does not only apply to inbound request but outbound. Due to security matter, system hosted in High Assurance Zone is not allowed to communicate back to the Internet. For example, your application needs to call an API from PKI (Public Key Infrastructure) server from a third-party vendor for multi-factor authentication. By default, Internet outbound rule is not permitted. The Government cloud provides a service called Forward Proxy, still followed by three-layer architecture to enable Internet outbound. The Forward Proxy acts as an intermediary for requests from High Assurance Zone seeking resources from the Internet.

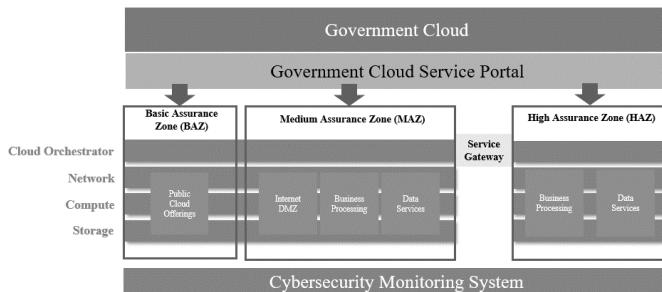


From the illustration, realize that you cannot configure to forward your outbound traffic from High Assurance Zone throughout the reverse proxy. This is not allowed. The outbound traffic from High Assurance Zone will be forwarded by the Government Cloud's Forward Proxy.

The Government cloud already defined compartment segment for your system as you can see in the reference architecture. When you submit your

system architecture for review, you have to indicate which virtual machines are placed in which compartment. The compartment is part of defense in depth strategy to isolate network subnet we discussed earlier. Ports and protocols between compartments must be defined specifically so the Government cloud team can review to approve or reject. This requirement also indicates that the Government cloud applies Deny-All Inbound rule. The Government cloud only configures its firewall to allow what to be submitted and approved.

By its name, the Government cloud a private cloud that was implemented in 2013 for Whole-of-Government (WOG) strategy for the country where security and governance requirements cannot be met by public cloud. The Government cloud offers compute, network and other infrastructure resources like any IaaS cloud provider.



The Government cloud architecture comprises of three mutually segregated zones catering to different levels of security assurance namely: Basic Assurance Zone (BAZ), Medium Assurance Zone (MAZ) and High Assurance Zone (HAZ).

- **Basic Assurance Zone (BAZ)** – provide an infrastructure resource pool which is shared with public cloud users, and does not have any connectivity to private government network.
- **Medium Assurance Zone (MAZ)** – provide an infrastructure resource pool which is shared with non-government cloud users. This zone consists of three hosting service compartment, namely:
  - Internet DMZ – provides compute resources for web services for public users to access to application from the Internet.

- Business – provides compute resources for application business processing logic services e.g. web and application service.
- Data – provides compute resources for database services.
- **High Assurance Zone (HAZ)** – provide a dedicated infrastructure resource pool which is used by the government staffs only, and is directly connected to the private government network via a wide area network (WAN) network. There are only two hosting service compartments, namely:
  - Business Processing – provides compute resources for application business processing logic services.
  - Data – provides compute resources for database services.

System hosted in High Assurance Zone is physically segregated from the Basic Assurance Zone and Medium Assurance Zone, and does not have any connectivity to the Internet.

On-boarding process involves the following parties to execute from end to end until your deployment is successfully on the Government cloud.

- **Tenant Facility Management team:** this team is responsible for anything related to infrastructure technically, from configuring network topology, setting up storage to supporting you all hardware related issues.
- **Provisioning team:** this team is responsible for virtual machine provisioning, installing operating system software, running automatic vulnerability assessment and load testing tool.
- **Customer Service & Service Request team:** this team is responsible for any service you may request, including new subscription service to two-factor token request.
- **Adoption team:** this team is responsible for the Government cloud adoption, including presales presentation, enrollment support and documentation.
- **Government Agency team:** this is the government agency who wish to host its system on the Government cloud.
- **Government Technology Organization:** this team is responsible for the technical architecture review, firewall justification and approval.

Vendors that are engaged to providing professional services to a government agency are commonly not allowed to be involved in any stage of the on-boarding process. Every request and form submission must be submitted by that government agency generally.

## Summary

In this chapter, you were introduced fundamental knowledge of defense in depth strategy in security by mediaeval castle and Prison Break serial movie. You learnt number of different approaches to defending your Azure virtual network. That includes the use of Azure Network Security, User-Defined Routing, Network Virtual Appliance, Azure Load Balancer and Azure VPN Gateway. You also explored some general information and sample reference of the Government cloud I mentioned. Now you have finished this chapter.

## Additional references

Below is the list of helpful additional references for you:

- Designing a defense-in-depth network security model:  
<http://searchsecurity.techtarget.com/feature/Designing-a-defense-in-depth-network-security-model>
- The Principles of Network Security Design:  
[http://www.clivu.pl/services/Principles\\_Network\\_Security\\_Design.pdf](http://www.clivu.pl/services/Principles_Network_Security_Design.pdf)
- Planning and design for VPN Gateway: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-plan-design>
- ExpressRoute Introduction: <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

*This page intentionally left blank*

# Chapter 4

# Protect your Virtual Machine

Virtual machine is the common target of attacks. Defending the hypervisor host is necessary but this is out of your scope as a cloud consumer. Virtual machine is part of computing environment which we need to protect. This is also your own responsibility we discussed in *Chapter 2, Microsoft Azure IaaS Security Shared Responsibility* section. In the previous chapter, we explored some approaches to defending Azure virtual network. In this chapter, we are going to explore several given solutions to protecting Azure virtual machine and storage.

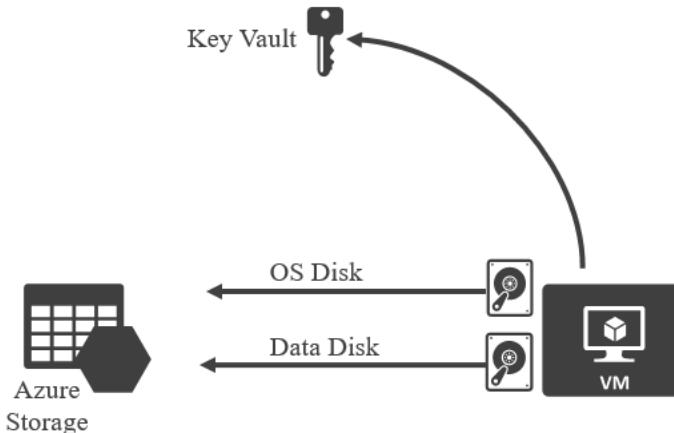
## Disk Encryption

We discussed at the beginning that the ultimate objective of security was to protect our data from any authorized access. Confidentiality should emphasize similarly. Controlling access to virtual machine and data sometimes does not work. Through a local attack, an attacker might have your disk where data is stored. In this situation, adding an extra protection layer by encrypting your disk is always a recommended best practice.

Azure Disk Encryption allows you to encrypt disk in virtual machine. During the encryption, disk-encryption key is stored in Azure Key Vault which is required for decryption. To successfully gain data inside your disk, an attacker must have not only data disk but also secret key to decrypt. Without the key, the attacker cannot mount the disk into his hypervisor

host for further analysis. Your virtual machines are encrypted at east in the storage account.

Azure Disk Encryption leverages BitLocker encryption technology on Windows and DM-Crypt on Linux.



We will explore steps to encrypt a virtual machine in *Appendix, Hands-On Lab.*

## Antimalware for Virtual Machine

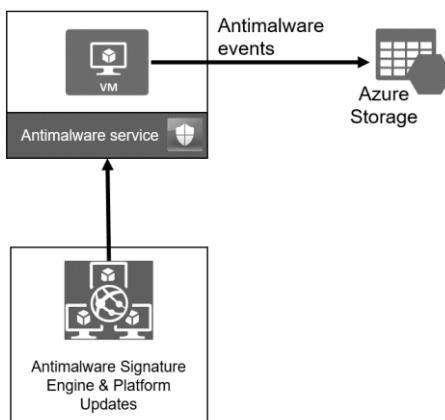
The world of virus and malware are unpredictable. There are many historically stories about the virus for example Conflicker or Nimda which damaged hugely to hijacked network. Some of the actions such a malware does is:

- Slow down your virtual machine
- Stop some critical services on your virtual machine
- Automatically attack other virtual machines in the same network
- Be a backdoor sending message and sensitive information to attacker

Such a malware can be very dangerous when infecting to your virtual machine. I used to involve in a disaster recovery for a big security incident in which a malware encrypted database of a SharePoint system. The root cause could come from a poisoned computer which did not install antimalware. Such a case is not new to the world, having happened everywhere.

Planning and deploying antimalware solution is always a good practice in security, especially in defense in depth strategy. Microsoft Azure provides you free real-time protection capability through something they call virtual machine extension to identify virus, spyware and malicious software like so-called antivirus software in your personal computer. Microsoft Azure antimalware offers the following features:

- Real-time protection
- Scheduled scanning
- Malware remediation
- Signature updates
- Antimalware Engine updates
- Antimalware Platform updates
- Active protection
- Samples reporting
- Exclusions
- Antimalware event collection



Antimalware service is running on your virtual machine, responsible for collecting signature and data from Microsoft Antimalware Engine. You can create a new storage account to store antimalware events.

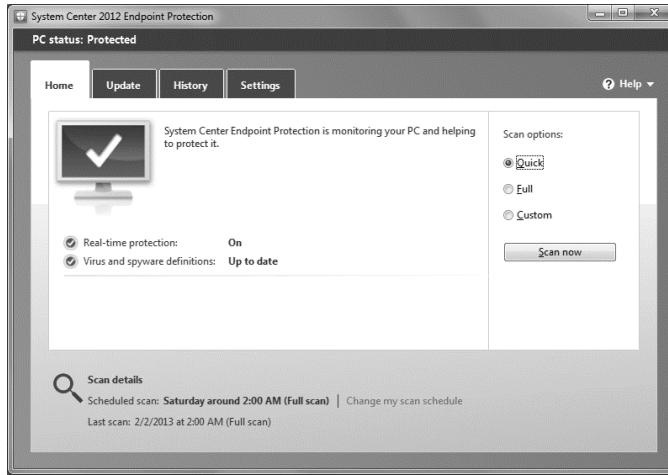
---

Note that if you apply Deny-All Outbound rule using Network Security Group, make sure to add a new “Allow” Outbound rule so your virtual machine can connect to Microsoft Antimalware engine.

---

When you install Microsoft antimalware extension, you are to install a client software on your virtual machine. The software looks like System

Center 2012 Endpoint Protection if running on Windows Server 2008 R2, 2012 and 2012 R2.



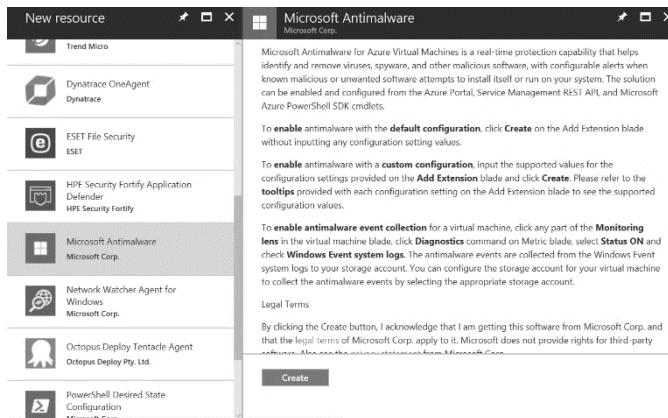
---

In Windows Server 2016, it's called Windows Defender.

---

You can enable Microsoft Antimalware extension for your virtual machine by the following ways:

1. Azure Portal
2. Visual Studio Virtual Machine configuration
3. PowerShell
4. Azure Security Center



Microsoft Antimalware extension is not the only option. You can go with third-party antivirus for enterprise such as Symantec, Trend Micro, Intel MacAfee to protect your virtual machine. These third-party products

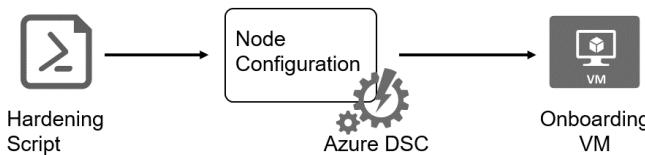
are not available in Azure virtual machine extensions. You must go to install individually.

The Government cloud I worked with preferred Symantec Endpoint Protection. It should be worth your time taking a look.

## Hardened Virtual Machine Deployment

During my time working with the Government Cloud, I recognized that every on-boarding virtual machine after successfully provisioned needed to apply a script called hardening. Digging into this script, I realized that it contained many security configuration policies. When running this script, Windows will automatically configure Local Security Policy and built-in advanced firewall (for Windows Server). This practice is part of security by default, and can be found in information security policy in large organizations, especially governmental environment. While it is to make sure new on-boarding machine will have intended configuration you need, and all machines will have the same hardening template.

In Microsoft Azure, you can automate provisioning your virtual machines while applying a custom script inside to configure security policies by using Azure Automation Desired State Configuration. It allows you to build a custom script, and trigger it in your virtual machine. The script may contain local security policy setting, firewall rule, antivirus deployment or other settings which may help protect your virtual machine. Azure Automation Desired State Configuration is built on top of PowerShell Desired State Configuration.



There are many hardening guidelines but I would highly recommend you to take Security Technical Implementation Guide conducted by USA Department of Defense (DoD) <http://iase.disa.mil/stigs/Pages/index.aspx>.

You can use custom script extension to automate triggering script in your virtual machine. However Azure Desired State Configuration is

still recommended for manageable centralized configuration and deployment.

---

## Virtual Machine Availability

Hosting your system on a cloud service provider does not mean your virtual machine is always available. The Service Level Availability may not be true today. That's why Microsoft states for its cloud platform that there are two type of events that can affect your virtual machine's availability:

- **Planned maintenance event:** it's like any maintenance plan you may have experience. In this type of event, Microsoft install updates, security, patch periodically into the physical host. There are some updates that require reboot of your virtual machine.
- **Unplanned maintenance event:** unlike planned maintenance event, unplanned one is when the physical hardware is broken in some ways. In such a failure, your virtual machine is automatically migrated to another physical hardware which affect your virtual machine during the migration.

To assist customer in the virtual machine's availability, Microsoft Azure provides a feature called Availability Set. By its name, an availability set often consists of at least two virtual machines. Microsoft has committed that if you put two virtual machines in an availability set, one of them is available and meets the 99.95% Azure SLA.

When working with Availability Set, you need to assign your virtual machine to one of these things: **Update domain** and **Fault domain**. Update domain is for planned downtime while fault domain is for unplanned downtime. The illustration below shows you four availability sets for each functioning virtual machine role. Each availability set must have minimum two virtual machines to achieve redundancy.

Do plan for your virtual machine's availability because it is part of CIA triad which is often used as keys to security.

## Summary

In this chapter, you were introduced several solutions to secure your virtual machines, from storage encryption to disk encryption. We also explored Microsoft Antimalware extension for your virtual machines. One of the

interesting things you discovered was Azure Automation DSC which allows you to apply a hardening configuration template to every virtual machine. Finally, availability set allows you to maintain availability of your virtual machines.

## Additional References

Here are some additional references that might be helpful:

- Microsoft Antimalware for Azure Cloud Services and Virtual Machines: [\*https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware\*](https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware)
- Manage the availability of Windows virtual machines in Azure: [\*https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability\*](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability)
- Getting started with Azure Automation DSC: [\*https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started\*](https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started)

*This page intentionally left blank*

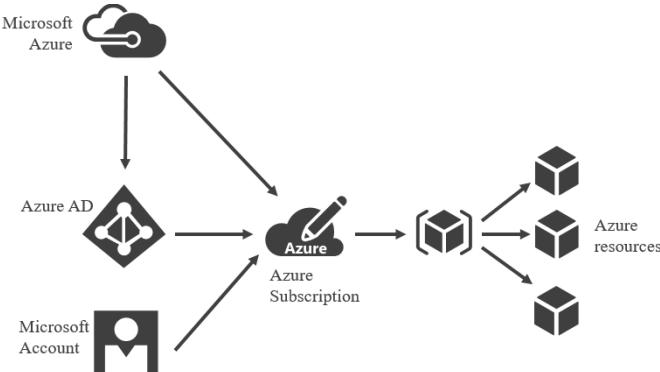
# Chapter 5

# Manage your identity

Many of the security incidents I have seen are related to identity. Identity is often referred to the account you use. It can be the one you use to log into your virtual machine. This can be the account to manage a system. It can be a service account. Whatever it is, if such an account's password is pawned to a bad guy, you will run into a security problem. This chapter primarily focuses on protecting your accounts used to log into Azure Management Portal and to manage Azure resources (e.g. virtual machine, network...).

## Understanding Azure Identity Access

Before you can better protect your identity, you need to understand fundamental Azure hierarchy. There are two types of account that you can use to log into Azure Management Portal to manage your Azure subscription. One is Microsoft Account (formerly known as Microsoft Live ID). One is Work and School account which is authentication via Azure Active Directory.



One Azure Active Directory account links to one Microsoft Azure subscription. You can have multiple subscriptions linked to one account. You can create and manage resource groups a subscription. Inside resource group are Azure resources (e.g. virtual machine, virtual network...). One resource can only be linked to one resource group. Each resource is accessible to an identity. In the next section, we will explore more Azure role-based access control.

## Role-based access control

In the industrial security, you may have only heard about Access Control practice to define privileges to your team, giving them access to a virtual machine for example. This can be enough in a small environment. However, if you manage many teams working on Microsoft Azure, giving them access to every Azure service is not what you expect. The idea is if you have a web application development team, you should be able to give the team access to only services in Azure App Service. While your system administrator team is given access to Azure virtual machine, virtual network or things related to infrastructure.

NAME	USERS	GROUPS
Owner	1	1
Contributor	0	0
Reader	0	0
API Management Service Contributor	0	0
API Management Service Operator Role	0	0
API Management Service Reader Role	0	0
Application Insights Component Contributor	0	0
Application Insights Snapshot Debugger	0	0
Automation Job Operator	0	0
Automation Operator	0	0

To help you control access to Azure resources, Microsoft Azure allows you to grant specific permission to user or group to perform their tasks. These tasks can be provisioning Azure virtual machines, creating virtual network or modifying your storages. Such a feature is called Role-based Access Control.

NAME	TYPE	ROLE	SCOPE
Subscription ad	Group	Owner	Inherited (Subscription)
thuusmg.1506	User	Owner	Inherited (Subscription)

Microsoft Azure provides approximately 40 built-in roles spanning across Azure services. The list can be found at <https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles>

As an Azure administrator, you can easily revoke unintended privileges by simply removing a user from a group in a specific Azure service or resource.

Role-based access control is useful feature in large and dynamic environment with periodical changes. Below can be a reference plan for your role-based access control in Microsoft Azure:

Group	Description	Azure Service	Role
Web Development	Group of people working on web development	Azure App Services	Web Plan Contributor Website Contribute
System Engineering	Group of system administrator	Azure Virtual Machine	Virtual Machine Contributor

If none of the built-in roles meet your requirement, you can create custom role using the following options:

- Azure PowerShell
- Azure Command-Line Interface (CLI)
- REST API

Custom roles can be assigned to users, groups, resource group and Azure resource level. It can be shared among Azure subscriptions that use the same Azure Active Directory.

## Multi-factor Authentication

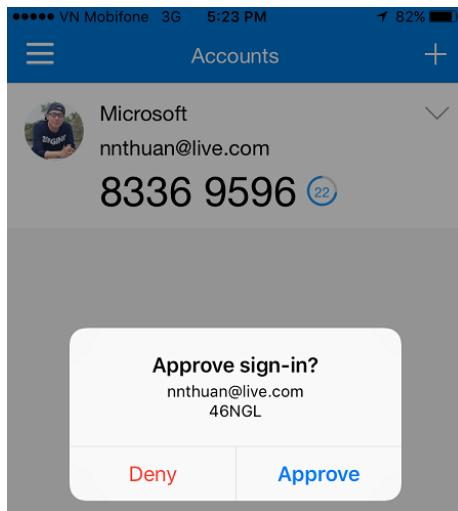
Multi-factor authentication means by its name, giving one more step of authentication to protect your account. The authentication step can be a time-based one-time password sent from a cloud authentication provider such as Google Authenticator, Microsoft Authenticator. The authentication step can also be a one-time code generated from an immediate authentication server sent to your email or your mobile phone in form of SMS message. Sometimes you can

see it in form of biology i.e. fingerprint. Whatever it is, after you enter your username and password in such a traditional way, you still need another step to completely get authenticated before having access to your resources. Multi-factor authentication is commonly required in security policy in medium to large organizations, including governmental environment.

There are basically two types of account Microsoft allows you to use to log into Azure Management portal.

- Work and School account
- Microsoft Account

If you have a doubt, just go to log-in page then click **Can't access your account?** you will see what Microsoft asks you. Work and School account is considered corporate account stored somewhere in your on-premises environment or Microsoft cloud identity service (Azure Active Directory). This type is commonly in form of email address (but it is actually the User Principal Name format) such as thuan@contoso.com. While Microsoft Account is previously called Windows Live ID. But now Microsoft combines several things into a centralized system including Outlook.com, OneDrive, Skype, Xbox Live, Bing or so on. Windows Live ID is no longer called by its name but people still prefer calling it. The new name is Microsoft account which many people are confused, misunderstanding that it's used for internal Microsoft employees.



With Microsoft account, there is no way as of this book to force to use multi-factor authentication during login time to Azure Management portal. However, if your account is created and managed by Azure AD you can create an enforcement policy to force people in your organization to set up multi-factor authentication before they can log into Azure. This is recommended if you are managing an Azure team, which are granted to work on your Azure subscription.



jackie@nnthuanlive.onmicrosoft.com

Your admin has required that you set up this account for additional security verification.

[Set it up now](#)

[Sign out and sign in with a different account](#)

[More information](#)

To know on how to enable multi-factor authentication for your account used to log into Azure Management Portal, refer to **Lab 4.2** in this book.

## Brute-force attack mitigation

Brute-force attack is simply to continuously attempt to discover your password by combining all possible passwords it can guess. That said, human can guess a password by trying to brainstorm all possibilities such as birthday, girlfriend name, a memorable location or even a combination of birthday and full name. The problem is that our brain cannot come up with a million of guesses and type the guessed password into the login form. Unless you are so-called a time-billionaire. With a tool, it can guess and automatically fill into the login form. Whenever it receives a message like "**Successful login**" it will stop the guessing process.

---

This section is not going to purposely show you how to perform a brute-force attack. You can find many sample scripts and tools over the Internet.

---

Attackers often choose brute-force technique because it's exploited against security unawareness of human. People tend to pick a simple password (sometimes I did too in order to quickly get into a system) that can be easily guessed. A few common ones include "*12345678*", "*pass@word1*", "*iloveyou*". They even keep the password by default that we see almost from setting up a new router. They don't mind to change to different password.

While setting up a simple password is a bad behavior, this results to huge security incident which damages to your business. Imagine your salesman's password is compromised to a bad guy, he can access to download all financial and sales report which can be sold to different competitor. Or simple password set by an administrator can allows attacker to perform an attack to try to RDP to virtual machine. Recently a colleague of mine used a simple password to work on Amazon AWS virtual machine via SSH. The attacker managed to grab the password after his brute-force attempt. As a result, he successfully logged into the virtual machine and uploaded the bash shell for further exploitation.

## Secure RDP

Normally when managing a virtual machine, an administrator uses Remote Desktop Connection (for Windows) or SSH (for Linux) to directly remotely connect. The problem we have seen with these types of protocols is that attackers can use brute-force techniques to try to guess the password. As mentioned in my principle of security awareness, if password does not meet complexity, it can be easily guessed.

We ideally need one more hop because an administrator can RDP to his virtual machine. In Microsoft Azure, you can set up VPN (Virtual Private Network) to add an extra authentication hop before connecting to the virtual machine. There are three options:

- Point-to-site VPN
- Site-to-site VPN
- ExpressRoutes

---

Refer to Chapter 3, “Secure remote connection” and “ExpressRoute” section for more information of RDP protection.

---

## DMZ Implementation

DMZ can be an approach to securing your virtual machine. If you do not expose your virtual machine to the Internet, attackers cannot perform a brute-force attack against the RDP. He has to perform escalation technique to try to exploit the external network first. This is how we call the discouragement of attack in defense in depth.

You should combine with Azure Network Security to not allow inbound network traffic on port 3389 from the Internet.

## Password Complexity

Brute-force attack targets to simple password. Hence, if password complexity is applied we are going to have more good feeling on this stuff. We can enable password complexity and force people to use it. The following table provided by Microsoft shows you the password complexity requirements for accounts stored in Azure Active Directory:

Property	Requirements
----------	--------------

Characters allowed	<ul style="list-style-type: none"> <li>• A – Z</li> <li>• a - z</li> <li>• 0 – 9</li> <li>• @ # \$ % ^ &amp; * - _ ! + = [ ] { }   \ : ' , . ? / ` ~ “ ( ) ;</li> </ul>
Characters not allowed	<ul style="list-style-type: none"> <li>• Unicode characters</li> <li>• Spaces</li> <li>• <b>Strong passwords only:</b> Cannot contain a dot character '.' immediately preceding the '@' symbol</li> </ul>
Password restrictions	<ul style="list-style-type: none"> <li>• 8 characters minimum and 16 characters maximum</li> <li>• <b>Strong passwords only:</b> Requires 3 out of 4 of the following: <ul style="list-style-type: none"> <li>○ Lowercase characters</li> <li>○ Uppercase characters</li> <li>○ Numbers (0-9)</li> <li>○ Symbols (see password restrictions above)</li> </ul> </li> </ul>
Account Lockout	<ul style="list-style-type: none"> <li>• After 10 unsuccessful sign-in attempts (wrong password), the user will be locked out for one minute. Further incorrect sign-in attempts will lock out the user for increasing duration.</li> </ul>

## Azure Active Directory Lockout Policy

Lockout policy is considered one of acceptable practices to mitigate brute-force attack. Unfortunately, right now the default value of attempt is 10 and you cannot modify it. Further incorrect sign-in attempts after 10 times will lock out the user for increasing duration.

The trade-off in this approach is that if the attacker knows the lockout policy, he can make a denial-of-service on lockout service for group of accounts. In this case, targeted accounts are locked. The unavailability is also considered part of a successful attack. In the SharePoint case, for example, if the service account is known, the attacker can take down the entire SharePoint farm by just trying as enough attempts as the lockout policy is applied. OWASP already listed out the disadvantages of lockout approach here ([https://www.owasp.org/index.php/Blocking\\_Brute\\_Force\\_Attacks](https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks))

## **Enable Multi-Authentication**

Another approach is to enable multi-factor authentication to mitigate brute-force attack. Even when password is successfully guessed, the attack cannot get into the system without being successfully authenticated at the second authentication

Consider that business users really hate security policy. They seem not to worry about security breach loss. But if you ask them to be authenticated one more time, they would blame you. They are not comfortable when having to enter passwords many times. We all know that so consider that multi-factor authentication enforcement can potentially affect user experience. But if the loss is huge then there is no reason not to enforce.

## **Identity Monitoring**

Monitoring your identity is to detect and have a prevention action timely. Azure Identity Protection provides number of different capabilities for identity thief detection. Refer to *Chapter 6, Monitoring your Azure resources* section.

## **Conditional Access Policy**

Conditional access policy in Azure Active Directory Premium allows you to control access based on policy. Although this is not related to brute-force attack, it can be a good choice to monitoring your identity and forcing corporate identities to be authenticated by your own policies. Attacker without knowing policies cannot make a successful attack.

There are four conditions:

- Device
- Sign-in

- Location
- Client App

Each condition provides a scope to apply. For example, with device policy you can choose to set the login from a specific device platform such as iOS, Android. Or from a location you can set a trusted IP addresses. This does help to block attacker's IP address when he tries to discover and log into from his location.

---

Azure Security Center can help detect brute-force attack with its Detection capability. However, as of this writing the Detection capability has not been shifted to Azure Active Directory. You can still benefit from the RDP Brute-force detection for your Azure virtual machine.

---

Brute-force attack is not new, but this is a common used technique because human mistake happens all the time.

---

## Summary

In this chapter, you were introduced the importance of protecting your identity when working on Azure. You also explored how Azure can help to secure an identity. The chapter also provided number of different ways to prevent brute-force attack against your identity.

## Additional References

Here are some additional references that might be helpful:

- Get started with Role-Based Access Control in the Azure portal  
<https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-what-is>
- Create custom roles for Azure Role-Based Access Control  
<https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-custom-roles>
- Conditional access in Azure Active Directory  
<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access>



*This page intentionally left blank*

# Chapter 6

# Monitoring your Azure

# resource

Security threat is very hard to detect and defend today. In *Chapter 1, Challenge in Cybersecurity today* section, we realized security challenges which require complex algorithm in machine learning for monitoring module to timely detect anomaly and suspicious activities. Monitoring is very crucial because it enables system administrators and security professional to monitor, track and identify security threat as soon as security breach happens on your system. In this chapter, we will explore some monitoring tools on Microsoft Azure.

## Azure Security Center

Microsoft Azure Security Center can be the monitoring central to protecting your Azure resources. Azure Security Center is built on the methodology called **Prevention – Detection – Response**.

Azure Security applies machine learning, behavioral analysis and advanced analytics to build many complicated defense patterns to detect anomaly access, suspicious attack or so on. With detection capabilities, Azure Security Center connects to the Microsoft threat intelligence center to perform security analysis to look up if any suspicious activity. When it comes to anomaly detection, there are advanced analytics and machine learning techniques to learn from you (e.g. normal time of login, login

location...) before building historical data. You would understand this in *Chapter 1, Challenge in cybersecurity today* section from credit card fraudulence detection sample.

Azure Security Center runs number of services under the Azure platform to audit Azure resources. If any resource is vulnerable based on Microsoft security baseline, it will provide security recommendations to remediate potential vulnerabilities. The security baseline uses Common Configuration Enumeration to assign unique identifiers for configuration rules.

NAME	MONITORED	SYSTEM UPDATES	ENDPOINT PROTE...	VULNERABILITIES	DISK ENCRYPTION
AppVM01	▲	●	●	●	●
AppVM02	▲	●	●	●	●
DNS01	▲	●	●	●	●
IIS01	▲	●	●	●	●
advVM	✓	●	●	●	●
sqlVM	✓	●	●	●	●
app-vm	✓	●	●	▲	●
db-vm	✓	●	●	▲	●

One of the interesting features is the recommendation that allows you apply. For example, when Azure Security recognizes your virtual machine has not used Disk encryption, it recommends you to take a look and apply the feature. Another example is Microsoft antimalware extension. If your virtual machine has not installed the extension yet, from Azure Security Center you can apply.

There are two tiers in Azure Security Center: **Free** and **Standard**. Each tier offers different range of features. Free tier provides you basic security policy, assessment and partner solution. While Standard tier adds threat detection capabilities on four resource types: Network, Virtual Machine, SQL Databases and Windows crashes. Standard tier also allows you to collect data on supported resources. Maximum allowed daily data collection is 500 MB per day.

## Azure Advisor

Azure Advisor is another service that Microsoft bring to assist cloud consumer to optimize Azure deployment. Azure Advisor focuses on four criteria:

- **High Availability:** provide recommendations for your Azure resources including availability set for your virtual machine, premium storage to keep things more reliable. As of this book, it only recommends for virtual machine and storage. Network availability is not being advised.
- **Security:** Azure Advisor integrates with Azure Security Center to help prevent, detect and respond to security vulnerability. Review *Chapter 6, Azure Security Center* section for more information.
- **Performance:** provide recommendations for Azure SQL Database, Redis Cache and App Service performance.
- **Cost:** provide recommendations to optimize your cost by looking at your Azure resources usage.

Impact	Description	Resource	Updated At
High	Improve the security of your Azure resources Follow Security Center recommendations	7 Recommendations	5/3/2017 10:55:19 AM
Medium	This virtual machine is not configured for fault tolerance For virtual machine redundancy, use availability sets	1 Virtual machine	5/3/2017 9:17:05 AM
Medium	Your virtual machine is not configured for backup For protection against accidental data deletion and corruption, enable virtual machine backup	1 Virtual machine	5/3/2017 10:55:19 AM

High availability and security criteria in Azure Advisor can be beneficial to your security plan. Related to Azure IaaS, Azure Advisor provides recommendation for virtual machines, availability sets, application gateway and SQL Server (if your application uses it).

## Azure Monitor

Azure Monitor is a basic monitoring tool that captures activity log on your Azure virtual machine. It also allows you to set metrics to monitor. For example, you want to monitor percentage CPU on a virtual machine. For virtual machine specifically, Azure Monitor supports the following metrics:

- Percentage CPU
- Network In
- Network Out
- Disk Read Bytes

- Disk Write Bytes
- Disk Read Operations/Sec
- Disk Write Operations/Sec

Activity log on your storage account can be captured by Azure Monitor. However, there is no metric for storage account level. However, you can set metric for Blob where your virtual machine disk is stored in.

Metrics in Azure Monitor can be helpful to trace if a virtual machine is slow. Moreover, you can set an alert based on pre-defined metric via SMS, email or even web hook to automate trigger next step if you like to automate infrastructure management and maintenance.

## Azure Log Analytics

Azure Log Analytics is a service in Operations Management Suite (OMS) providing you the capability to monitor your Azure resources. It can monitor on-premises but we are not going to explore the on-premises capability. Azure Log Analytics gives you an insight of operational data in your Azure environment, mostly focused on Azure virtual machine. Moreover, it can visualize data in a single place called workspace.

Related to security monitoring, below are the list of monitoring packages you can deploy to your workspace:

- **AD Assessment:** Assess the risk and health of Active Directory environment
- **Antimalware Assessment:** view status of antivirus and antimalware scan across your virtual machine.
- **Activity Log Analytics:** track all create, update and delete activities in your Azure subscription.
- **Change Tracking:** track configuration changes across your virtual machines.
- **Network Performance Monitor:** provide near real-time monitoring of network performance
- **Automation & Control:** increase control with automation and configuration management
- **Insight & Analytics:** monitor and troubleshoot infrastructure issue
- **Security & Compliance:** secure and audit security with advanced threat detection
- **Security and Audit:** provide the ability to explore security related data and identify security breaches.
- **Wire Data 2.0:** explore wire data and identify network related issues.
- **Key Vault Analytics:** understand key vault usage through log.
- **Azure Network Security Group Analytics:** provide insight of Network Security Group logs

We will practice one of these monitor modules later in chapter *Appendix, Hands-On Lab.*

## Network Monitoring

The term “Defense in depth” would drive us to another in depth strategy called monitoring in depth. That said, it is recommended to monitor every perimeter we have. For deep-dive investigation if a security incident occurs, we do need to analyze network packet and its flow, which Azure Security

Center does not provide. DDoS monitoring should be mentioned as a common case of deep inspection.

Microsoft Azure recently announced a new feature called Network Watcher. Network Watcher provides you a central of network monitoring to see your network topology, what virtual network and subnet you have, what network security group you configure to your subnet or network interface card and how it flows across your virtual machines. Not only such a general information, Network Watcher provides network diagnostic tools including IP flow verification, next hop, security group view and package capture, network security group flow and logging.

Network Watcher is very important for network monitoring on Microsoft Azure. It can help in many cases. Firstly, if you receive a performance complaint from your customer or business user, you may have to look into network factor first to see whether any core network packet is dropped or not.

Secondly, if your system is receiving a large network attack (e.g. DDoS, Botnet), you do need to monitor to trace the source of attack, and to have preventive action as soon as possible.

Currently as of this book, Network Watcher is in Public Preview with 3 regions available (US West Central, US North Central and US West).

# Storage Monitoring

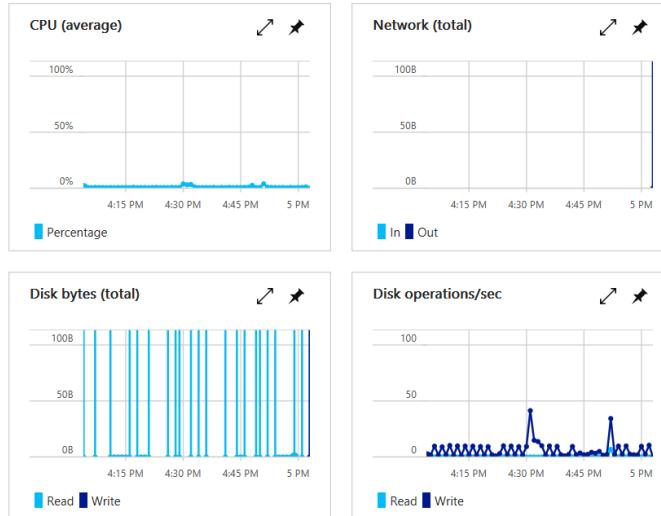
Azure Monitor can help monitor activity log on your Azure storage account. There are many metrics in Azure storage account which are worth using (e.g. **AnonymousAuthorizationError**, or **AnonymousSuccess**).

# Virtual Machine Monitoring

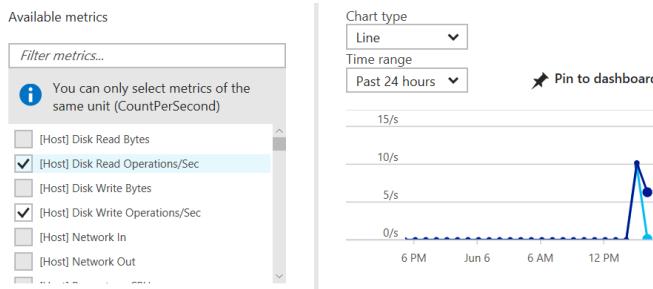
By default, you can monitor CPU (average), Network, Disk bytes and Disk operations from the overview view when opening a virtual machine. The

dashboard shows you data collected with offering of six time frames: 1 hour, 6 hours, 12 hours, 1 day, 7 days and 30 days.

Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days



These are not the only available metrics. You can add more metrics from the list of approximately 70 supported metrics. With each metric, you can control alerting. We will explore steps to set a metric for a virtual machine in Appendix, Hands-On Lab.



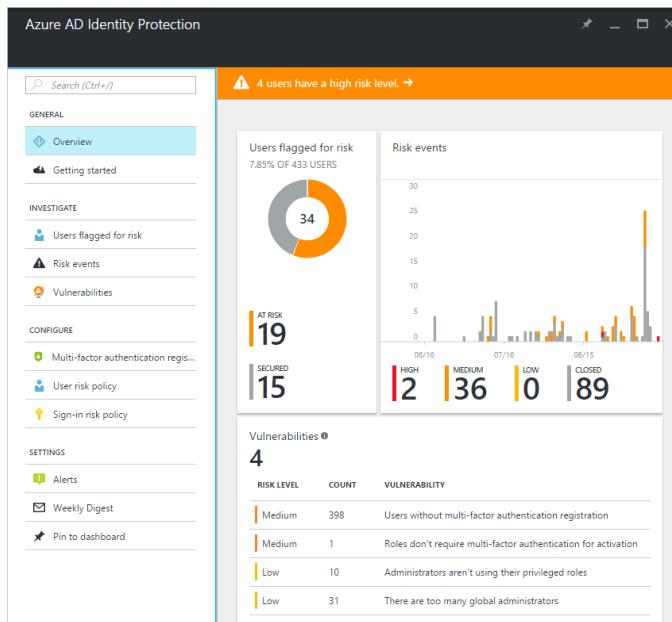
Activity log of your virtual machine can be visualized in Azure Log Analytics for monitoring. F

## Identity Monitoring

When you centralize your identity in Microsoft Azure, your team is given access to different Azure resources. In this case, you need to monitor and

manage them. With Azure Active Directory Premium, you take fully advantages of building a risk-based policy to automatically protect identities. These can include:

- Leaked credentials
- Impossible travel to atypical locations
- Sign-ins from infected devices
- Sign-in from anonymous IP addresses
- Sign-ins from IP addresses with suspicious activity
- Signs in from unfamiliar locations



More information about these capabilities, read here  
<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection>

## Summary

In this chapter, you were introduced several tools to monitor your Azure IaaS resources, including virtual machine, storage, network and identity. These tools do not only provide activity and diagnostics log but also allow you to set alert based on many metrics. We also explored Azure Security Center which specifically focuses on helping you protect Azure resources

with capabilities of detection and security recommendation on each Azure resource. Now you have finished this chapter.

## Additional References

Here is the list of additional references for each of offering in this chapter you need to learn more:

- Azure Security Center planning and operations guide:  
<https://docs.microsoft.com/en-us/azure/security-center/security-center-planning-and-operations-guide>
- Packet inspection with Azure Network Watcher:  
<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-deep-packet-inspection>
- Overview of metrics in Microsoft Azure:  
<https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-metrics>
- Get started with a Log Analytics workspace:  
<https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-get-started>

*This page intentionally left blank*

# Appendix

## Hands-On Lab

I am glad that you read to this line. This means you have finished six chapters in the book, exploring number of different features and approaches to protecting and defending your Azure IaaS. It is hard to say every chapter is written enough for you because knowledge has no limit to reach out. The more you learn, there more your knowledge. To finish the book, there should be a hands-on lab (HOL) step-by-step guidance to help you build something to practice. That is why I would love to spend more time writing this chapter.

The lab assumes you have little experience with Microsoft Azure, or you have already finished six chapters before your practice. Nevertheless, you need to do progressive step by step to complete your lab.

### **Lab 1 – Build your base SharePoint Farm**

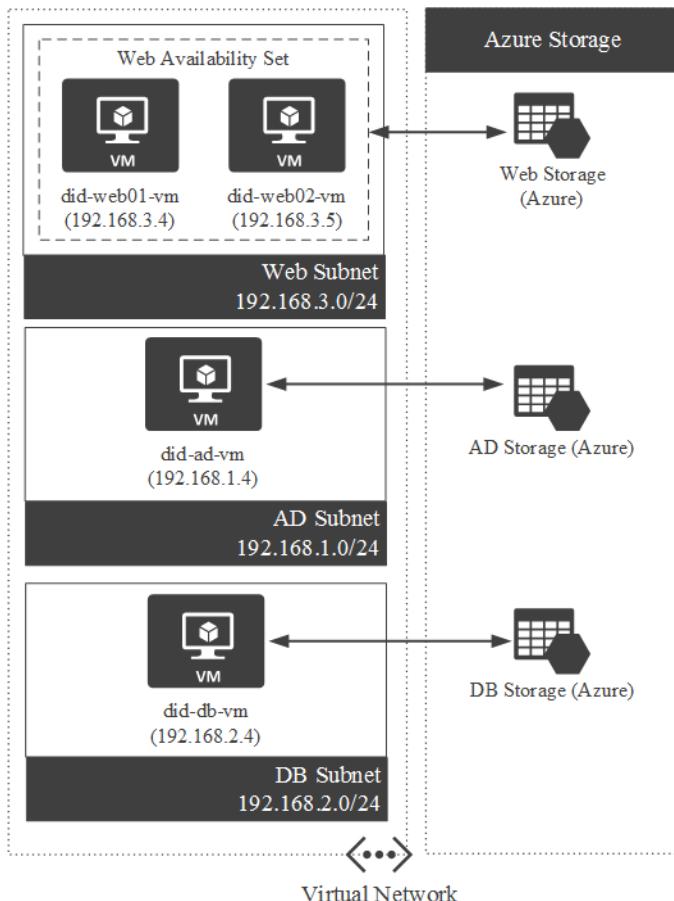
Why did I choose SharePoint farm deployment for the lab? I am not going to introduce Microsoft SharePoint platform to you. The reason that I picked SharePoint platform for the hands-on lab is because SharePoint is flexible to build on multiple servers. Each server can be easily configured to play as a specific role (e.g. web front-end role, Search Index role, database role). Moreover, SharePoint is a web application based platform that we can deploy Azure Load Balancer and Azure Application Gateway (Web Application Firewall) for further experiment. Finally, I could not think of any more appropriate platform than SharePoint for the hands-on lab in this book.

In this section, we will perform the following things:

- Lab 01: Creating Azure resource group to group all resources we need for a SharePoint farm.
- Lab 02: Creating Azure storage account to store virtual machine disks.
- Lab 03: Creating an Azure virtual network for the SharePoint farm
- Lab 04: Creating subnets for each SharePoint server role to follow network segmentation practice.
- Lab 05: Creating availability set for web front-end virtual machine to follow virtual machine availability
- Lab 06: Creating an Active Directory virtual machine
- Lab 07: Configuring Active Directory domain controller
- Lab 08: Creating SharePoint account
- Lab 09: Creating an SQL Server virtual machine from Azure Image Gallery
- Lab 10: Joining the SQL Server virtual machine to the domain controller
- Lab 11: Creating two SharePoint Server 2013 virtual machines and joining to the domain controller
- Lab 12: Provisioning and configuring SharePoint Server 2013 farm
- Lab 13: Adding the second web front-end virtual machine
- Lab 14: Creating a SharePoint website

These labs can be done very quickly with PowerShell for Azure. However, I am not going to use it. The step-by-step guidance with screenshots are more helpful to get you familiar with Microsoft Azure. Another note is that the deployment model is Resource Manager (as known as Azure RM) because this is recommended in the modern cloud deployment on Microsoft Azure.

You will have the base SharePoint farm as follows:



## Lab 1.1 – Creating your Azure resource

Azure Resource Group is the best way to group all Azure resources for better management. This lab is going to walk you through steps to create resources group for the SharePoint deployment.

---

I assume before this lab you have already registered an Azure subscription with 30 trial days.

---

After completing the lab, you will have five resource group:

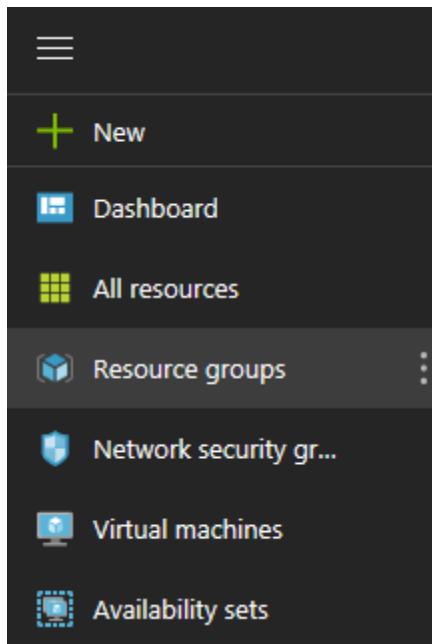
- **Active Directory:** includes virtual machine, storage account, network interface card for Active Directory role
- **Web Front-End:** includes virtual machines and storage account, network interface card for Web front-end role

- **Database:** includes virtual machine, storage account, network interface card for database role:
- **Infrastructure:** include network resources such as virtual network, load balancer, application gateway.

Role	Name	Subscription	Location
Active Directory	did-ad-rg	Visual Studio Enterprise	Southeast Asia
Web front-end	did-web-rg	Visual Studio Enterprise	Southeast Asia
Database	did-db-rg	Visual Studio Enterprise	Southeast Asia
Infrastructure	did-infra-rg	Visual Studio Enterprise	Southeast Asia

Perform the following steps to complete the lab:

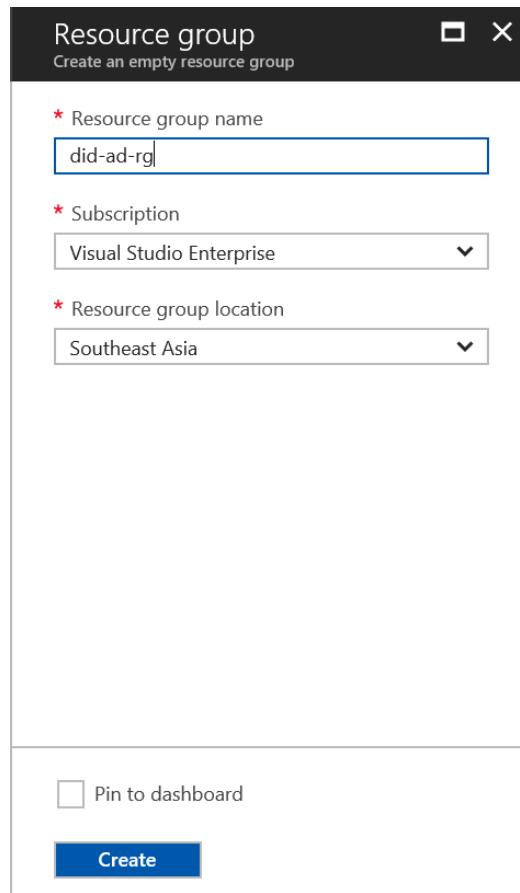
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Resource groups**



3. On the **Resource groups** blade, click **Add**.

A screenshot of the 'Resource groups' blade. The title bar says 'Resource groups' and 'TS Consulting (nnthuanlive.onmicrosoft.com)'. Below the title are buttons for '+ Add', 'Columns', and 'Refresh'. A message 'Subscriptions: 1 of 2 selected – Don't see a subscription? Switch directories' is displayed. There is a 'Filter by name...' input field and a 'Visual Studio Enterprise' button.

4. On the **Resource group** blade, type resource group name, choose your subscription and resource group location. You should choose the nearest location where you are located for better connection.



5. Click **Create**.
6. Repeat **step 1 – 5** for the other resource groups.
7. Open resource group to check the newly created resource groups.

## Resource groups

TS Consulting (nnthuanlive.onmicrosoft.com)

 Add  Columns  Refresh

**Subscriptions:** 1 of 2 selected – Don't see a subscription? [Switch directories](#)

Filter by name...

Visual Studio Enterprise

5 items

NAME	SUBSCRIPTI...	LOCATION
 did-ad-rg	Visual Studio E...	Southeast Asia
 did-db-rg	Visual Studio E...	Southeast Asia
 did-infra-rg	Visual Studio E...	Southeast Asia
 did-web-rg	Visual Studio E...	Southeast Asia

Now you have completed this lab. Remember the purpose of each resource group so you can create your resources to each group accordingly.

## Lab 1.2 – Creating Azure Storage Account

Azure Storage account is used to store your OS and data disk. This lab is going to walk you through steps to create storage account for the SharePoint deployment.

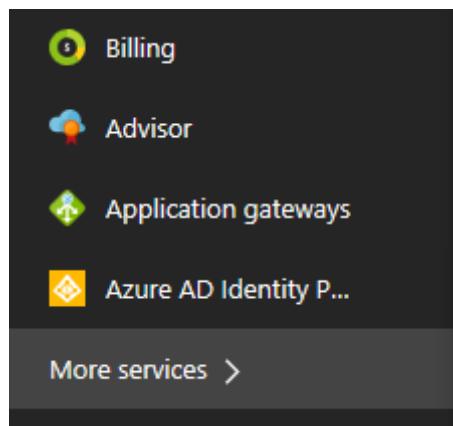
After completing the lab, you will have five resource group:

Storage account name	Type	Resource group name	Description
strdidllabad01	Standard	did-ad-rg	Storage account for AD virtual machine
strdidllabdb01	Standard	did-db-rg	Storage account for Database virtual machine
strdidllabweb01	Standard	did-web-rg	Storage account for first Web

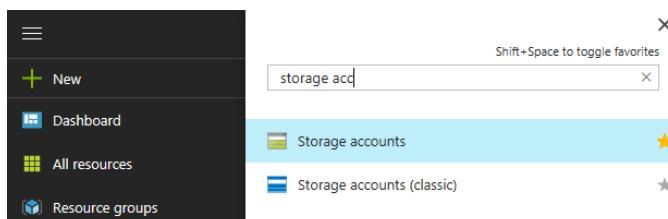
			front-end virtual machine
strdidlabweb02	Standard	did-web-rg	Storage account for second Web front-end

Perform the following steps to complete the lab:

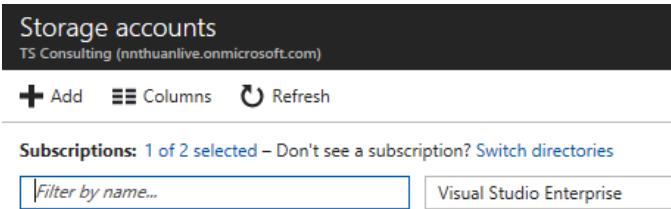
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Storage accounts**
3. If you do not see it, the navigation of storage account has not been added. To add it, scroll down to the bottom and click **More services**.



4. From the **Filter** box, type **Storage account** to search for it. Click **Storage accounts**. Do not confuse with **Storage accounts (classic)** which is only used for Azure Classic model that is out of the lab scope. Stick to the yellow star on the left to completely add the navigation of storage account to the Azure panel.

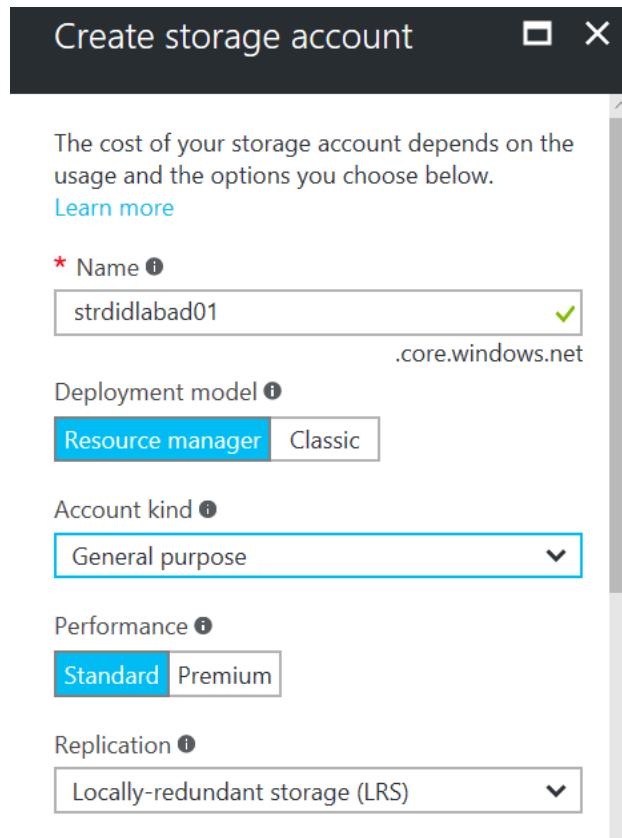


5. On the **Storage accounts** blade, click **Add**.



The screenshot shows the 'Storage accounts' blade in the Azure portal. At the top, it displays 'Storage accounts' and 'TS Consulting (nthuanlive.onmicrosoft.com)'. Below this are buttons for 'Add', 'Columns', and 'Refresh'. A message 'Subscriptions: 1 of 2 selected – Don't see a subscription? Switch directories' is shown. A search bar contains the placeholder 'Filter by name...'. A single subscription, 'Visual Studio Enterprise', is listed.

6. On the **Create storage account** blade, type the name of the new storage account, followed by the table at the beginning of this lab. Azure helps validate your storage account name to make sure it's not available.
7. Select **Resource manager** under **Deployment model** setting.
8. Select **General purpose** under **Account kind** setting.
9. Select **Standard** under **Performance** setting
10. Select **Locally-redundant storage (LRS)** under **Replication** setting.



11. Select **Disabled** under **Storage service encryption**. We will enable it later.
12. Select your **Azure subscription** under **Subscription** setting.
13. Select **Use existing** under **Resource group** setting. From the drop-down list of existing resource groups, select **did-ad-rg** because we are creating a new storage account for Active Directory virtual machine.
14. Click **Create**.

\* Storage service encryption ⓘ

\* Subscription

Visual Studio Enterprise

\* Resource group ⓘ

Create new  Use existing

did-ad-rg

\* Location

Southeast Asia

Pin to dashboard

15. Repeat from **step 5 – 14** to create other storage accounts. For database, virtual machine and application virtual machine, you can choose Premium storage if you want to experience high performance. Make sure to choose the correct resource group per storage and role. Note that two separate storage accounts for two web front-end virtual machines are still in the same resource group **did-web-rg**.
16. After that, go to check the newly created list of storage accounts.

Storage accounts					
TS Consulting (n nthuanlive.onmicrosoft.com)					
+		Add	Columns	Refresh	
<b>Subscriptions:</b> 1 of 2 selected – Don't see a subscription? <a href="#">Switch directories</a>					
<input type="text" value="Filter by name..."/>				Visual Studio Enterprise	
5 items					
NAME	KIND	RESOU...	SKU	LOCATI...	
strdidlabweb02	Storage	did-web-rg	Standard_L...	Southeast...	
strdidlabweb01	Storage	did-web-rg	Standard_L...	Southeast...	
strdidlabdb01	Storage	did-db-rg	Standard_L...	Southeast...	
strdidlabad01	Storage	did-ad-rg	Standard_L...	Southeast...	

Now you have completed this lab. Remember to create storage accounts to corresponding resource groups we planned at the beginning of this lab.

## Lab 1.3 – Creating a virtual network

This lab is going to walk you through steps to create a virtual network for the SharePoint farm.

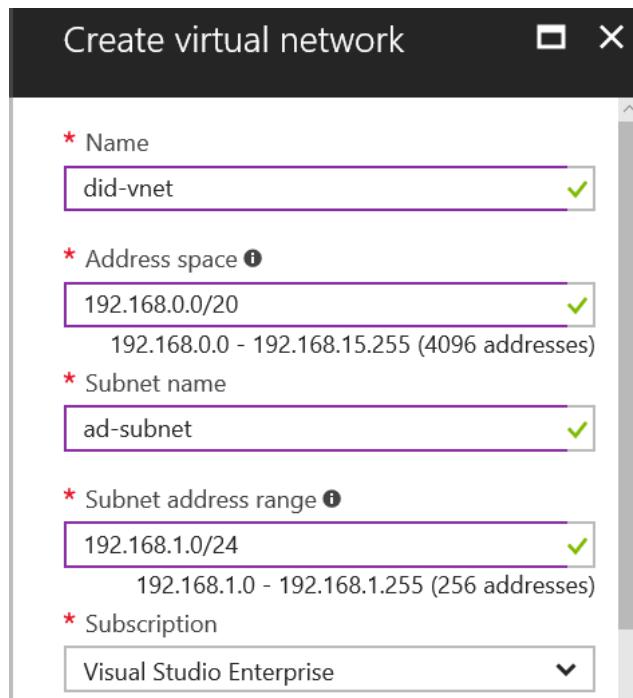
Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual networks**. If it has not been added yet, follow step 4 in **Lab 02** to add the navigation of virtual network to the left panel.
3. On the **Virtual networks** blade, click **Add**.

Virtual networks					
TS Consulting (n nthuanlive.onmicrosoft.com)					
+		Add	Columns	Refresh	
<b>Subscriptions:</b> 1 of 2 selected – Don't see a subscription? <a href="#">Switch directories</a>					
<input type="text" value="Filter by name..."/>				Visual Studio Enterprise	

4. On the **Create virtual network** blade, type the name of the new virtual network.
5. Type the IP address space under **Address space** setting. In this setting, enter **192.168.0.0/20** for our deployment.

- Type **ad-subnet** under **Subnet name** setting.
- Type **192.168.1.0/24** as the subnet address range under **Subnet** address range setting.
- Select your subscription under **Subscription** setting. Make sure you keep everything under one subscription in the lab.



- Select **Use existing** under **Resource group** setting. From drop-down list, select **did-infra-rg** because we purposely store all network resources in this resource group.
- Click **Create**.

\* Resource group [i](#)  
 Create new  Use existing  
 [v](#)

\* Location  
 [v](#)

Pin to dashboard

[Create](#) [Automation options](#)

11. After that, go to check the newly created virtual network.

Virtual networks		TS Consulting (mthuanlive.onmicrosoft.com)	★	×
		<a href="#">+ Add</a>	<a href="#">Columns</a>	<a href="#">Refresh</a>
<b>Subscriptions:</b> 1 of 2 selected – Don't see a subscription? <a href="#">Switch directories</a>				
<input type="text" value="Filter by name..."/> <a href="#">Visual Studio Enterprise</a> <a href="#">v</a>				
1 items	NAME	RESOURCE GR...	LOCATION	SUBSCRIPTION
	<a href="#">did-vnet</a>	<a href="#">did-infra-rg</a>	Southeast Asia	Visual Studio Ente... <a href="#">...</a>

Now you have completed this lab. The virtual network you just created will be used until the end of the Hands-On lab.

## Lab 1.4 – Creating Azure subnet

Azure subnet allows you to create network segment inside the virtual network you created in the previous lab. In *Chapter 3, Network Segmentation* section we discussed why we should create several segments. This lab is going to walk you through steps to create the other two subnets for Database and Web front-end virtual machines because Active Directory subnet (**ad-subnet**) was created previously.

Role	Subnet Name	Address Space	Resource group

Active Directory subnet	ad-subnet	192.168.1.0/24	did-ad-rg
Database subnet	db-subnet	192.168.2.0/24	did-db-rg
Web subnet	web-subnet	192.168.3.0/24	did-web-rg

Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual networks**.
3. Click your virtual network. In this case, it is **did-vnet**
4. Click **Subnet** under Settings.

The screenshot shows the Azure Management Portal interface. On the left, the 'Virtual networks' blade is open, showing a list of subnets under the 'did-vnet' virtual network. One subnet, 'ad-subnet', is highlighted in blue. On the right, the 'did-vnet - Subnets' blade is open, with the 'Subnets' section selected in the navigation menu. The 'Subnets' section shows the details of the 'ad-subnet' and other subnets.

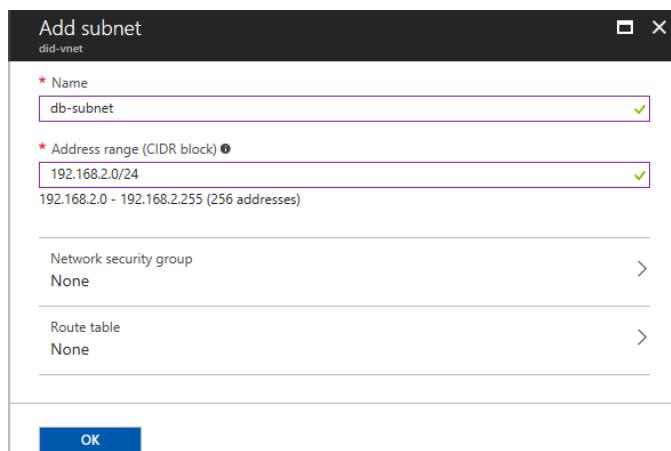
5. From the list of subnets, there is one subnet name **ad-subnet** you created in Lab 03. Now you are going to need to create more two subnets for the other roles, namely:
  - db-subnet
  - web-subnet

6. Click **Subnet**.

---

 Subnet	 Gateway subnet
<input type="text"/> Search subnets	
NAME	ADDRESS RANGE
ad-subnet	192.168.1.0/24

7. Enter the name of the new subnet for database: **db-subnet**.
8. Enter **192.168.2.0/24** under **Address range (CIDR block)** setting.
9. Leave **Network security group** and **Route table** setting by default. We will configure later.
10. Click **OK**.



11. Repeat from step 6 – 10 for web front-end subnet with the Address range value is **192.168.3.0/24**
12. Open the list of existing subnets to verify three subnets you created.

<b>+</b> Subnet	<b>+</b> Gateway subnet
<b>Search subnets</b>	
<b>NAME</b>	
<b>ADDRESS RANGE</b>	
<b>AVAILABLE ADD...</b>	
ad-subnet	
192.168.1.0/24	
251	
db-subnet	
192.168.2.0/24	
251	
web-subnet	
192.168.3.0/24	
251	

Now you have completed creating different subnets which will be associated to different virtual machine accordingly.

## Lab 1.5 – Creating web front-end availability set

In the SharePoint farm that we are going to deploy on Microsoft Azure, there are two web front-end virtual machines. To achieve the availability of web front-end role, we need availability set. This lab is going to walk you through steps to create availability set for web front-end role.

---

Please find advanced deployment of fully highly available SharePoint Server 2016 farm on Microsoft Azure in my upcoming book. Follow my blog at <http://thuansoldier.net> for an update.

---

Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Availability sets**. If it has not been added yet, follow step 4 in **Lab 02** to add the navigation of virtual network to the left panel.
3. On the **Availability sets** blade, click **Add**.

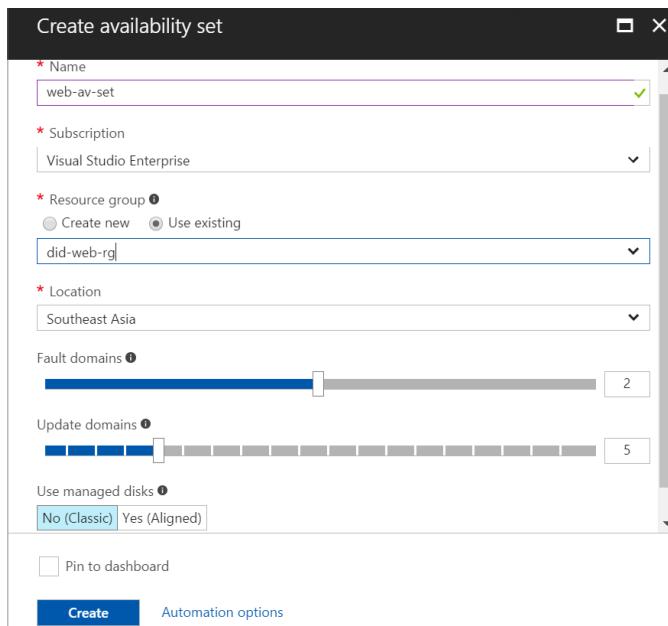
**Availability sets**  
TS Consulting (nnthuanlive.onmicrosoft.com)

**+** Add   **≡** Columns   **⟳** Refresh

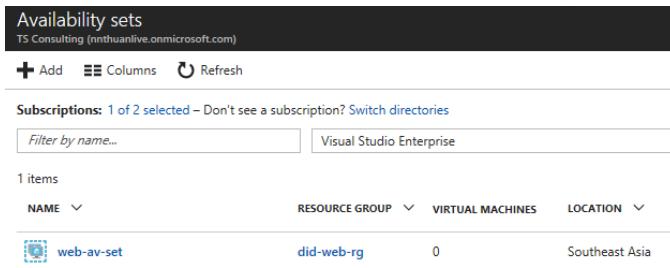
**Subscriptions: 1 of 2 selected** – Don't see a subscription? [Switch directories](#)

Visual Studio Enterprise

4. Enter the name of your availability set. In this case, it is **web-av-set**.
5. Select your subscription under **Subscription** setting.
6. Select **Use existing** under **Resource group** setting. From the drop-down list, select **did-web-rg**.
7. Select your location under **Location** setting.
8. Keep **Fault domains** and **Update domains** values by default.
9. Select **No** under **Use managed disks** setting. We do not use **Managed Disk** feature in this lab. Instead we will specify storage account accordingly.
10. Click **Create**.



11. After that, go to check the newly created availability set for web front-end virtual machines. Note that we have not added web front-end virtual machines to this availability set so from the screen the number of virtual machine (in **VIRTUAL MACHINE** column) is **0**.



NAME	RESOURCE GROUP	VIRTUAL MACHINES	LOCATION
web-av-set	did-web-rg	0	Southeast Asia

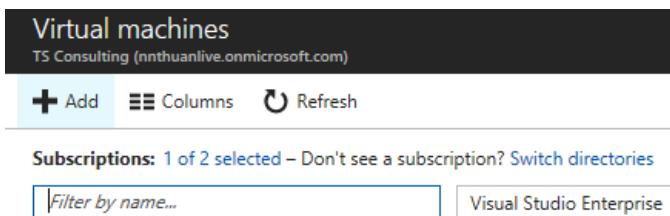
Now you have completed this lab. You will be configuring two web front-end virtual machines to be associated to this availability set.

## Lab 1.6 – Creating an Active Directory virtual machine

Active Directory virtual machine will run Active Directory Domain Service and be promoted to be the main domain controller for the SharePoint farm. The authentication and all accounts used for the SharePoint farm is processed and managed on this Active Directory virtual machine. This lab is going to walk you through steps to create a new Active Directory virtual machine.

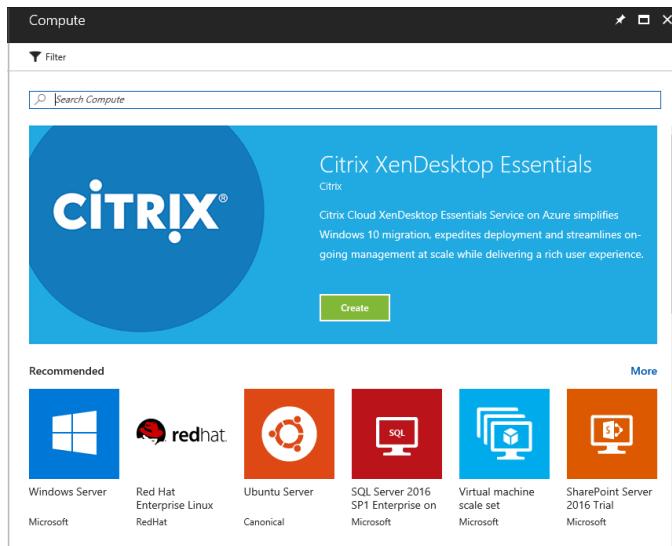
Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual machines**. If it has not been added yet, follow step 4 in **Lab 02** to add the navigation of virtual network to the left panel.
3. On the **Virtual machines** blade, click **Add**.

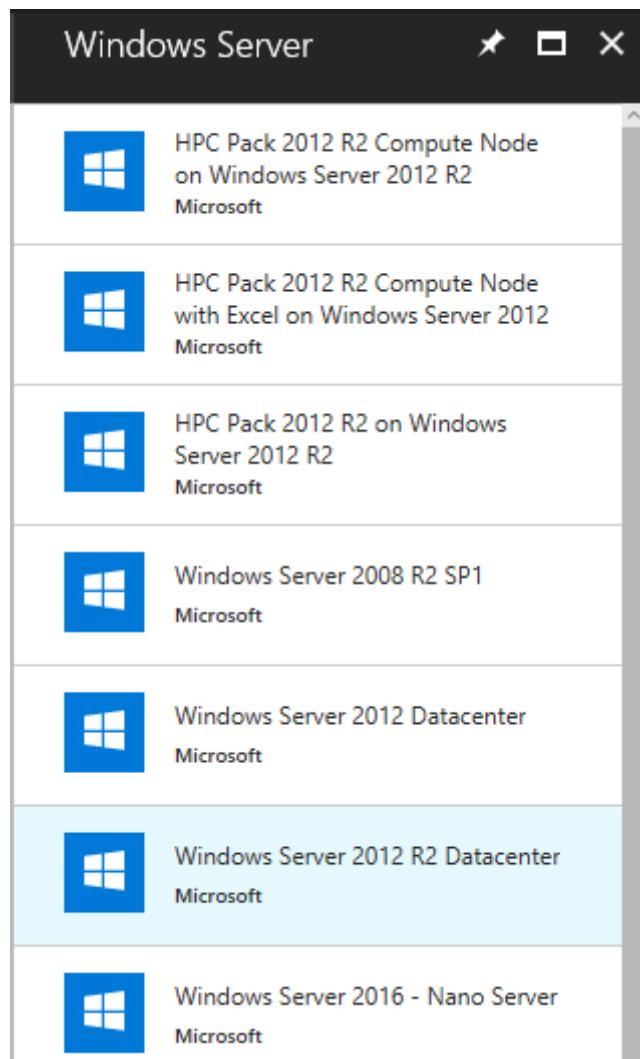


NAME	RESOURCE GROUP	VIRTUAL MACHINES	LOCATION
Visual Studio Enterprise	did-web-rg	0	Southeast Asia

4. From the **Compute** blade, select **Windows Server**.



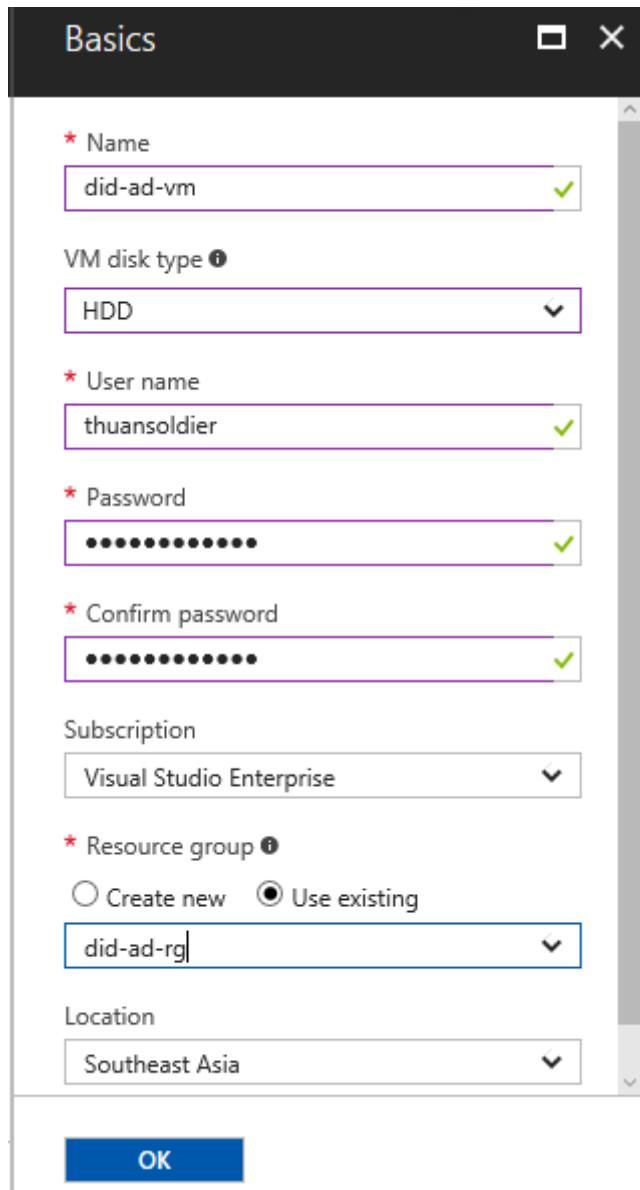
5. Select **Windows Server 2012 R2 Datacenter** image.



6. On the **Windows Server 2012 R2 Datacenter** blade, select **Resource Manager** under **Select a deployment model** setting.
7. Click **Create**.



8. On the **Create virtual machine** blade, you need to configure and specify configuration for this virtual machine.
9. On the **Basics** blade, enter the name for the virtual machine. In this case, we name **did-ad-vm**.
10. Select **HDD** under **VM disk type** setting.
11. Enter the username of the local account you will use to log into after creating the virtual machine.
12. Enter the password. This must follow password complexity.
13. Select your subscription under **Subscription** setting.
14. Select **Use existing** under **Resource group** setting. From the drop-down list, select **did-ad-rg** because your virtual machine will be put into this resource group.
15. Select your location under **Location**.
16. Click **OK**.



17. On the **Choose a size** blade, select the virtual machine size for your Active Directory virtual machine. Click **View all** to see all options. For testing, look for **Standard\_D2** size.
18. Click **Select**.

Choose a size  
Browse the available sizes and their features

<b>476.16</b> USD/MONTH (ESTIMATED)	<b>952.32</b> USD/MONTH (ESTIMATED)	<b>72.91</b> USD/MONTH (ESTIMATED)
<b>D2 Standard</b>	<b>D3 Standard</b>	<b>D4 Standard</b>
2 Cores	4 Cores	8 Cores
7 GB	14 GB	28 GB
4 Data disks	8 Data disks	16 Data disks
4x500 Max IOPS	8x500 Max IOPS	16x500 Max IOPS
100 GB Local SSD	200 GB Local SSD	400 GB Local SSD
Load balancing	Load balancing	Load balancing
<b>145.82</b> USD/MONTH (ESTIMATED)	<b>291.65</b> USD/MONTH (ESTIMATED)	<b>583.30</b> USD/MONTH (ESTIMATED)
<b>D11 Standard</b>	<b>D12 Standard</b>	<b>D13 Standard</b>
2 Cores	4 Cores	8 Cores
14 GB	28 GB	56 GB
4	8	16
<b>Select</b>		

19. On the **Settings** blade, select **No** under **Use managed disks** setting.
20. Select the storage account we created for Active Directory virtual machine. It's **strididlabad01** (refer to *Lab 02*).

Settings

Choose storage account

Storage

Use managed disks **No** **Yes**

\* Storage account **strididlabad01**

Network

\* Virtual network **(new) did-ad-rg-vnet**

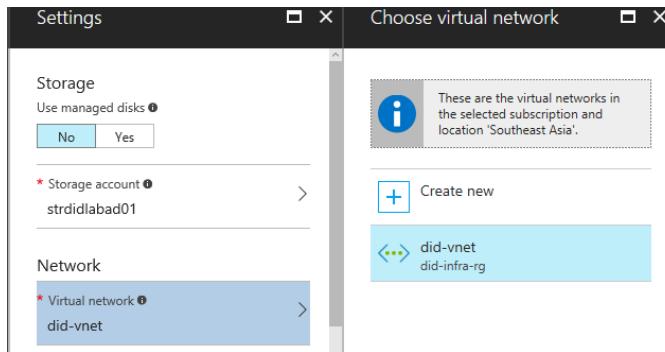
\* Subnet **did-ad-rg**

**strididlabad01** did-ad-rg Southeast Asia...

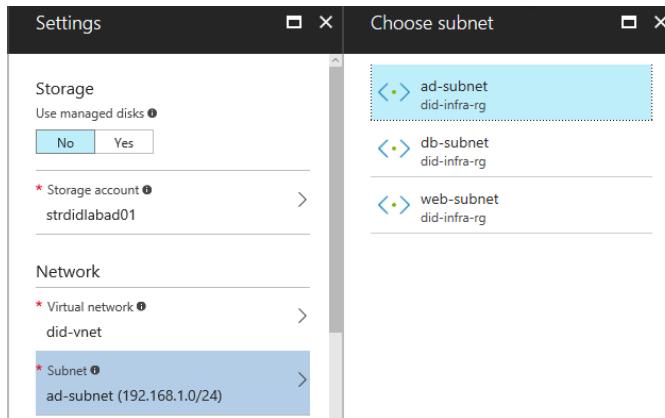
**Zd1993southeastasia** securitydata Southeast Asia...

**strididlabad01** did-db-rg Southeast Asia...

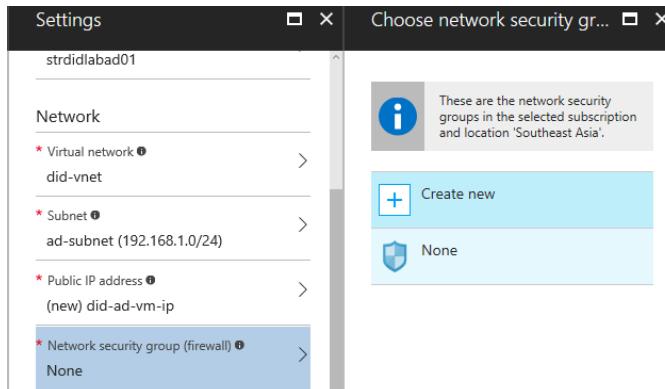
21. Click **Virtual network** and select the virtual network you created in *Lab 03*. It is **did-vnet**.



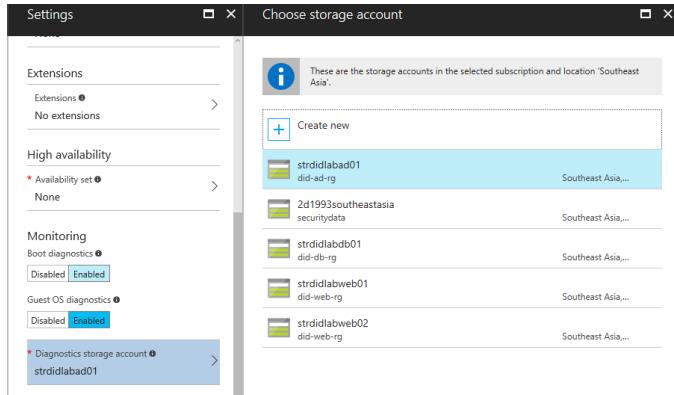
22. Click **Subnet** and select **ad-subnet** we created in Lab 03.



23. Keep **Public IP address** setting by default if Azure has already created a public IP address for you. We initially need it to remotely connect to configure Active Directory virtual machine
24. Click **Network security group (firewall)** setting and select **None**. We will practice soon in the next few labs.

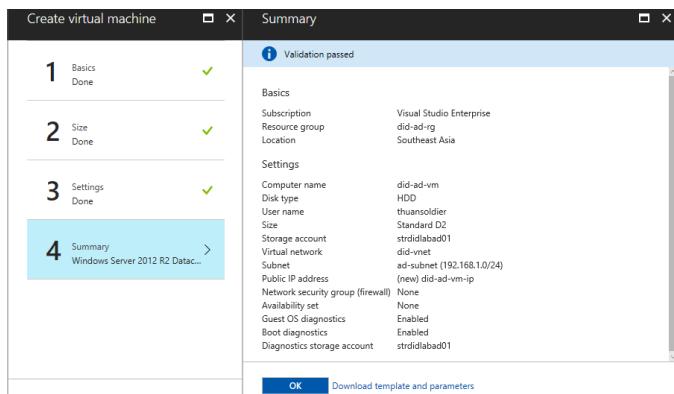


25. Keep **Extensions** setting by default with no extension. We will manually add Microsoft Antimalware extension later.
26. Keep **High availability** setting by default because we do not use availability set for the Active Directory virtual machine.
27. Select **Enabled** under **Boot diagnostics**.
28. Select **Enabled** under **Guest OS diagnostics**.
29. In **Diagnostics storage account** setting, select **strdidlabad01**.
30. Click **OK**.

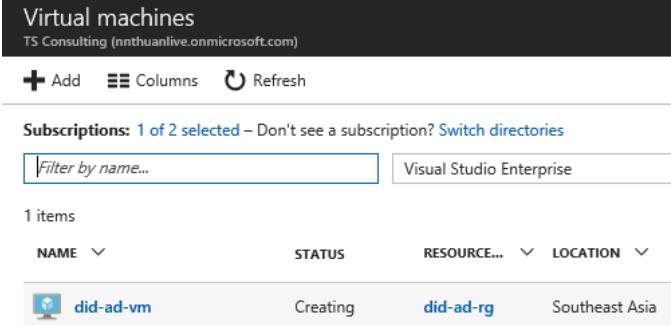


31. You are going to finalize the last step. In **Summary** blade, review again all information for the new Active Directory virtual machine. Make sure you are going to put your Active Directory virtual machine to the correct resource group (**did-ad-rg**). This virtual machine must be stored in the storage account (**strdidlabad01**). The virtual network must be **did-vnet**. Its subnet must be **ad-subnet**.

32. Click **OK** to start provisioning the virtual machine.



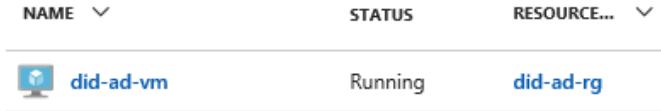
33. You can check the status of virtual machine provisioning at the **STATUS** column.



The screenshot shows the Azure Virtual Machines list. At the top, there are buttons for 'Add', 'Columns', and 'Refresh'. Below that, a message says 'Subscriptions: 1 of 2 selected – Don't see a subscription? [Switch directories](#)'. There is a 'Filter by name...' input field and a dropdown for 'Visual Studio Enterprise'. The table has columns: NAME, STATUS, RESOURCE..., and LOCATION. One item is listed: did-ad-vm, STATUS: Creating, RESOURCE...: did-ad-rg, LOCATION: Southeast Asia.

NAME	STATUS	RESOURCE...	LOCATION
did-ad-vm	Creating	did-ad-rg	Southeast Asia

34. Wait around 5-10 minutes to complete provisioning Active Directory virtual machine.



The screenshot shows the Azure Virtual Machines list again. The table has columns: NAME, STATUS, RESOURCE... . One item is listed: did-ad-vm, STATUS: Running, RESOURCE...: did-ad-rg.

NAME	STATUS	RESOURCE...
did-ad-vm	Running	did-ad-rg

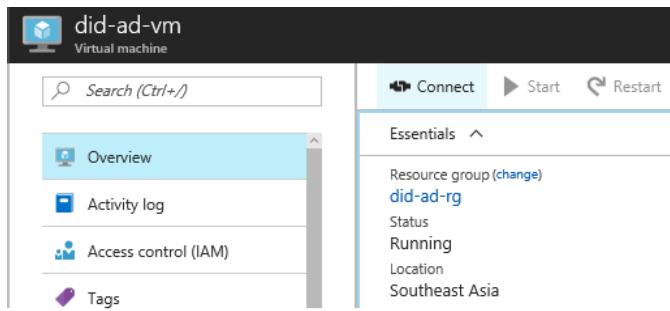
Now you have completed this lab.

## Lab 1.7 – Configuring Active Directory Domain Services

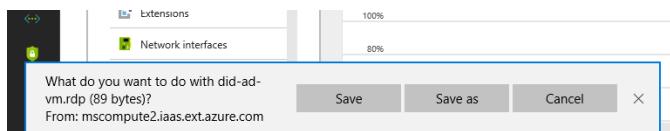
After creating a new virtual machine for Active Directory, now you need to promote this machine to be a domain controller. This lab is going to walk you through steps to configuring Active Directory Domain Services for the newly created virtual machine.

Perform the following steps to complete the lab:

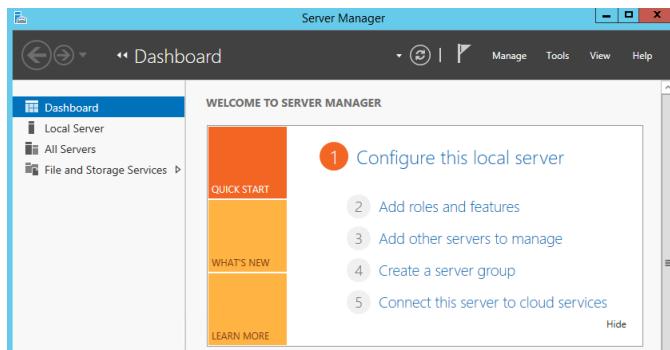
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual machines**.
3. Click **did-ad-vm**
4. Click **Connect**



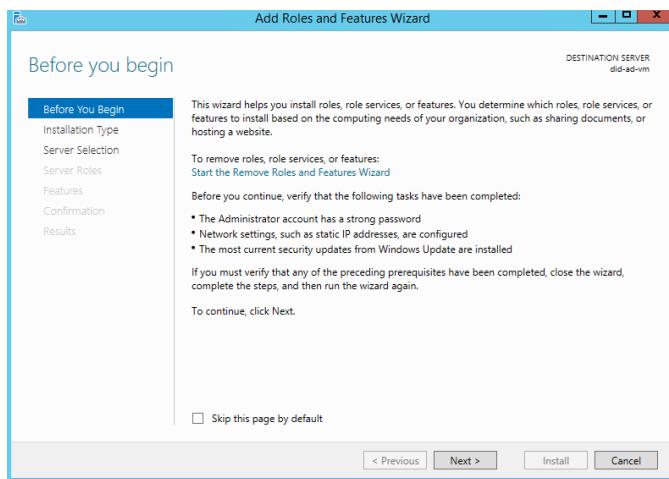
5. The browser asks you to download the .RDP file to remotely connect to the virtual machine. Click **Save**.



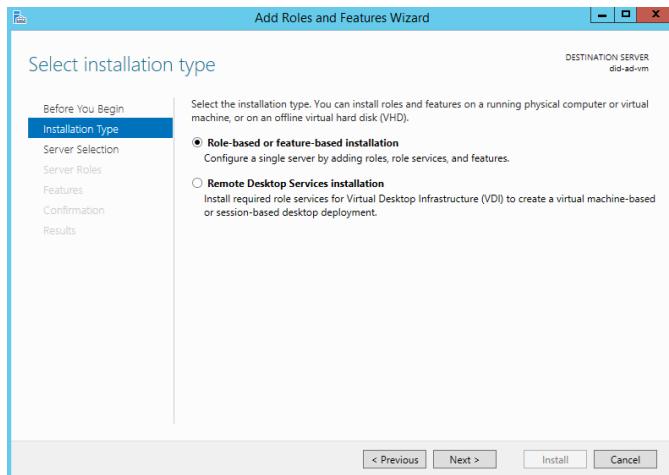
6. Double click **did-ad-vm.rdp** file. The Remote Desktop Connection client is opened. It asks you to confirm to connect because the publisher of this remote connection cannot be identified. Click **Connect**.
7. Enter the username and password you set in step 11 and 12 of **Lab 1.6**.
8. Click **OK**.
9. You are asked to confirm again because the certificate to establish the remote connection is not from a trusted certifying authority. Click **Yes**.
10. When you log in the virtual machine at the first time, the **Server Manager** tool is automatically opened. Click **Add roles and features**.



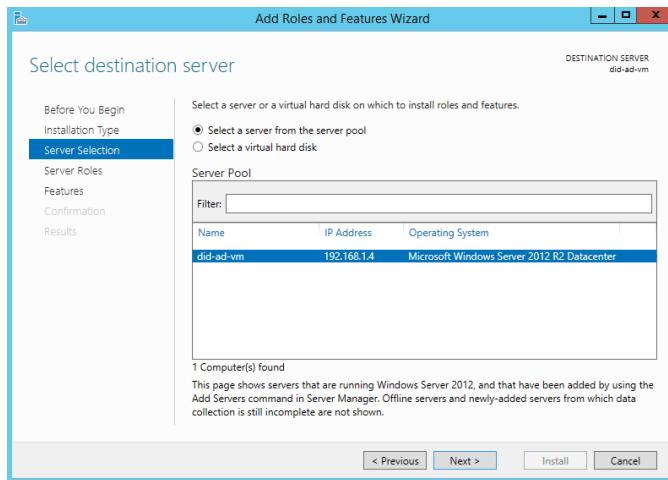
11. In **Before you begin** page, read the introduction from Microsoft. Click **Next**.



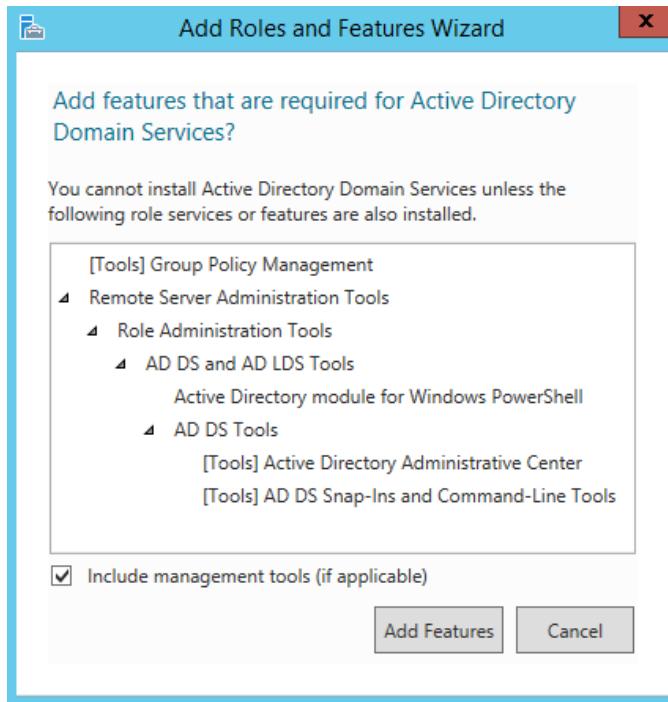
12. In **Select installation type** page, select **Role-based or feature-based installation**. Click **Next**.



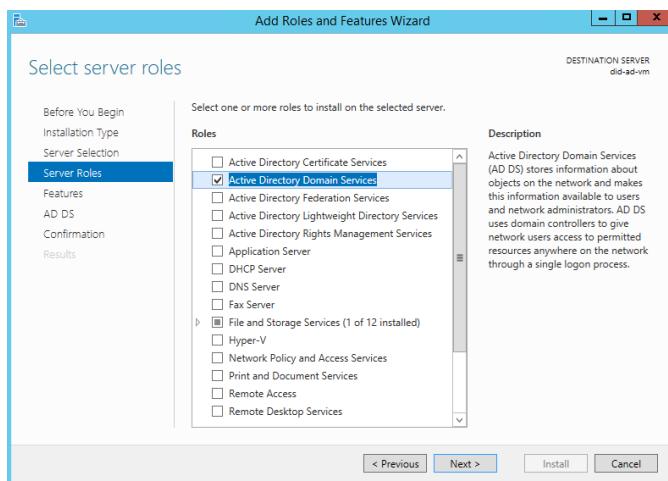
13. In **Select destination server** page, select **Select a server from the server pool**. Click the virtual machine you created (**did-ad-vm**). Click **Next**.



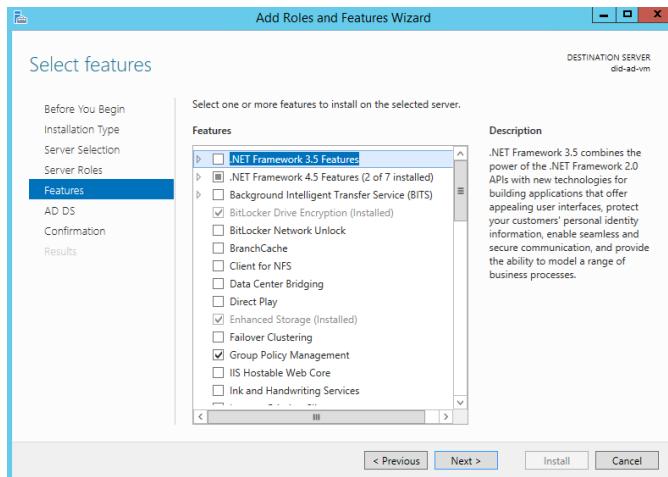
14. In **Select server role** page, select **Active Directory Domain Services**. There is a pop-up asking you to add required features before you can add the Active Directory Domain Services role.
15. Click **Add features**



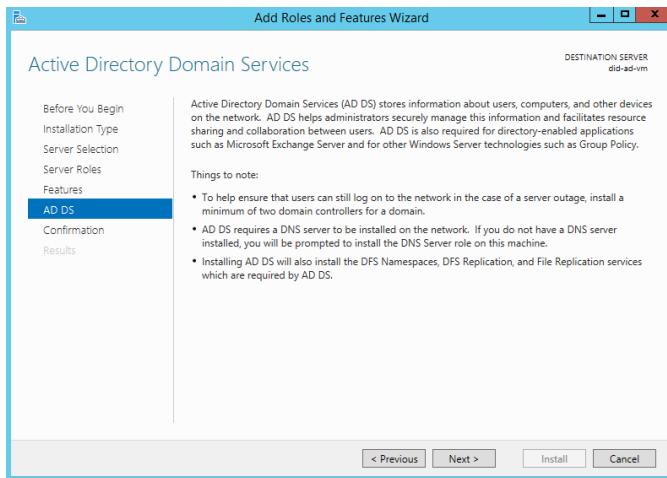
16. Make sure Active Directory Domain Services role is selected. Click **Next**.



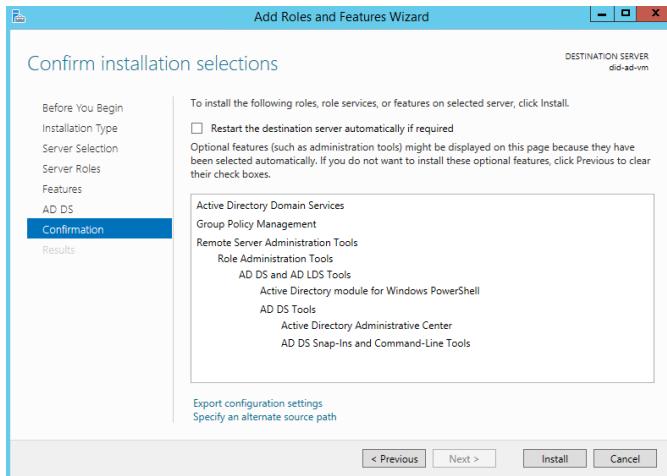
17. In **Select features** page, keep everything by default. Click **Next**.



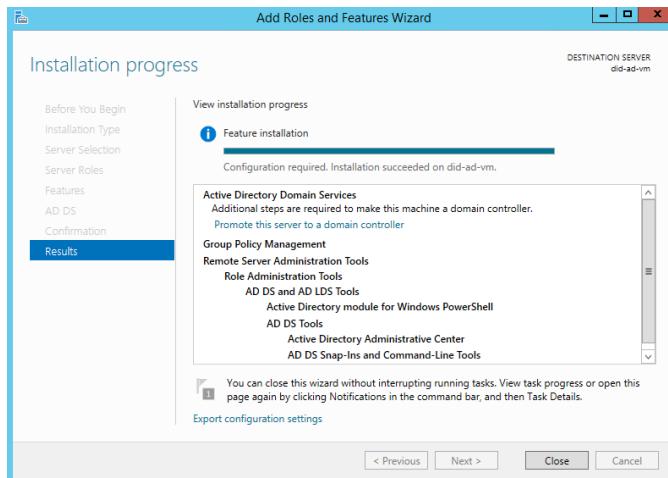
18. In **Active Directory Domain Services** page, read the information about Active Directory Domain Services capabilities and some notes.



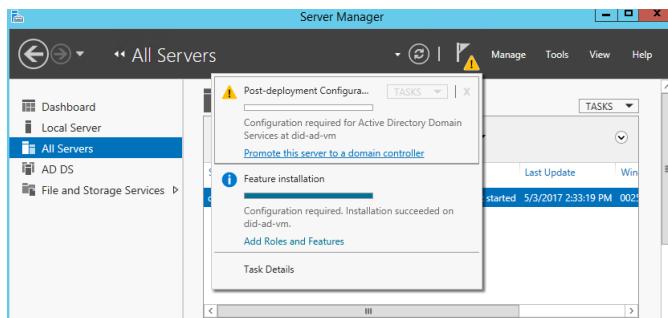
19. In **Confirm installation selections** page, click **Install**.



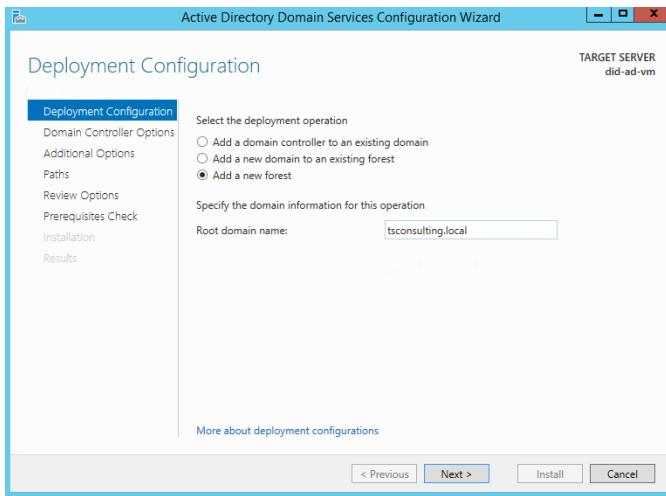
20. Wait a few minutes to complete the installation. Click **Close**.



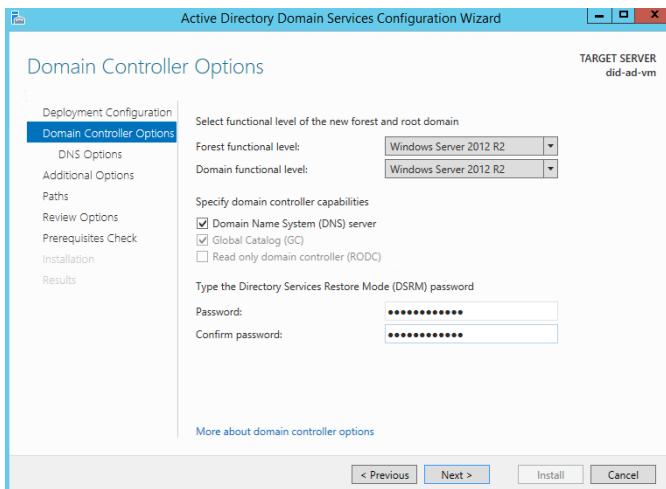
21. From **Server Manager** tool, click small yellow triangle in top bar. Click **Promote this server to a domain controller**.



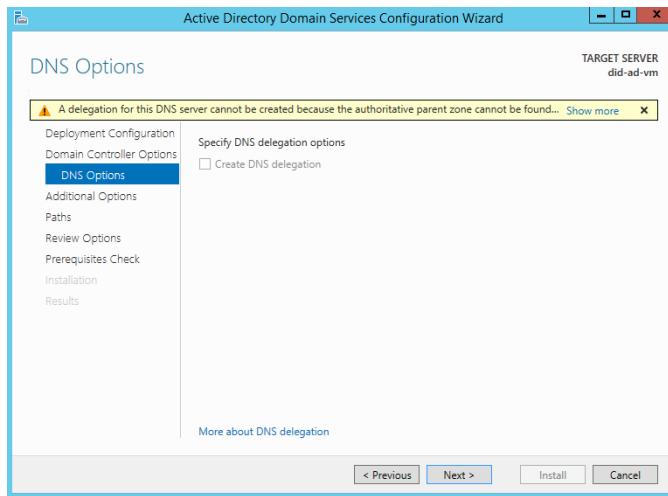
22. In **Deployment Configuration** page, select **Add a new forest**. Enter the root domain name. For example, **tsconsulting.local**. Click **Next**.



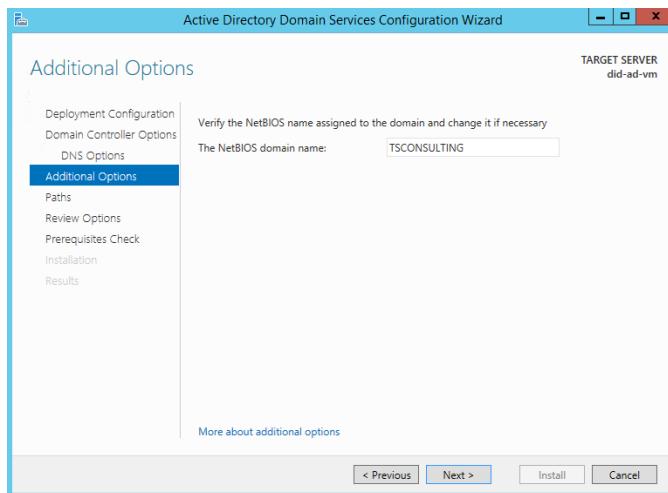
23. In **Domain Controller Options** page, keep settings by default with Enter the **Directory Services Restore Mode (DSRM)** password. Click **Next**



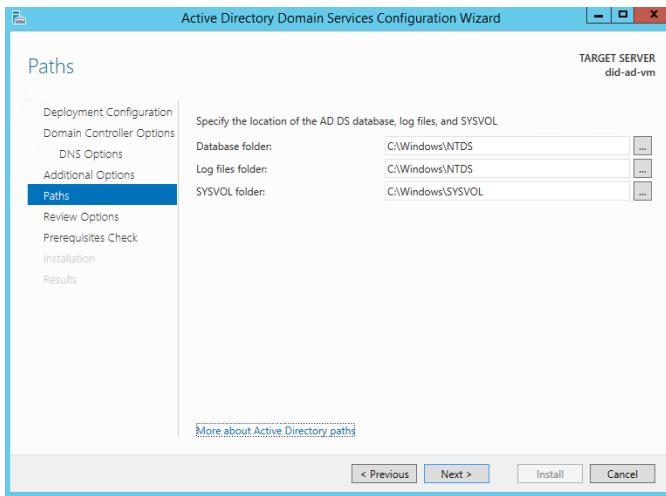
24. In **DNS Options** page, ignore the warning message. Click **Next**.



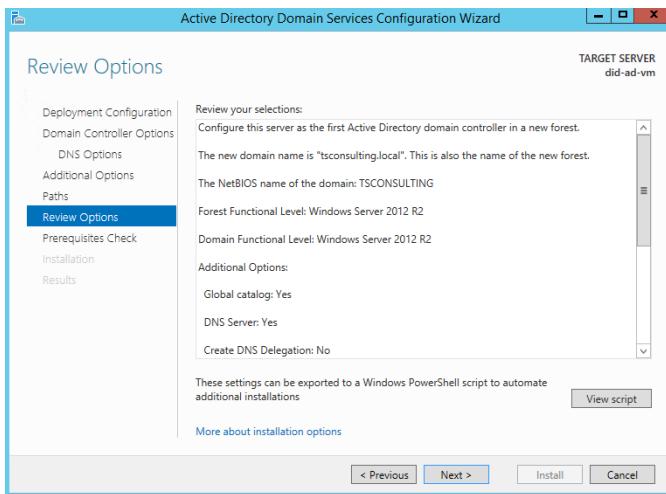
25. In **Additional Options** page, the NetBIOS name is automatically generated. Click **Next**



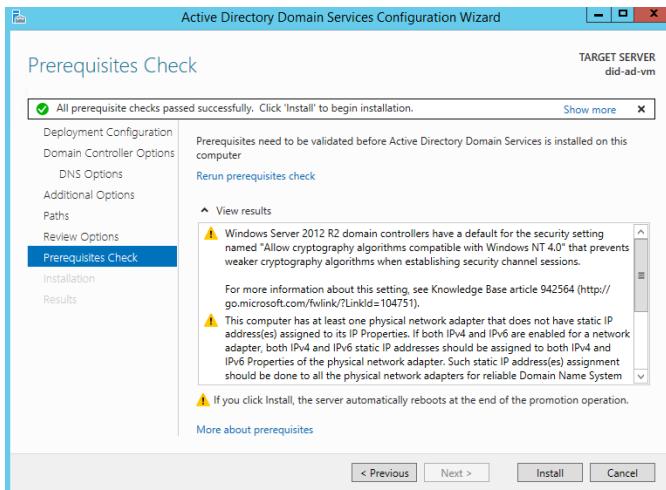
26. In **Paths** page, specify location of the AD DS database, log files and SYSVOL. Keep everything by default. Click **Next**.



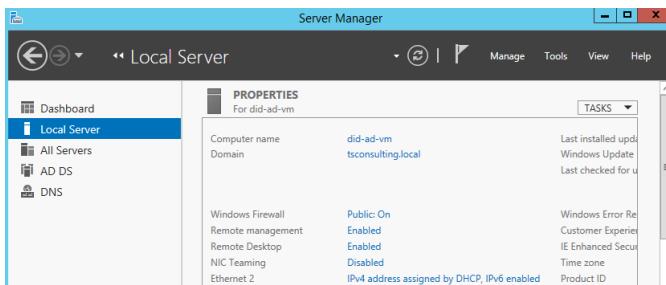
27. In **Review Options** page, review all settings you have set up. Click **Next**.



28. In **Prerequisites Check** page, ignore warning messages. We only need to promote the virtual machine to domain controller for authentication, as well as SharePoint account management only. Click **Install**.



29. Wait 5-10 minutes for the domain controller configuration. The virtual machine will be automatically restarted after the configuration is complete.
30. Repeat step 4 in this lab to connect to the Active Directory virtual machine.
31. Use the domain account instead of the local account. It is `tsconsulting\thuansoldier`. Click **OK**.
32. You are asked to confirm the untrusted certificate. Note that you are not connecting to the local virtual machine anymore. It's the full qualified domain name `did-ad-vm.tsconsulting.local`. Click **Yes**.
33. From **Server Manager** tool, click **Local Server**. Verify your domain name at **Domain** setting.

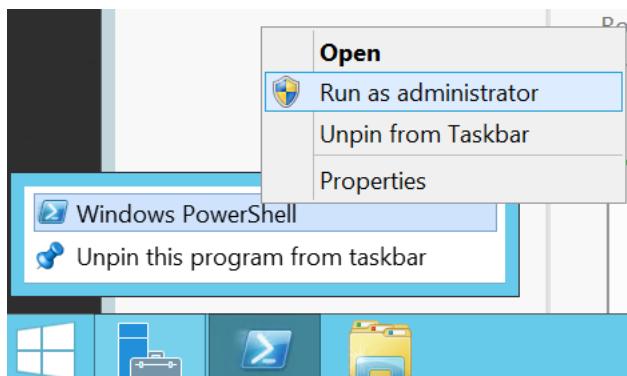


## Lab 1.8 – Creating Active Directory accounts

You can use the domain administrator account for testing. However, for more practical, you should create a few accounts including system administrator account, SharePoint farm account. This lab is going to walk you through steps to create a few Active Directory accounts by PowerShell.

Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. RDP to your Active Directory virtual machine, followed by step 3 to 9 in *Lab 07*. Make sure you log into the virtual machine using domain account (in this case it is `tsconsulting\thuansoldier`)
3. From the Task bar, right click on PowerShell icon. Keep right clicking on Windows PowerShell and select **Run as administrator**.



4. Type the following PowerShell command to create **sp\_farm** account

```
New-ADUser -SamAccountName sp_farm -AccountPassword (read-host "Enter password" -assecurestring) -name "SharePoint Farm Account" -enabled $true -PasswordNeverExpires $true -ChangePasswordAtLogon $false
```

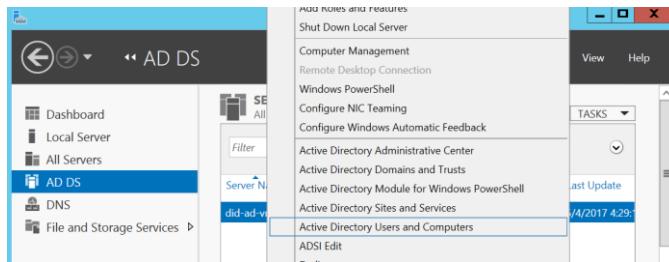
5. We need to disable **Password never expires** and **User must change password at next login** policies for testing purpose. In production environment, these policies need to be enabled. We



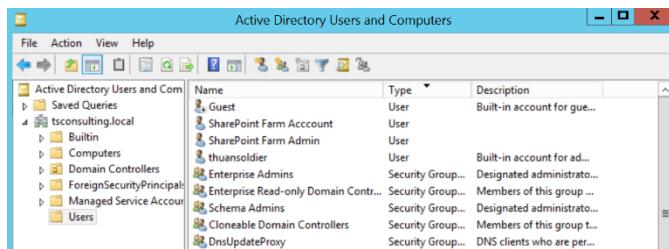
- Repeat step 4 again for another account. It can be your system administrator account e.g. **sp\_admin**. (Change the value in *SamAccountName* property inside PowerShell script)

```
New-ADUser -SamAccountName sp_admin -AccountPassword
(read-host "Enter password" -assecurestring) -name
"SharePoint Farm Admin" -enabled $true -
PasswordNeverExpires $true -ChangePasswordAtLogon $false
```

- To check if the two accounts above are successfully created, open Server Manager. Click **AD DS**.
- Right click on the domain controller virtual machine and click **Active Directory Users and Computers**.



- In **Active Directory Users and Computers** windows, expand your domain. Right click on **Users** and select **New**. Select **User**.
- From the list of users, look for the two newly created accounts.



Now you have completed this lab. These accounts will be used for SharePoint farm configuration and management later.

## Lab 1.9 – Creating an SQL Server virtual machine

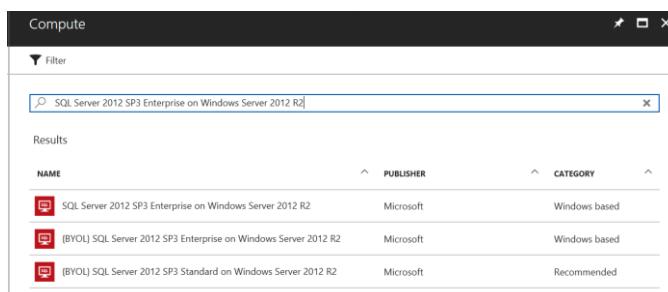
Database virtual machine will be running SQL Server 2012 and be the main database server for the SharePoint farm. This lab is going to walk you through steps to create a new SQL Server 2012 virtual machine from Microsoft Azure Image Gallery.

Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual machines**
3. Click **Add**.
4. On the **Compute** blade, search for SQL Server 2012 from *Search Compute* search box. There is an auto-generated drop-down list of SQL Server 2012 images. Select **SQL Server 2012 SP3 Enterprise on Windows Server 2012 R2** image.



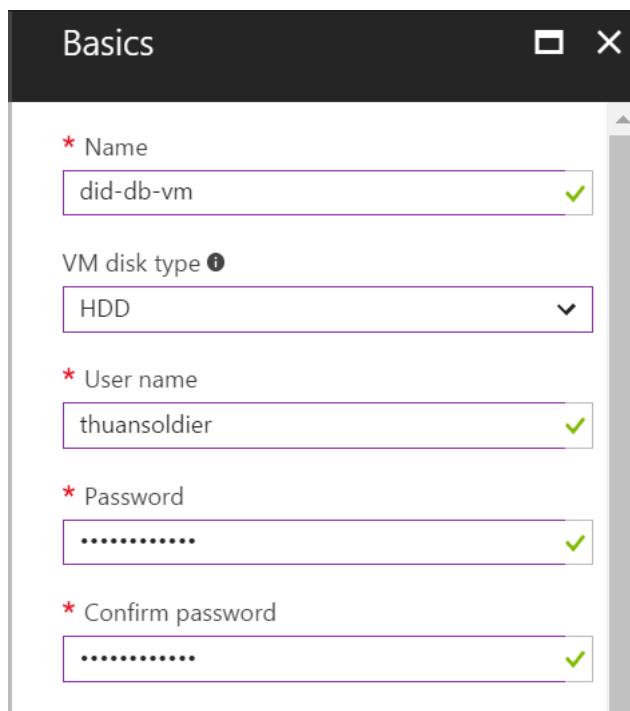
5. There are three versions after you select the image. Select the first one, **SQL Server 2012 SP3 Enterprise on Windows Server 2012 R2**.



6. On the **SQL Server 2012 SP3 Enterprise on windows Server 2012 R2** blade, make sure the deployment model is **Resource Manager**.
7. Click **Create**.

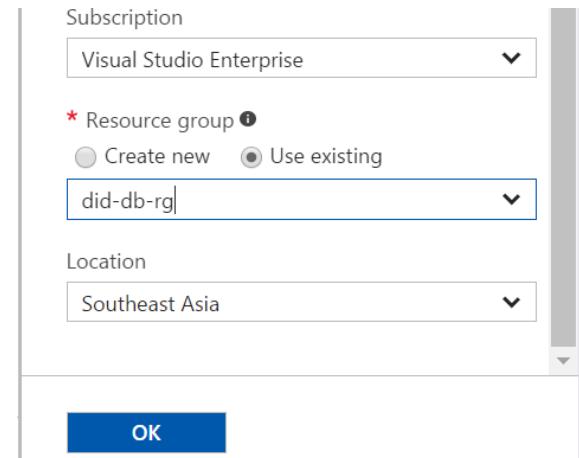


8. On the **Basics** blade, enter the name for the virtual machine. In this case, we name **did-db-vm**.
9. Select **HDD** under **VM disk type** setting.
10. Enter the username of the local account you will use to log into after creating the virtual machine.
11. Enter the password. This must follow password complexity.



12. Select your subscription under **Subscription** setting.

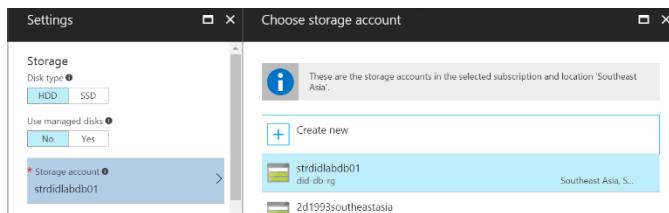
13. Select **Use existing** under **Resource group** setting. From the drop-down list, select **did-db-rg** because your virtual machine will be put into this resource group.
14. Select your location under **Location**.
15. Click **OK**.



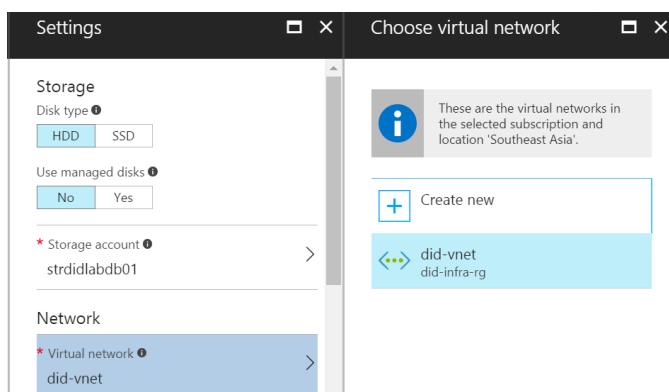
16. On the **Choose a size** blade, select the virtual machine size for your SQL Server 2012 virtual machine. Click **View all** to see all options. For testing, look for **Standard\_DS2** size. Click **Select**.

Choose a size		
Browse the available sizes and their features		
DS2 Standard	DS3 Standard	DS4 Standard
2 Cores	4 Cores	8 Cores
7 GB	14 GB	28 GB
4 Data disks	8 Data disks	16 Data disks
6400 Max IOPS	12800 Max IOPS	25600 Max IOPS
14 GB Local SSD	28 GB Local SSD	56 GB Local SSD
Load balancing	Load balancing	Load balancing
Premium disk support	Premium disk support	Premium disk support
145.82 USD/MONTH (ESTIMATED)		
DS11 Standard	DS12 Standard	DS13 Standard
2 Cores	4 Cores	8 Cores
14 GB	28 GB	56 GB
4	8	16
291.65 USD/MONTH (ESTIMATED)		
583.30 USD/MONTH (ESTIMATED)		
<b>Select</b>		

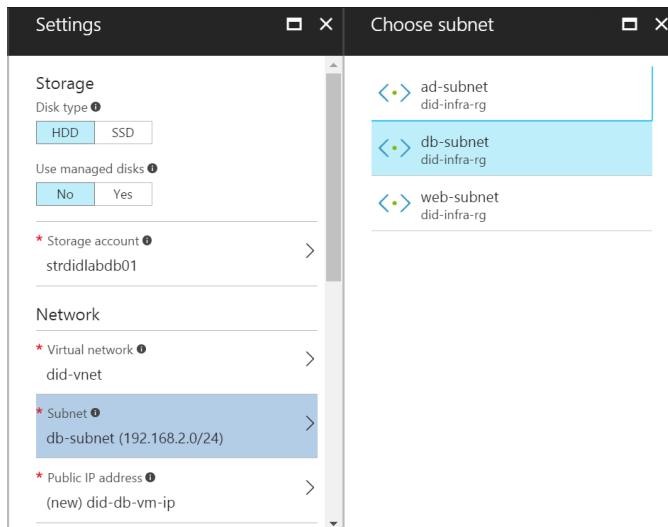
17. On the **Settings** blade, you may see the warning information about Premium disk supportability. Ignore this message while we are testing only.
18. Select **HDD** under **Disk type** setting
19. Select **No** under **Use managed disks** setting.
20. Select the storage account we created for your database virtual machine. It's **strdidlabdb01** (refer to **Lab 1.2**).



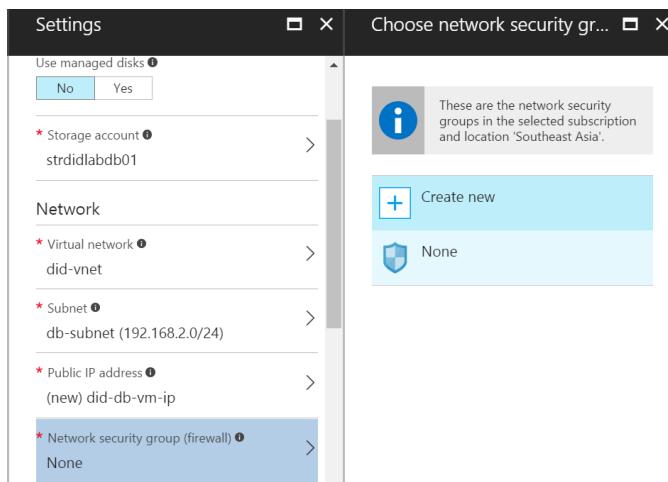
21. Click **Virtual network** and select the virtual network you created in **Lab 03**. It is **did-vnet**.



22. Click **Subnet** and select **db-subnet** we created in *Lab 04*.

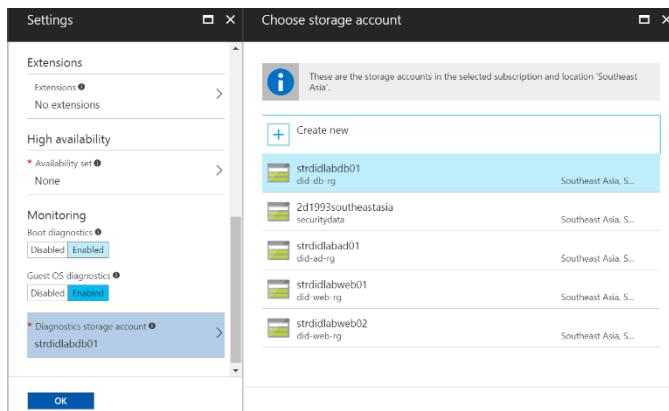


23. Keep **Public IP address** setting by default if Azure has already created a public IP address for you. We initially need it to remotely connect to configure the SQL Server virtual machine
24. Click **Network security group (firewall)** setting and select **None**. We will practice soon in the next few labs.

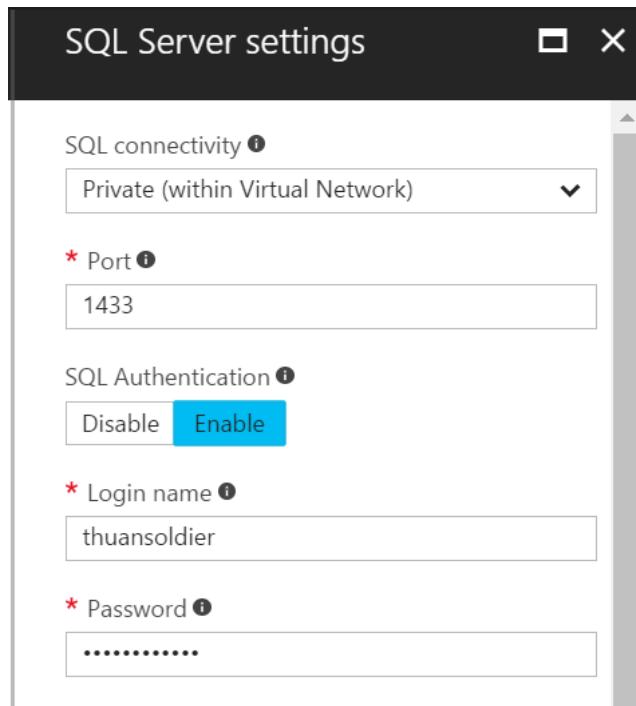


25. Keep **Extensions** setting by default with no extension. We will manually add Microsoft Antimalware extension later.
26. Keep **High availability** setting by default because we do not use availability set for the database virtual machine in the lab.
27. Select **Enabled** under **Boot diagnostics**.

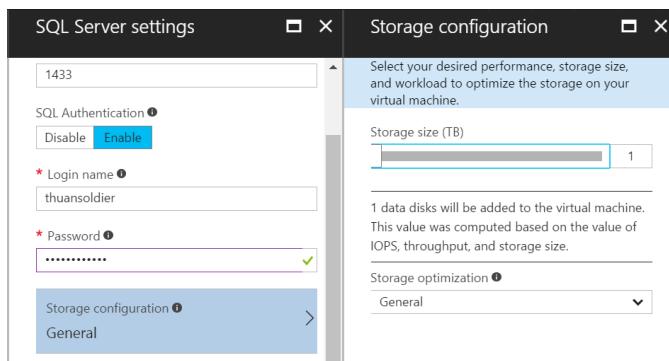
28. Select **Enabled** under **Guest OS diagnostics**.
29. Under **Diagnostics storage account** setting, select **strididlabdb01**
30. Click **OK**.



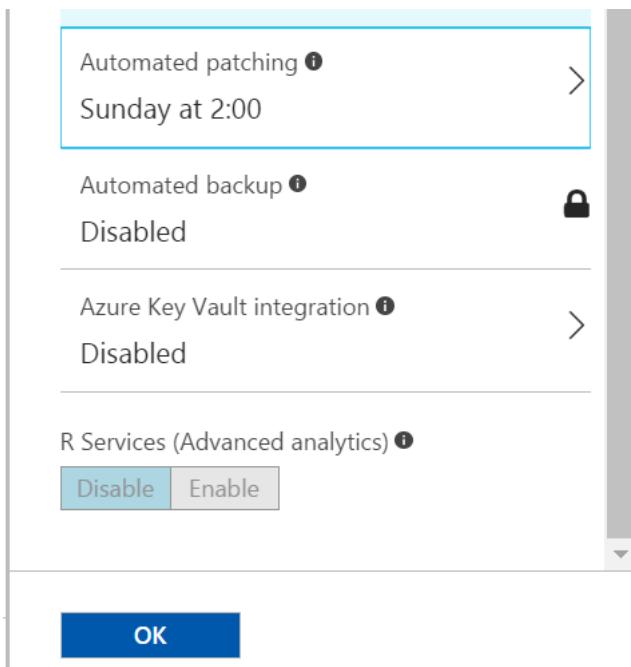
31. In **SQL Server settings** blade, you are given number of specific settings for SQL Server. It is different from a general virtual machine you created in *Lab 06*.
32. Select **Private (within Virtual Network)** option under **SQL connectivity** setting. We do not expose the SQL Server to the Internet.
33. By default, SQL Server listens on port 1433. You can keep it by default.
34. Select **Enable** under **SQL Authentication** setting. We will need to log into SQL Server instance for several initial permission configurations.
35. Enter login name and password under **Login name** and **Password** settings.



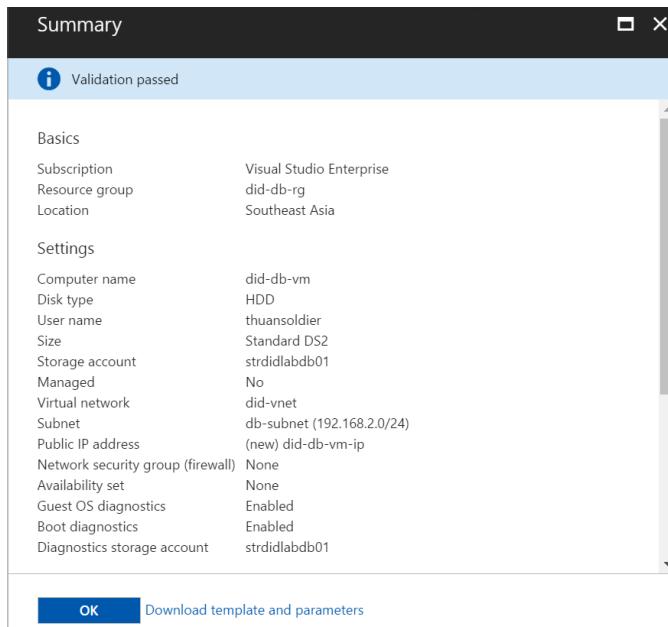
36. Click **Storage configuration** to see given offering from Microsoft. By default, you are given 1 TB. Under **Storage optimization** setting, keep **General** setting by default.



37. Keep Automated patching by default at **Sunday at 2 PM**
38. Keep **Automated backup**, **Azure Key Vault integration** and **R Services** settings by default.
39. Click **OK**.



40. In Summary blade, review your configuration again. Make sure the new SQL Server virtual machine is associated to **did-db-rg** **resource** group. Its name is **did-db-vm**. Storage account is **strdidlabdb01**. The virtual machine needs to be in **did-vnet** virtual network and is associated to **db-subnet**.
41. Click **OK** to start provisioning the virtual machine.



42. Wait around 5-10 minutes to complete provisioning an SQL Server virtual machine.

NAME	STATUS	RESOURCE GROUP
did-ad-vm	Running	did-ad-rg
did-db-vm	Running	did-db-rg

43. Connect to the new SQL Server virtual machine to test if it is successfully provisioned and is manageable (Follow step 1 – 8 in *Lab 07* if you are not still familiar with virtual machine RDP).

Now you have completed this lab.

## Lab 1.10 – Joining SQL Server to the domain controller

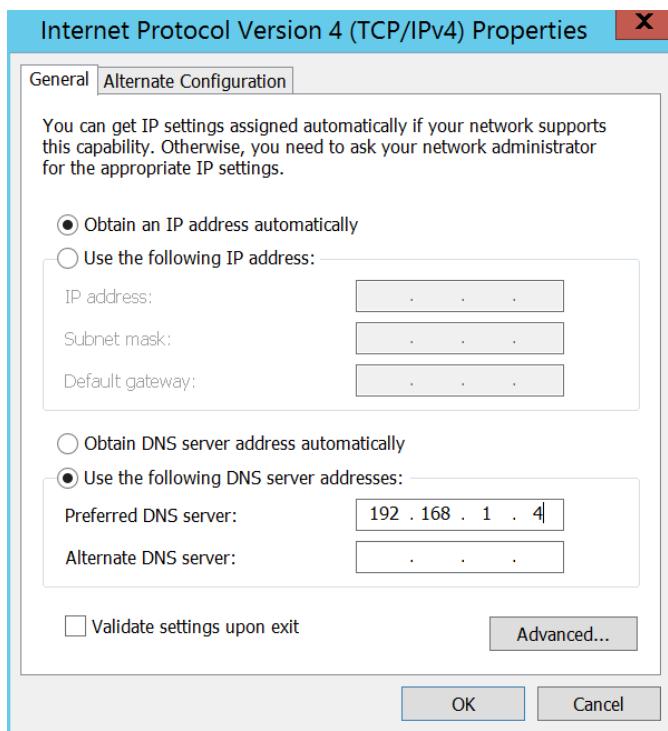
This lab is going to quickly walk you through steps to join the new SQL Server virtual machine to the domain controller.

Perform the following steps to complete the lab:

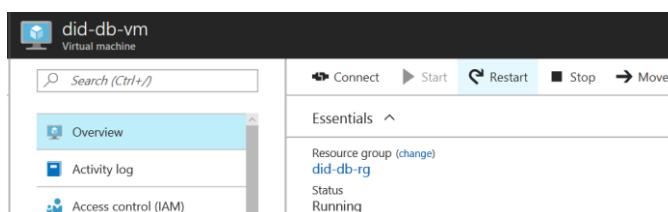
1. RDP to your SQL Server virtual machine.
2. You need to set the IP address of the DNS server for the new SQL Server virtual machine. The DNS server's IP address is the one of

Active Directory virtual machine because we used the same virtual machine for DNS role.

3. Click **OK**.



4. After you click **OK**. You will lose the RDP connection because your virtual machine's DNS IP address is no longer assigned dynamically by Microsoft Azure. In this case, to make the change effective, you need to restart the virtual machine.
5. **Restart** button is close to **Connect** button you are familiar with.

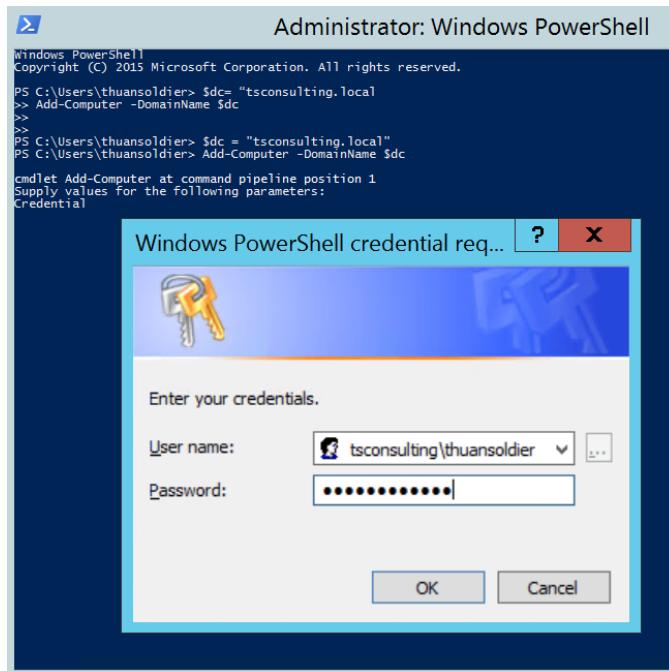


6. RDP again to the virtual machine.

- Follow step 1 – 3 in Lab 08 to open PowerShell. If PowerShell icon is not added to Task bar yet, press **Windows (icon) + R** and type **PowerShell**.
- Type the following command line by line and press **Enter**.

```
$dc= "tsconsulting.local"
Add-Computer -DomainName $dc
```

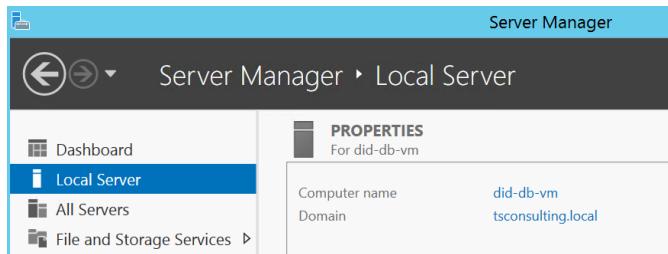
- A credential login popup opens. Type the domain administrator account and password (use the password you set from step 23 in **Lab 1.7**)



- After the configuration is successfully applied. You do need to restart your computer. You can do by following step 5 in this lab or running **Restart-Computer** command.

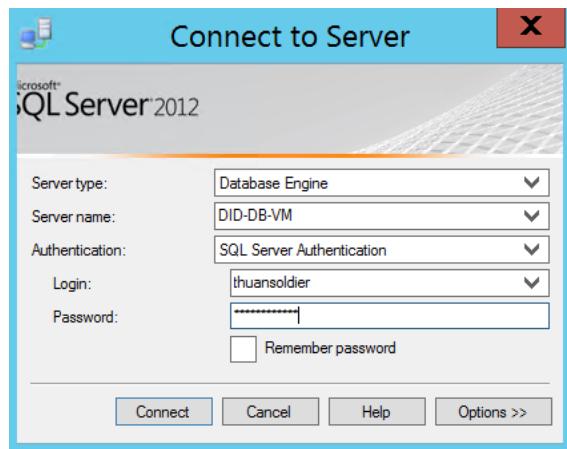
```
$dc= "tsconsulting.local"
Add-Computer -DomainName $dc
cmdlet Add-Computer at command pipeline position 1
Supply values for the following parameters:
Credential
WARNING: The changes will take effect after you restart the computer did-db-vm.
PS C:\Users\thuansoldier> Restart-Computer -
```

11. RDP to your virtual machine using the domain administrator account (`tsconsulting\thuansoldier`) to verify.

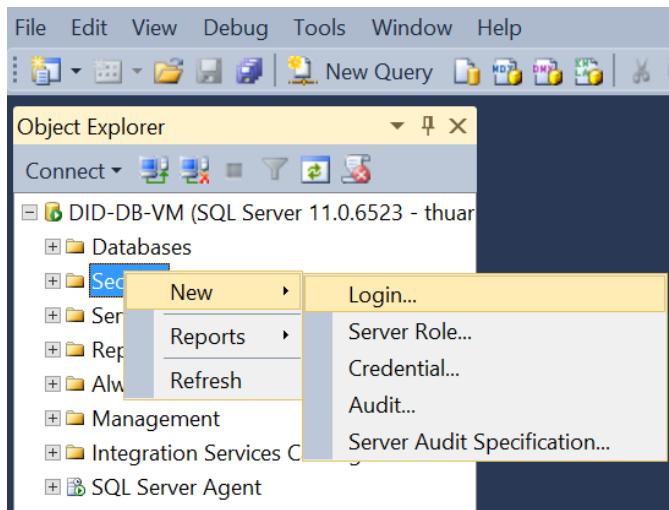


12. Log off the virtual machine and RDP again using the local account.
13. Open SQL Server Management Studio in the database virtual machine and log into the SQL Server using the account you specified from step 11 in *Lab 09*.

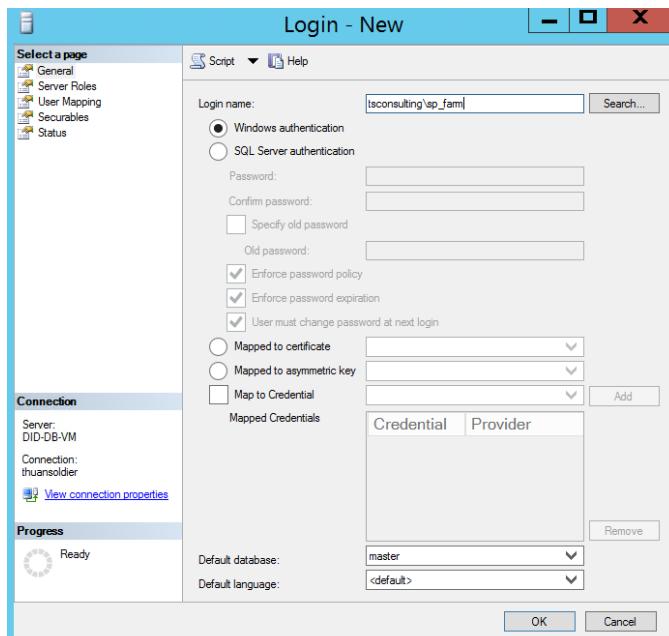
14. Click **Connect**.



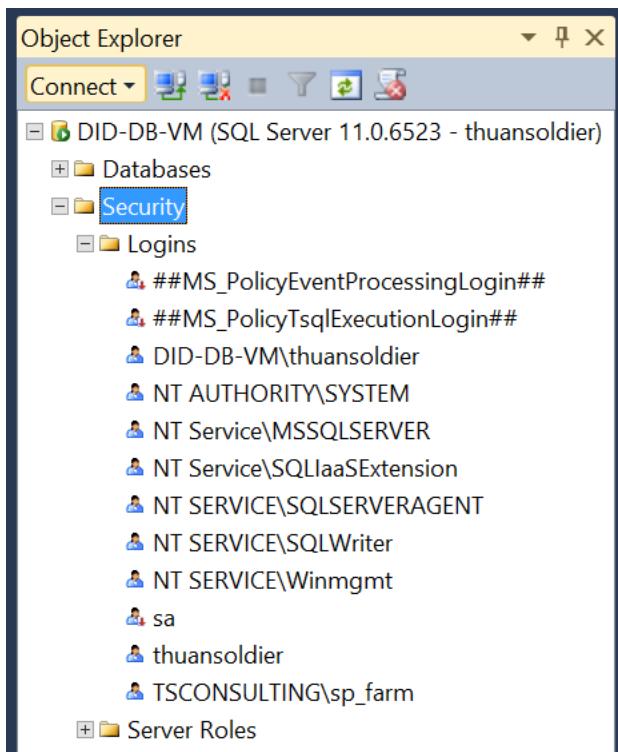
15. Right click on **Security**. Select **New**. Select **Login...**



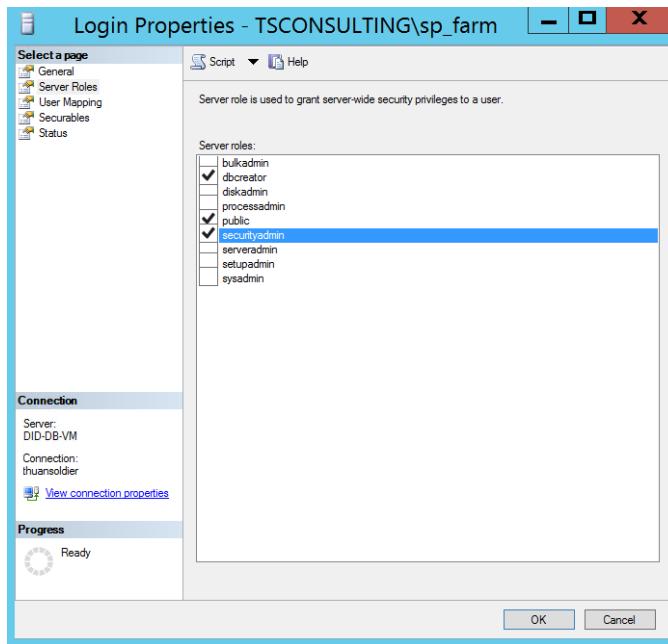
16. In **Login – New** windows, from **General** tab, enter the SharePoint farm account you created in *Lab 08*. In this step, we need to add `sp_farm` to SQL Server instance which will be used to host SharePoint databases. This account also need to have two SQL Server roles: **dbcreator** and **securityadmin**.
17. Keep other settings by default



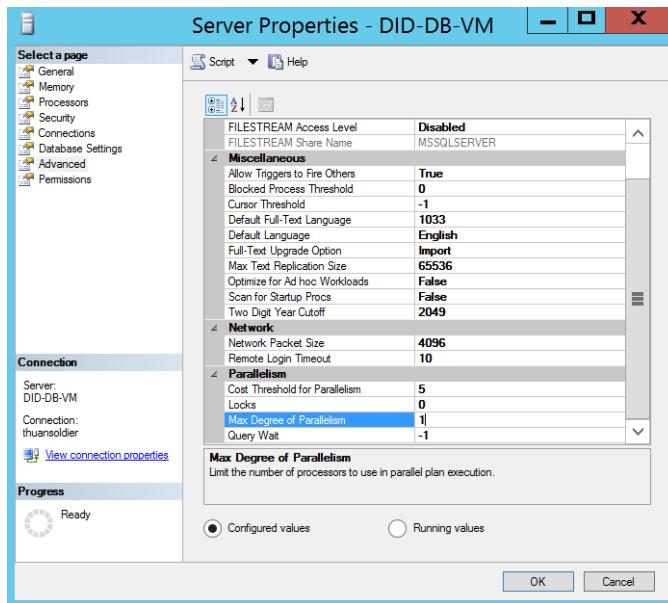
18. From **Security** tree, expand the **Logins** and double click on the newly added account (**tsconsulting\sp\_farm**)



19. Under **Select a page**, click **Server Roles**.  
20. Select **dbcreator** and **securityadmin** roles.  
21. Click **OK**.



22. Right click on the database instance and select **Properties**.
23. In **Server Properties** windows, under **Select a page**, click **Advanced**.
24. Scroll down to look for the setting of **Max Degree of Parallelism**.
25. Change the value from **0** to **1**.
26. Click **OK**.



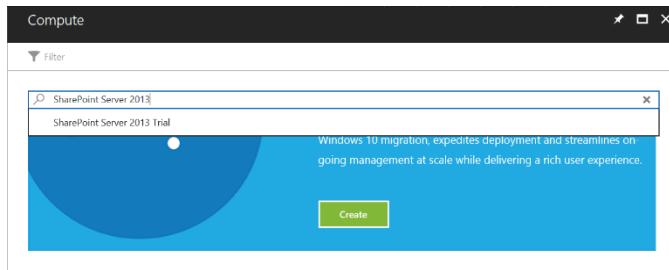
Now you have completed this lab. We will use the `sp_farm` to configure SharePoint farm later.

## Lab 1.11 – Creating two SharePoint Server 2013 virtual machines

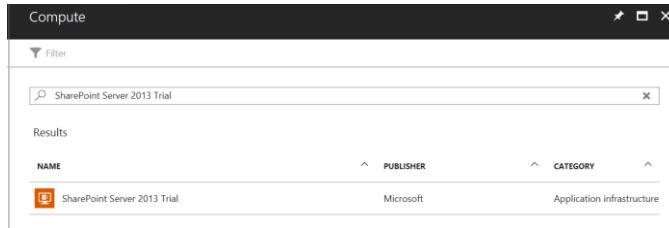
We have successfully provisioned two virtual machines: Active Directory and SQL Server. Each virtual machine is associated to corresponding subnet and storage account. This lab is going to walk you through steps to provision a SharePoint Server 2013 virtual machine from Microsoft Azure Image Gallery.

Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual machines**
3. Click **Add**.
4. On the **Compute** blade, search for SharePoint Server 2013 from *Search Compute* search box. There is an auto-generated drop-down list of **SharePoint Server 2013 Trial** image. Select it.

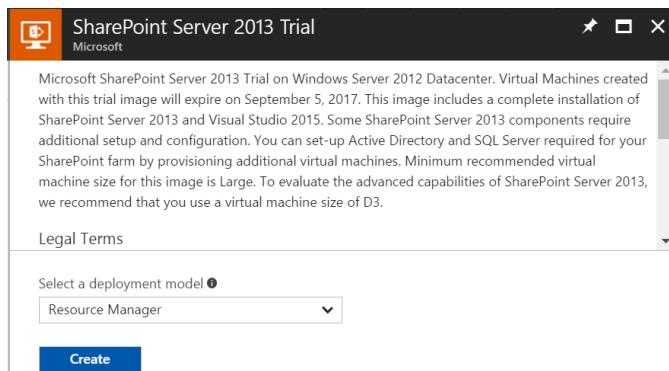


5. There is only one version after you select the image.

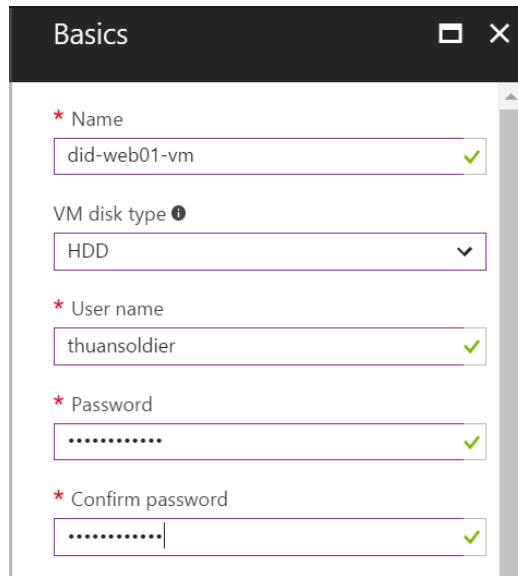


6. On **SharePoint Server 2013 Trial** blade, make sure the deployment model is **Resource Manager**. This model is commonly recommended for the new fresh deployment. Classic model is will be soon deprecated.

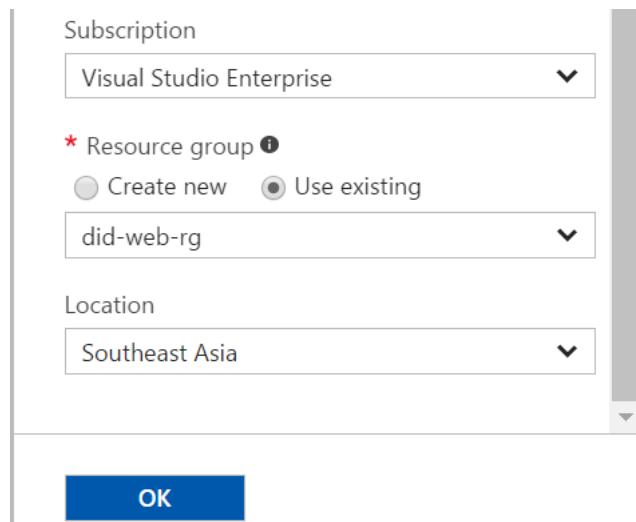
7. Click **Create**.



8. On the **Basics** blade, enter the name for the virtual machine. In this case, we name **did-web01-vm**.
9. Select **HDD** under **VM disk type** setting.
10. Enter the username of the local account you will use to log into after creating the virtual machine.
11. Enter the password. This must follow password complexity.

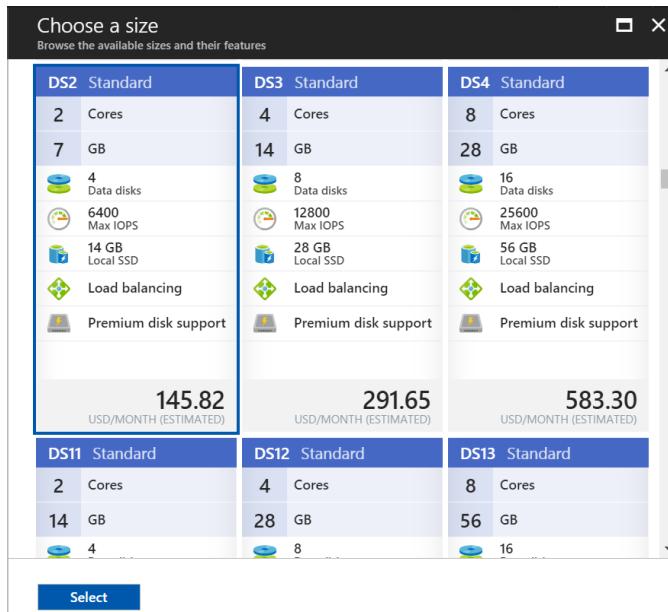


12. Select your subscription under **Subscription** setting.
13. Select **Use existing** under **Resource group** setting. From the drop-down list, select **did-web-rg** because your virtual machine will be put into this resource group.
14. Select your location under **Location**.
15. Click **OK**.

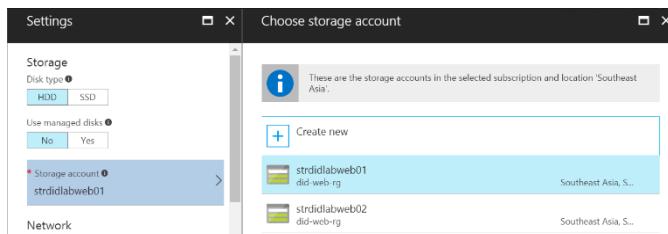


16. On the **Choose a size** blade, select the virtual machine size for you're the first web front-end virtual machine. Click **View all** to

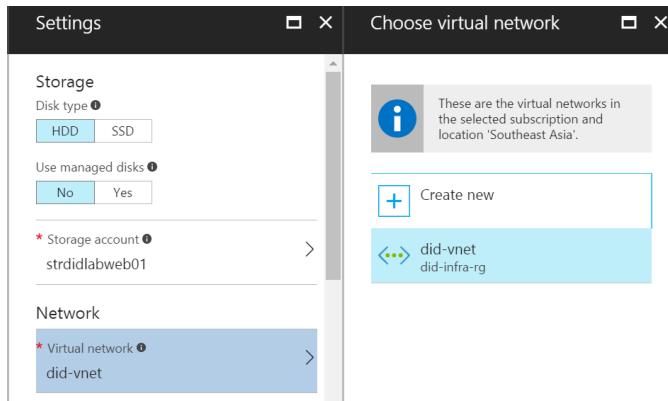
see all options. For testing, look for **Standard\_DS2** size. Click **Select**.



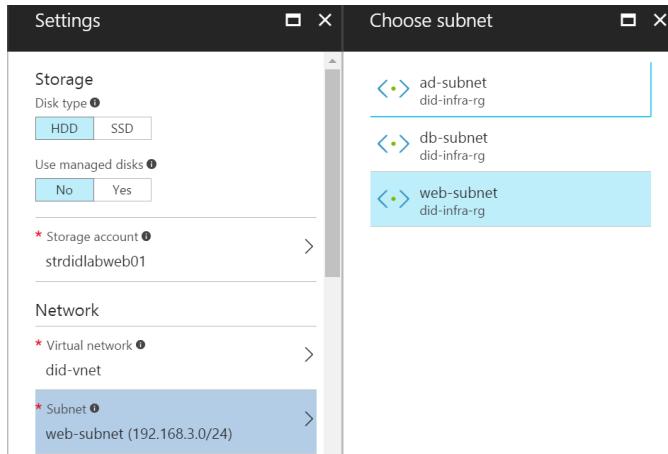
17. On the **Settings** blade, you may see the warning information about Premium disk supportability. Ignore this message while we are testing only.
18. Select **HDD** under **Disk type** setting
19. Select **No** under **Use managed disks** setting.
20. Select the storage account we created for your database virtual machine. It's **strdidlabweb01** (refer to *Lab 02*).



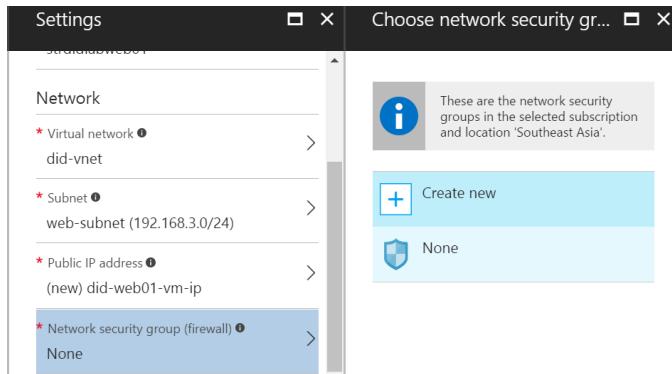
21. Click **Virtual network** and select the virtual network you created in **Lab 1.3**. It is **did-vnet**.



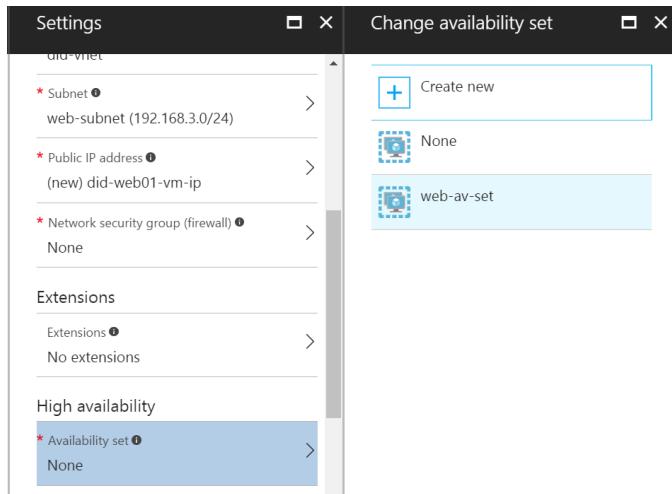
22. Click **Subnet** and select **web-subnet** we created in *Lab 04*



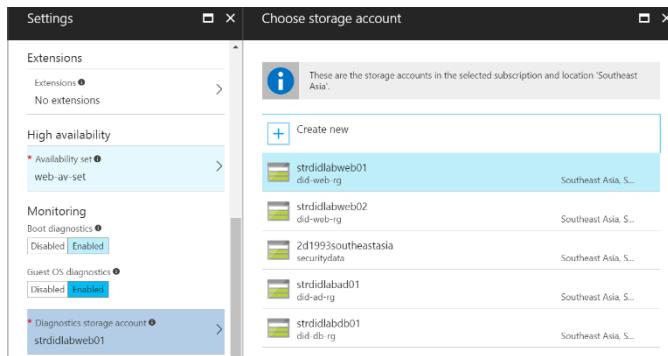
23. Keep **Public IP address** setting by default if Azure has already created a public IP address for you. We initially need it to remotely connect to configure the SQL Server virtual machine
24. Click **Network security group (firewall)** setting and select **None**. We will practice soon in the next few labs.



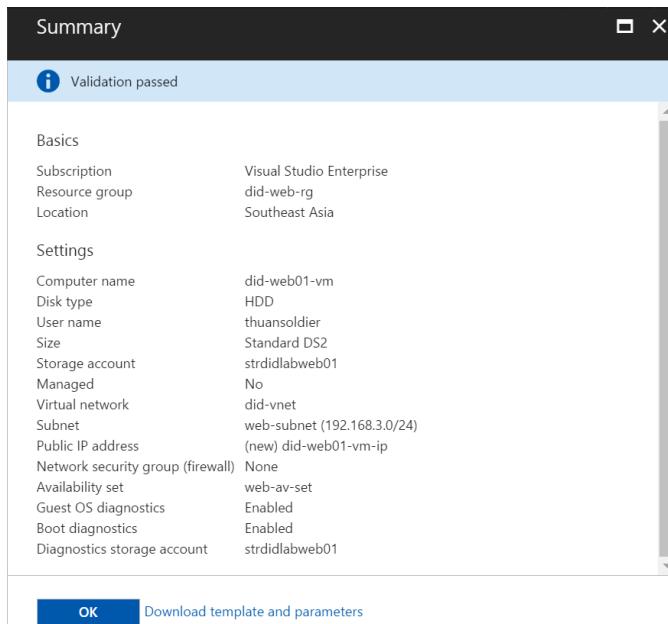
25. Keep **Extensions** setting by default with no extension. We will manually add Microsoft Antimalware extension later.
26. Click **High availability** setting. Select **web-av-set** we created in **Lab 1.5**.



27. Select **Enabled** under **Boot diagnostics**.
28. Select **Enabled** under **Guest OS diagnostics**.
29. Under **Diagnostics storage account** setting, select **strdidlabweb01**
30. Click **OK**.

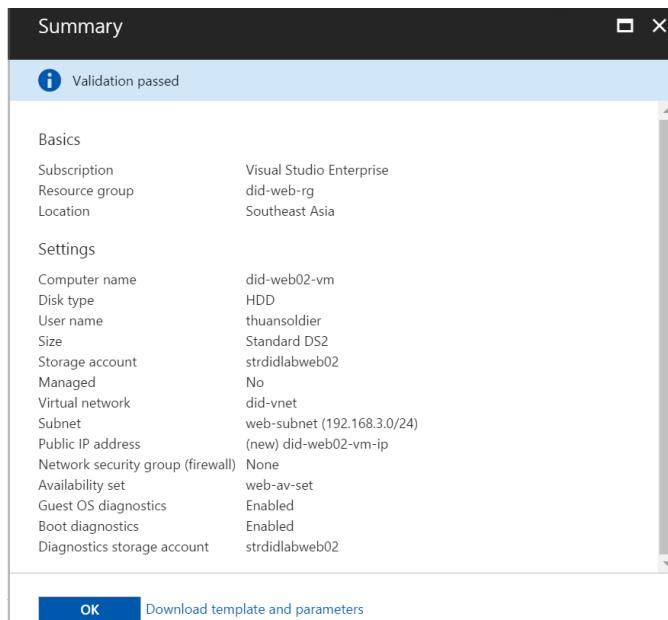


31. On the **Summary** blade, review your configuration again. Make sure the first SharePoint Server 2013 virtual machine is associated to **did-web-rg** resource group. Its name is **did-web01-vm**. Storage account is **strididlabweb01**. The virtual machine needs to be in **did-vnet** virtual network and is associated to **web-subnet**. The virtual machine will be in **web-av-set** availability set.
32. Click **OK** to start provisioning the virtual machine.



33. Wait around 5-10 minutes to complete provisioning a SharePoint Server 2013 virtual machine.
34. Repeat from step 1 – 32 again for the second SharePoint Server 2013 virtual machine. The two differences are the virtual machine

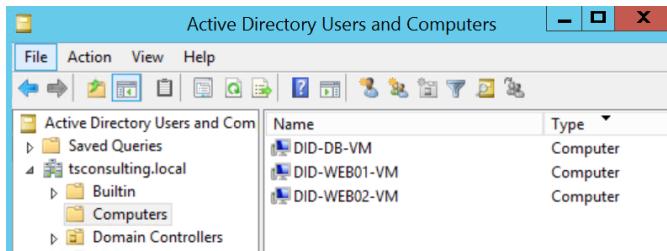
name and storage account. Other settings should be the same with the first web front-end virtual machine.



35. Go to verify four virtual machines you created. Note that each of the virtual machine is correctly associated to a resource group.

NAME	STATUS	RESOURCE GROUP
did-ad-vm	Running	did-ad-rg
did-db-vm	Running	did-db-rg
did-web01-vm	Running	did-web-rg
did-web02-vm	Running	did-web-rg

36. RDP to each web front-end virtual machines to join to the domain controller. You need to follow the steps in Lab 10 exactly from setting up IP address, restarting virtual machines and running the PowerShell script to join to the domain controller.
37. RDP to **did-ad-vm** to verify all 3 virtual machines to be joined to the domain controller.
38. Open **Active Directory Users and Computers**. (Refer to step 8 and 9 in **Lab 1.8**).
39. Expand the domain. Click **Computers**. There are three clients that are already in the domain controller.



Now you have completed this lab.

## Lab 1.12 – Provisioning and configuring SharePoint Server 2013 farm

This is the final lab in the series of labs of building a SharePoint Server 2013 farm for testing. We assume this farm is the main target of attacker from the Internet that we need to protect. This lab is going to walk you through steps to configure create a SharePoint Server 2013 farm and add the second web front-end to the farm.

---

Before this lab, you need to grant Remote Desktop privilege for **sp\_farm** and **sp\_admin** account. These accounts also need to be added to the local Administrator group on both web front-end virtual machines

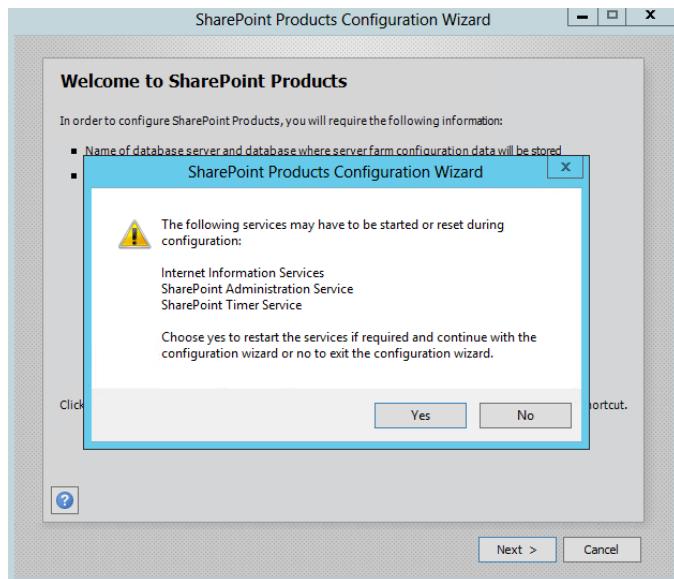
---

Perform the following steps to complete the lab:

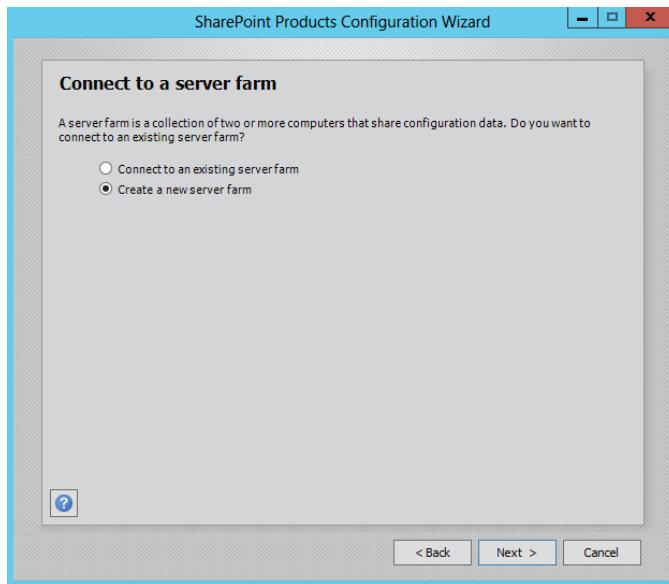
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual machines**
3. Click **did-web01-wm**
4. Connect to this virtual machine and log into it using **sp\_farm** account. Make sure you enter domain name, namely *tsconsulting\sp\_farm*
5. Click **Start** icon at the bottom left corner and search for SharePoint



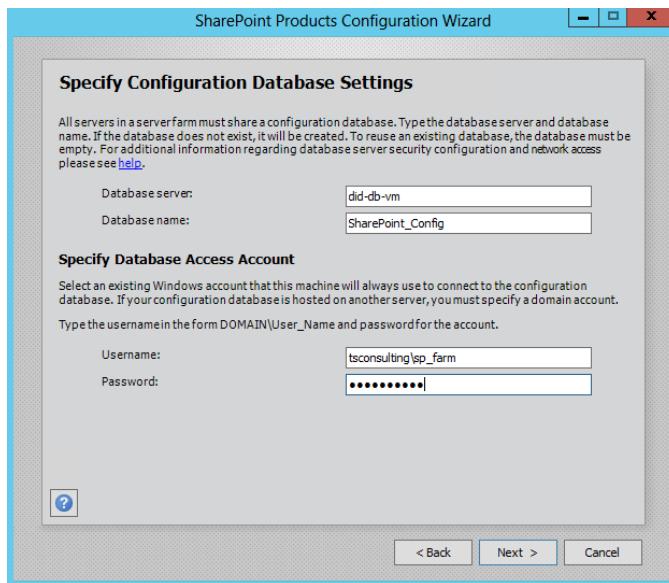
6. Click **SharePoint 2013 Products Configuration Wizard**.
7. In **Welcome to SharePoint Products** page, click **Next**. You are asked to confirm to restart three services before SharePoint farm configuration. Click **Yes**.



8. In **Connect to a server farm** page, select **Create a new server farm**.
9. Click **Next**.



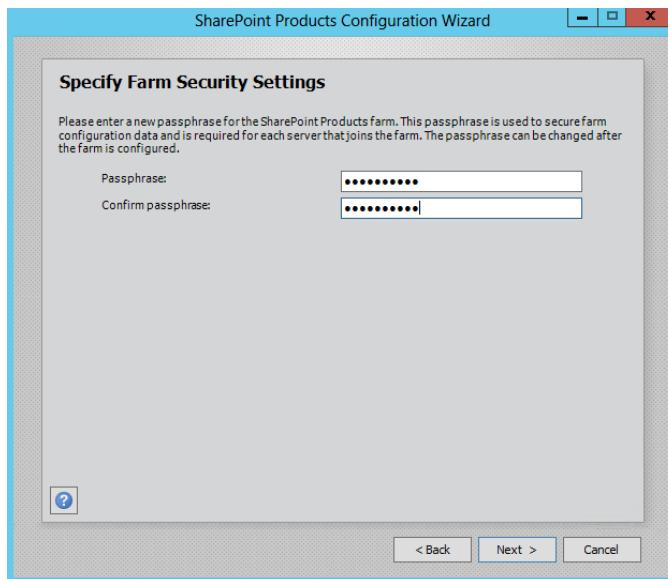
10. In **Specify Configuration Database Settings** page, enter your database virtual machine name in **Database server** box. Enter **sp\_farm** account in **Username** and **Password** boxes.
11. Click **Next**.



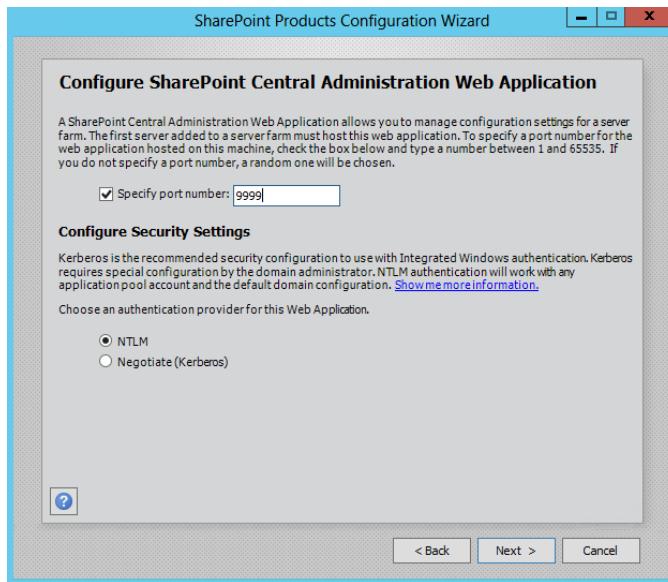
12. In **Specify Farm Security Settings** page, type passphrase and remember it. You will need it to add the second web front-end

virtual machine to the SharePoint farm. The passphrase must follow password complexity.

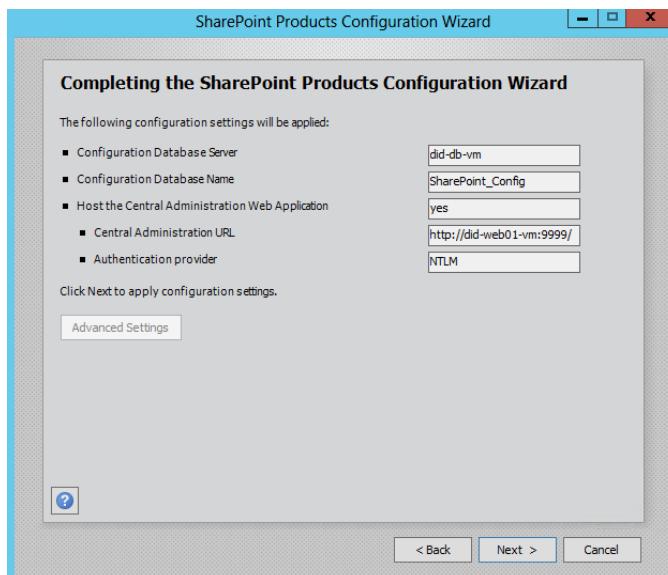
13. Click **Next**.



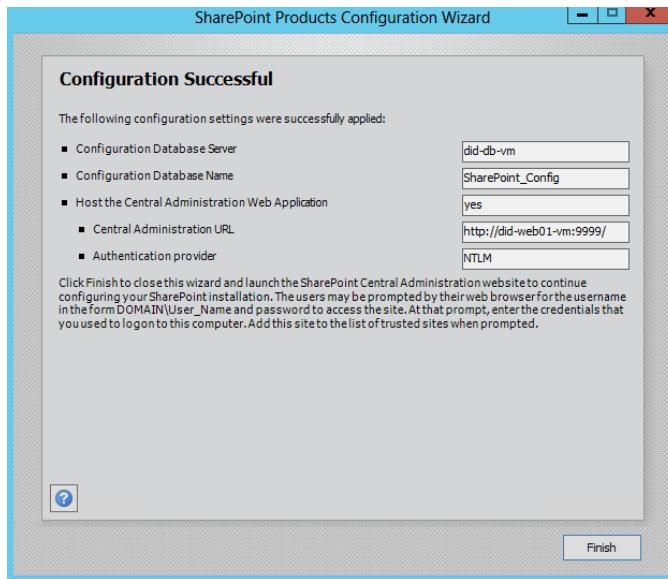
14. In **Configure SharePoint Central Administration Web Application** page, select **Specify port number** and enter **9999**. Well, the number does not have to be four-nine. I just wanted to make sure this number is memorable for further test if you need. For example, blocking HTTP request on port 9999 to your Central Administration site from the jump virtual machine.
15. Keep the authentication provider with **NTLM** option selected.
16. Click **Next**.



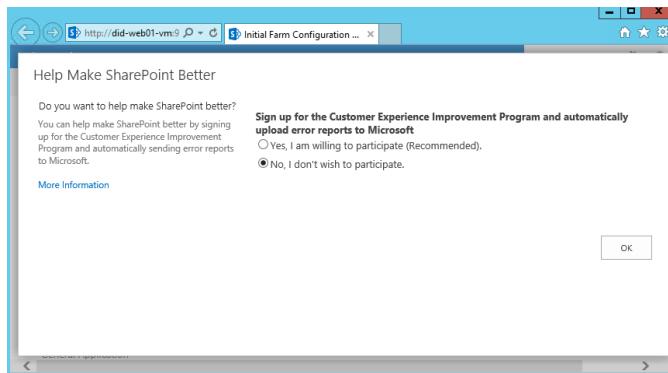
17. In **Completing the SharePoint Products Configuration Wizard** page, review all configuration values again.
18. Click **Next**.



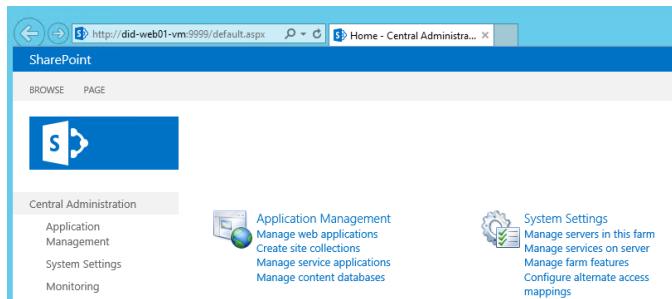
19. In **Configuration Successful** page, review information again. You now have finished creating a new SharePoint farm.
20. Click **Finish**



21. The Central Administration website is automatically opened.
22. Select **No, I don't wish to participate**.
23. Click **OK**.



24. From the Central Administration website (the URL is *http://did-web01-vm:9999* if you follow and use the same configuration), click **Manage web application** under **Application Management**.



Now you have completed this lab.

## Lab 1.13 – Adding the second web front-end virtual machine

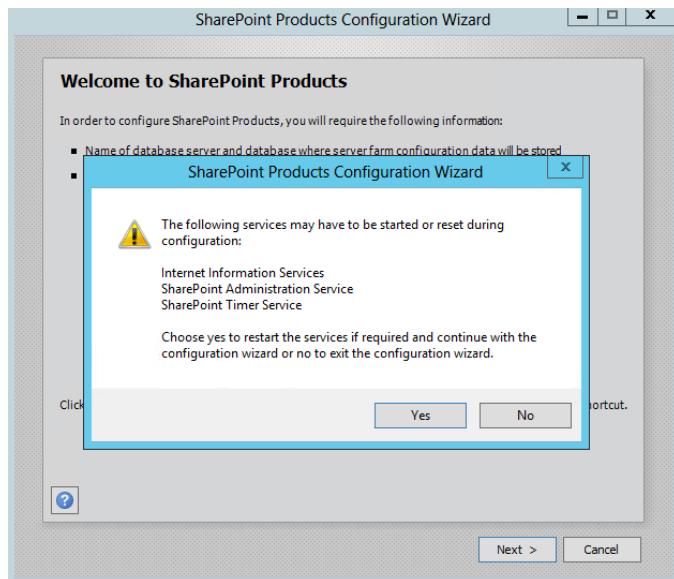
As planned from the beginning, there are two web front-end virtual machines in your SharePoint farm hosted on Microsoft Azure. We will configure internal Azure Load Balancer later in the Hands-On Lab to experiment network availability which is part of the CIA triad. This lab is going to walk you through steps to add the second web front-end virtual machine to the existing SharePoint farm you successfully provisioned in *Lab 12*.

Perform the following steps to complete this lab:

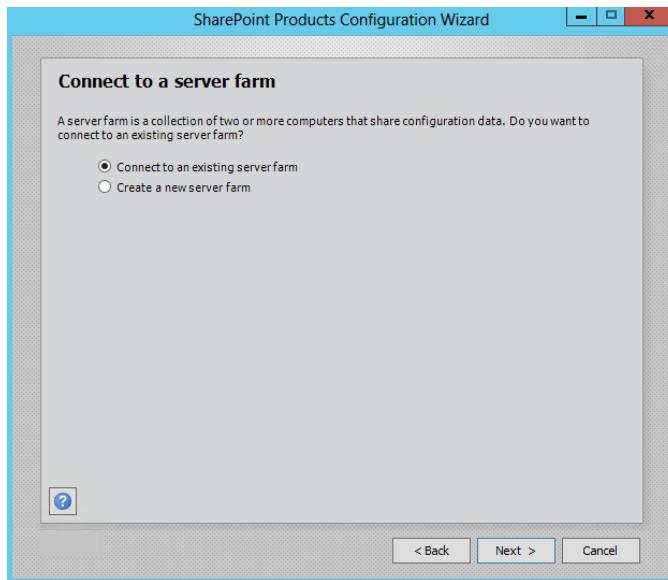
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual machines**
3. Click **did-web02-wm**. This is the second web front-end virtual machine you created in *Lab 11*.
4. Connect to this virtual machine and log into it using `sp_farm` account. Make sure you enter domain name, namely `tsconsulting\sp_farm`. Make sure you already added this account to Remote Desktop User and local Administrator group.
5. Click **Start** icon at the bottom left corner and search for SharePoint



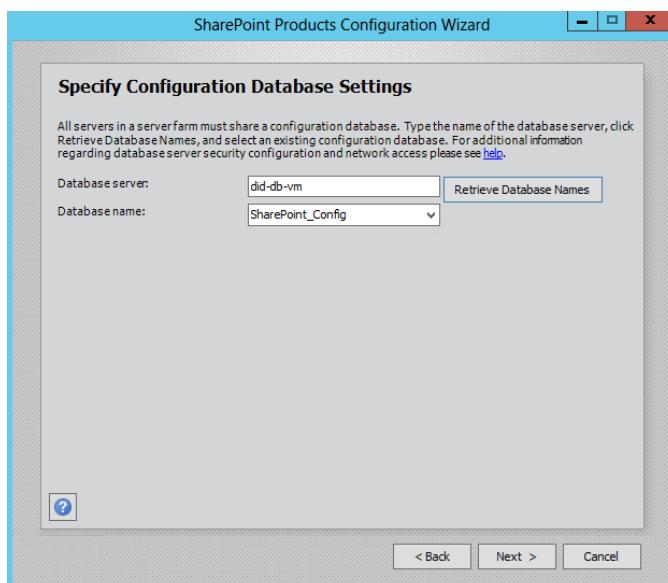
6. Click **SharePoint 2013 Products Configuration Wizard**.
7. In **Welcome to SharePoint Products** page, click **Next**. You are asked to confirm to restart three services before SharePoint farm configuration. Click **Yes**.



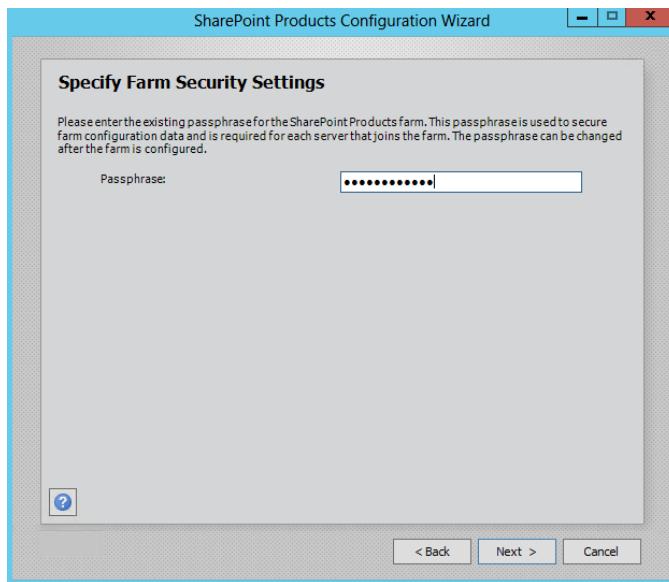
8. In **Connect to a server farm** page, select **Connect to an existing server farm**.
9. Click **Next**.



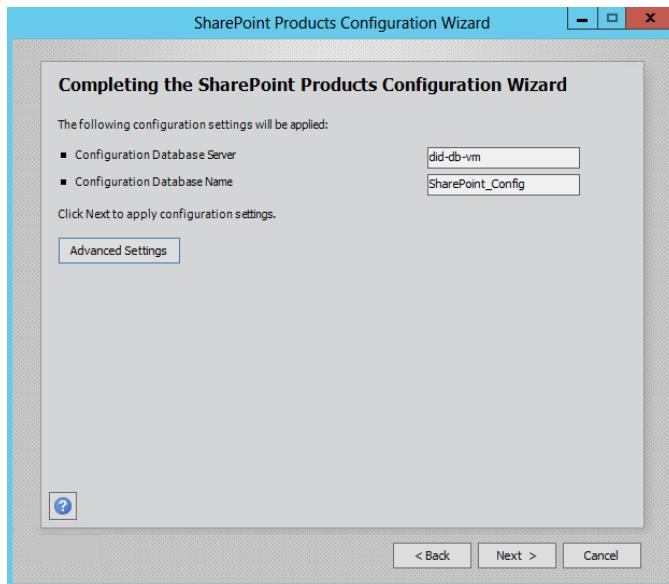
10. In **Specify Configuration Database Settings** page, enter the database virtual machine name and click **Retrieve Database Names**. The **SharePoint\_Config** database is automatically populated.
11. Click **Next**.



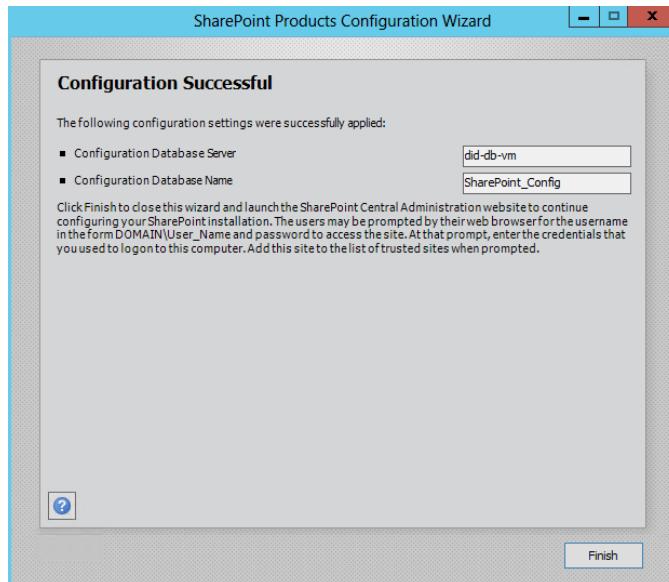
12. In **Specify Farm Security Settings** page, enter the passphrase you set from step 13 in *Lab 12*.
13. Click **Next**.



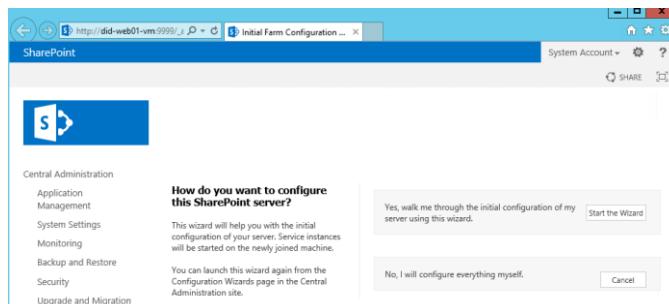
14. In **Completing the SharePoint Products Configuration Wizard** page, click **Next**. Keep advanced settings by default.



15. In **Configuring SharePoint Products** page, wait around 5-10 minutes until the process is completed.
16. In **Configuration Successful** page, click **Finish**.



17. The browser automatically opens your **Central Administration** website. Click **Cancel** at the option of “**No, I will configure everything myself**”.



Now you have completed this lab.

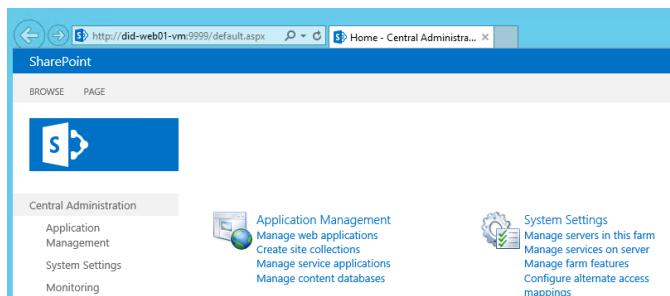
## Lab 1.14 – Creating a SharePoint website

This is the final lab in the series of creating a base SharePoint farm before you can practice with Azure features we explored in the book to product your system. Although the SharePoint farm is provisioned successfully, you

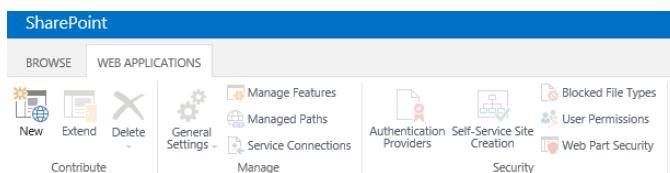
still have not created any website for internet-facing testing yet. This lab is going to walk you through steps to create a SharePoint website and publish it over the Internet so you can access your SharePoint site from the Internet. We will also configure Azure Load Balancer to distribute network traffic to this internet-facing website across the web front-end virtual machines.

Perform the following steps to complete this lab:

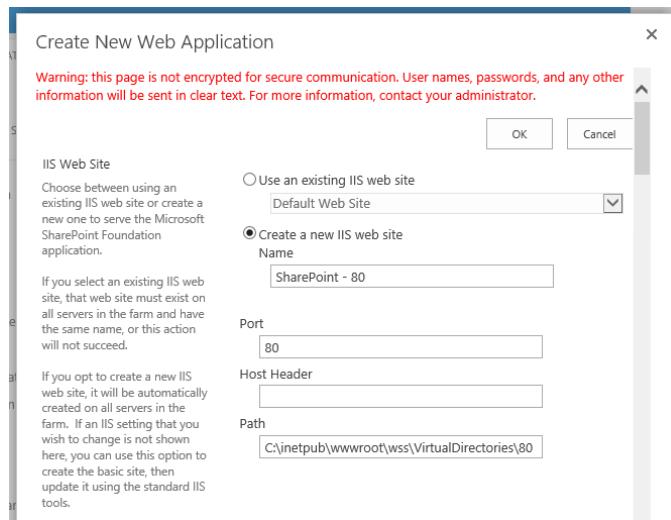
1. From the Central Administration website (the URL is `http://did-web01-vm:9999` if you use the same variables during the lab).
2. Under **Application Management**, click **Manage web applications**.



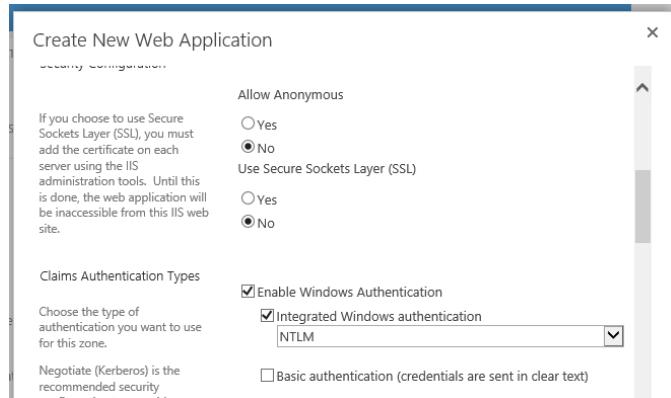
3. In the Ribbon, click **New**.



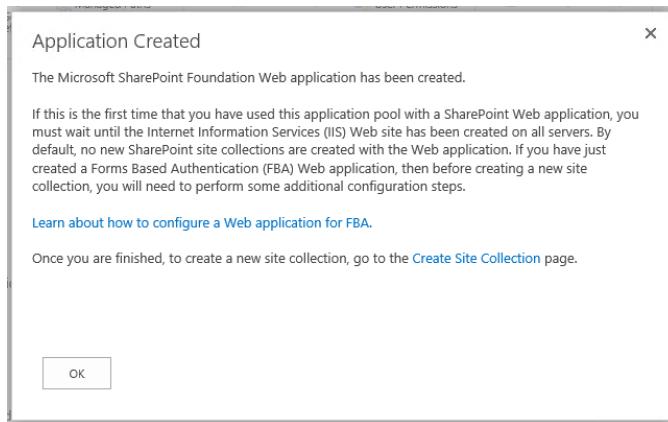
4. Enter the web application name under **Create a new IIS web site**. You can keep it by default.
5. Under **Port**, keep the value **80** by default.
6. Keep **Path** by default.



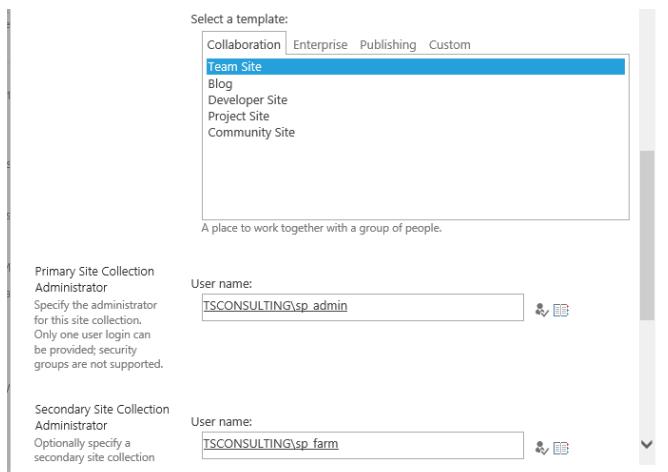
7. Select **Yes** under **Allow Anonymous** setting because the website is intentionally configured as an internet-facing website.
8. Select **No** under **Use Secure Sockets Layer (SSL)**. In production environment, it is recommended to use SSL. However, this book does not focus on web application security.
9. Make sure **Enable Windows Authentication** and **Integrated Windows authentication with NTLM** are selected.



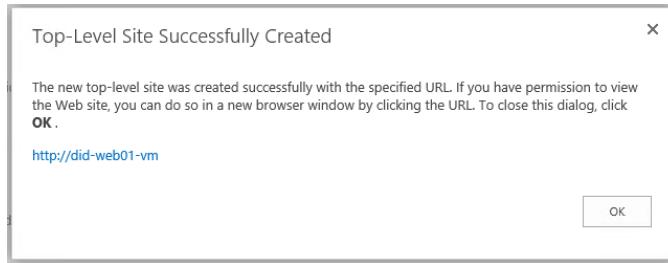
10. Keep all other settings by default. If anything we need to change, we can do later via Central Administration. Click **OK**.
11. In **Application Created** page, click **Create Site Collection** link.



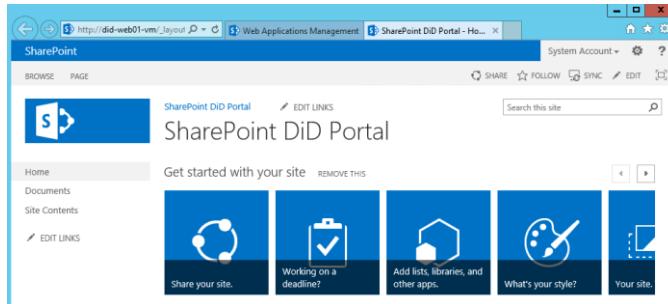
12. In **Create Site Collection** page, under the **Title** enter the site collection title (e.g. SharePoint DiD Portal).
13. Keep the URL by default.
14. Keep **2013** under **Select experience version** setting. Under **Select a template** setting, select **Team Site**.
15. Enter `sp_admin` as the primary site collection administrator and `sp_farm` as a secondary one.
16. Keep **No Quota** by default.
17. Click **OK**.



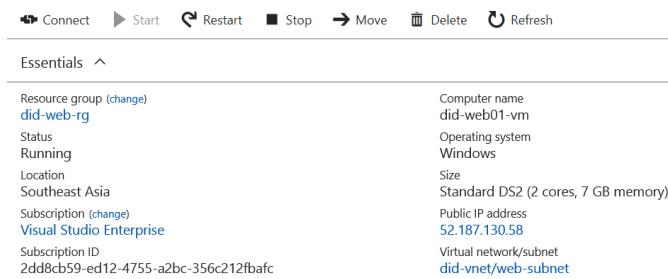
18. In **Top-Level Site Successfully Created** page, click your new site collection URL to verify.



19. If you see the following screen, congratulation on being successful.



20. Go to your Azure Management Portal. Click one web front-end virtual machine to check its public IP address under **Public IP address** setting.



21. Go to your Central Administration website inside a web front-end virtual machine. Click **Application Management**. Click **Configure alternate access mappings** under **Web Applications**.



## Application Management

Central Administration  
Application Management

System Settings  
Monitoring  
Backup and Restore  
Security



### Web Applications

Manage web applications | Configure alternate access mappings



### Site Collections

Create site collections | Delete a site collection | Confirm site use and deletion | Specify quota templates | Configure quotas and locks | Change site collection administrators | View all site collections | Configure self-service site creation

## 22. In **Alternate Access Mappings** page, click **Edit Public URLs**

### Alternate Access Mappings

Edit Public URLs   Add Internal URLs   Map to External Resource		
Alternate Access Mapping Collection: Show All ▾		
Internal URL	Zone	Public URL for Zone
<a href="http://did-web01-vm:9999">http://did-web01-vm:9999</a>	Default	<a href="http://did-web01-vm:9999">http://did-web01-vm:9999</a>
<a href="http://did-web01-vm">http://did-web01-vm</a>	Default	<a href="http://did-web01-vm">http://did-web01-vm</a>

## 23. From the list of Alternate Access Mapping Collection, click **No selection**. Click **Change Alternate Access Mapping Collection** then select your web application. It is “SharePoint – 80” you created

### Edit Public Zone URLs

Alternate Access Mapping Collection  
Select an Alternate Access Mapping Collection.

#### Public URLs

Enter the public URL protocol, host, and port to use for this resource in any or all of the zones listed. The Default Zone URL must be defined. It will be used if needed where the public URL for the zone is blank and for administrative actions such as the URLs in Quota e-mail.  
<http://go.microsoft.com/fwlink/?LinkId=114854>

Alternate Access Mapping Collection: **No selection** ▾

Change Alternate Access Mapping Collection

Default

Intranet

Internet

## 24. Enter the public IP address to the **Internet** setting. Make sure to add **HTTP** before the IP address. 25. Click **Save**.

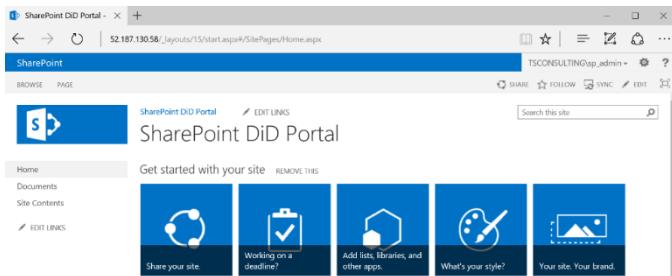
## Edit Public Zone URLs

Alternate Access Mapping Collection  
Select an Alternate Access Mapping Collection.

Public URLs  
Enter the public URL protocol, host, and port to use for this resource in any or all of the zones listed. The Default Zone URL must be defined. It will be used if needed where the public URL for the zone is blank and for administrative actions such as the URLs in Quota e-mail.  
<http://go.microsoft.com/fwlink/?LinkId=114854>

Default	<input type="text" value="http://did-web01-vm"/>
Intranet	<input type="text"/>
Internet	<input type="text" value="http://52.187.130.58"/>
Custom	<input type="text"/>
Extranet	<input type="text"/>

26. Now go to your computer, open browser and try to access using the Internet URL. If the configuration is successful, you are asked to provide username and password to log into the SharePoint website. Use `sp_farm` or `sp_admin` to log in. Make sure to use full domain name (e.g. `tsconsulting\sp_admin`)



Configuration! You have finally finished the SharePoint farm deployment on Microsoft Azure in which you created a virtual network, created several subnet and provisioned virtual machines for each role. You also knew on how to add a new web front-end virtual machine to the existing SharePoint farm. You also did the good job of creating a web application and published the first SharePoint website over the Internet.

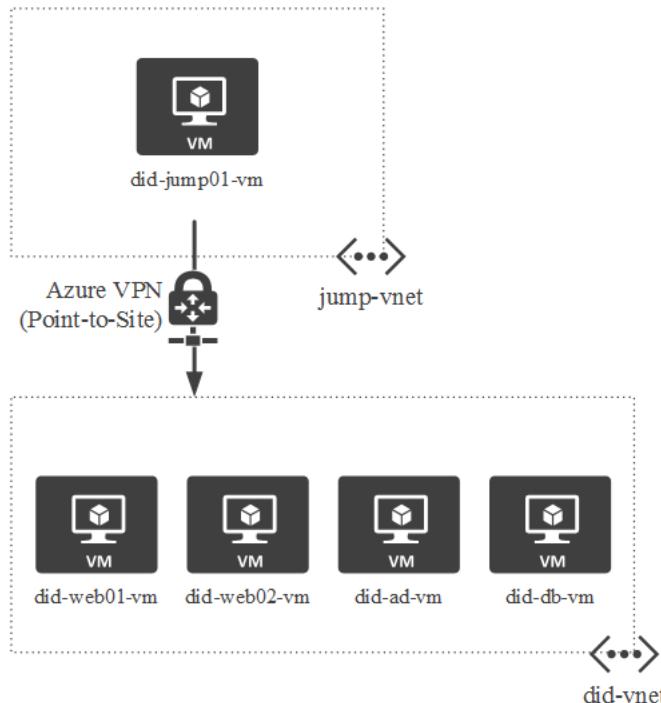
## Lab 2 – Azure Network Security Lab

In Chapter 3, we explored Azure Network Security Group on Microsoft Azure which is helpful for implementing a DMZ-like topology, and for controlling your network traffic. In **Lab 2**, we will practically configure some Azure features to secure your Azure network.

## Lab 2.1 - Setting up a jump virtual machine

Connecting directly through RDP to your system is not recommended in a practical security. It is because the RDP connection goes through the Internet which is weak. To add more extra layer of security, you should set up a jump virtual machine (as known as bastion host) which connects privately to your system via Point-to-site VPN. The illustration below shows you the setup target. In this setup, there is a virtual machine which resides in a different virtual network to connect to your private network. There is a Point-to-site connection between the jump virtual network and your private virtual network to secure the connection.

This lab is going to walk you through steps to do provision a new virtual machine running on a dedicated virtual network.



Perform the following steps to complete the lab:

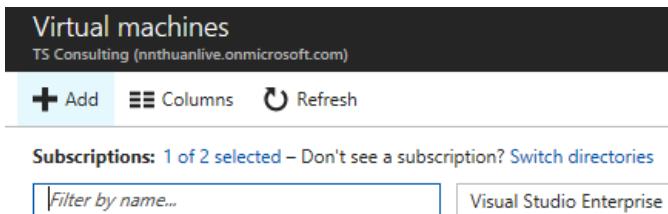
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual machines**
3. On the **Virtual machines**, click **Add**.

Virtual machines  
TS Consulting (n nthuanlive.onmicrosoft.com)

**+** Add   **Columns**   **Refresh**

Subscriptions: 1 of 2 selected – Don't see a subscription? [Switch directories](#)

[Visual Studio Enterprise](#)



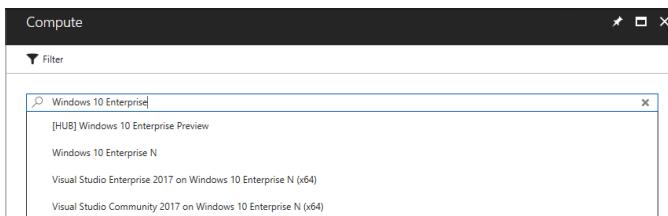
4. Ideally the jump virtual machine should use server core build (e.g. Windows Server 2016 Server Core) to reduce surface attack. This basically means attacker must be good at scripting and PowerShell to use the jump virtual machine to remotely connect to your system in the private network. It is because the GUI is not available in server core build. In this lab, we will focus on simpler thing by choosing Windows 10. On the **Compute** blade, enter **Windows 10 Enterprise** into the search box and select **Windows 10 Enterprise N** from the drop-down list.

Compute

**Filter**

x

- [HUB] Windows 10 Enterprise Preview
- Windows 10 Enterprise N
- Visual Studio Enterprise 2017 on Windows 10 Enterprise N (x64)
- Visual Studio Community 2017 on Windows 10 Enterprise N (x64)



5. On the **Windows 10 Enterprise N** blade, make sure the deployment model is **Resource Manager**.
6. Click **Create**.

Windows 10 Enterprise N

Microsoft

This image contains Windows 10 Enterprise N (x64) (Anniversary Update) and is exclusively available to Visual Studio subscribers. It allows you to easily and quickly set up an environment in Azure to develop and test applications targeting Windows 10. Join the Windows Insider Program (<https://insider.windows.com/>) to receive more frequent, incremental builds of Windows.

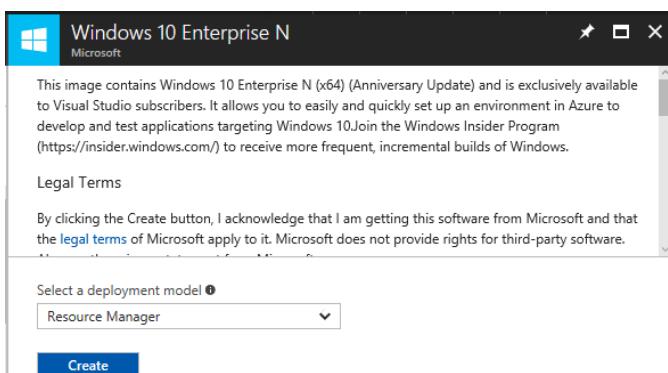
Legal Terms

By clicking the Create button, I acknowledge that I am getting this software from Microsoft and that the [legal terms](#) of Microsoft apply to it. Microsoft does not provide rights for third-party software.

Select a deployment model ?

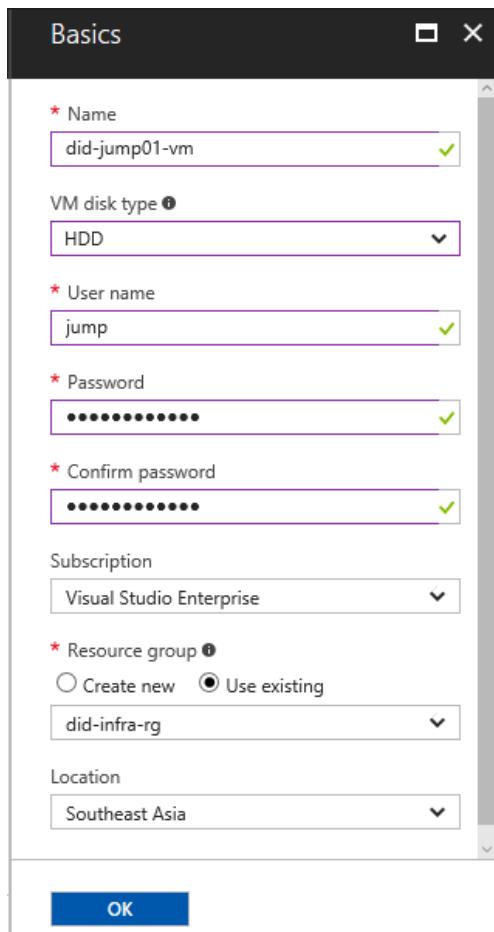
Resource Manager

**Create**

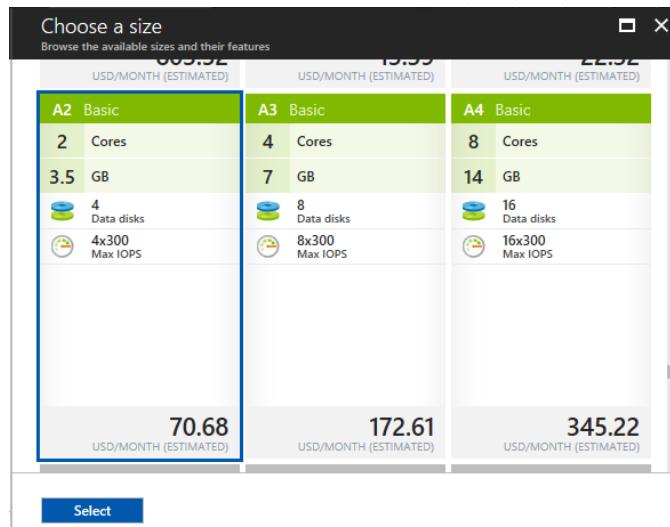


7. On the **Basics** blade, enter the jump virtual machine name.
8. Select **HDD** under **VM disk type** setting.

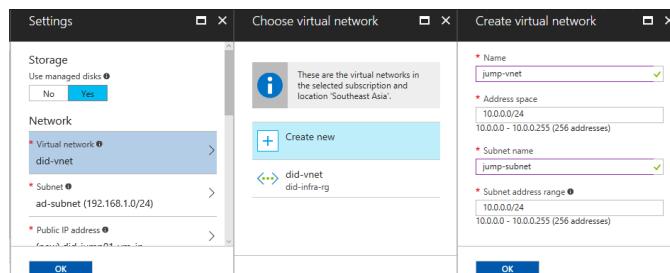
9. Enter username and password for the local administrator account of this virtual machine.
10. Choose the same subscription you did for the base lab.
11. Under **Resource group** setting, select **Use existing** and select **did-infra-rg**
12. Select the location under **Location** setting.
13. Click **OK**.



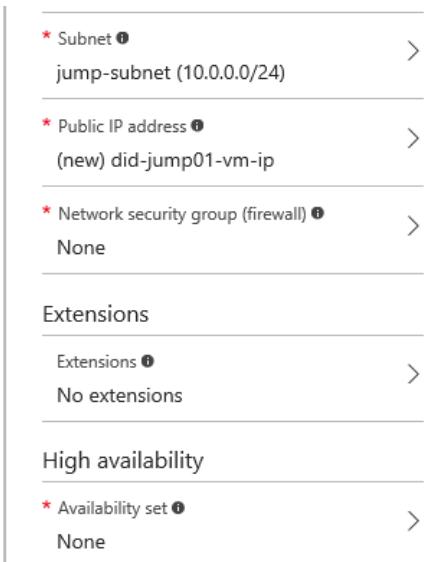
14. On the **Choose a size** blade, click **View all**. Look for **A2 Basic** virtual machine size. Click **Select**.



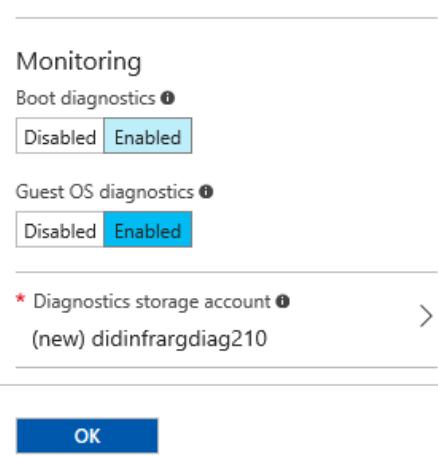
15. On the **Settings** blade, select **Yes** under **Use managed disks**. The reason we choose this setting is because we do not need to manage a storage account for the jump virtual machine. Microsoft Azure helps you manage this disk. If you wish to choose and manage the storage account, select **No**.
16. Click **Virtual network**. Under **Choose virtual network** blade, click **Create new**. Previously you created a new virtual network via virtual network central management portal. However, in this lab you are introduced to way.
17. On the **Create virtual network** blade, enter name of the new virtual network.
18. Keep address space and subnet address range by default if you do not specify your own value. Enter name of the subnet name for your jump virtual machine.
19. Click **OK**.



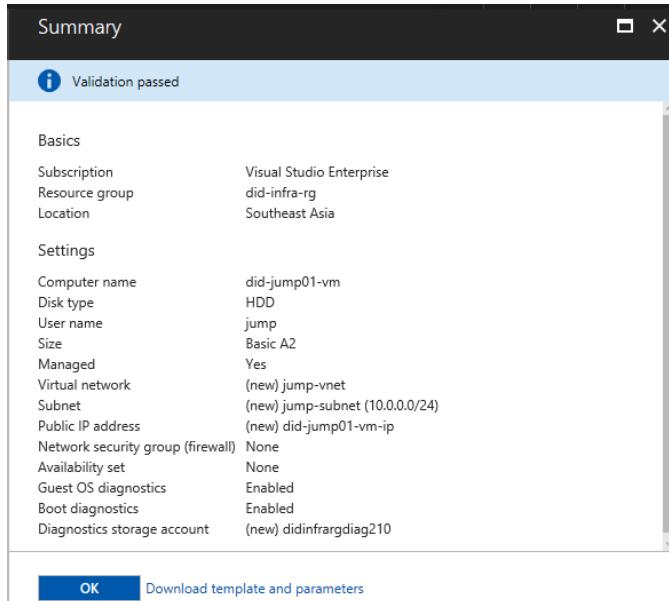
20. Keep the value under Public IP address by default.
21. Click **Network security group (firewall)** setting and select **None**.  
We will manually create a new network security group later.
22. Keep **Extensions** and **High availability** as none by default.



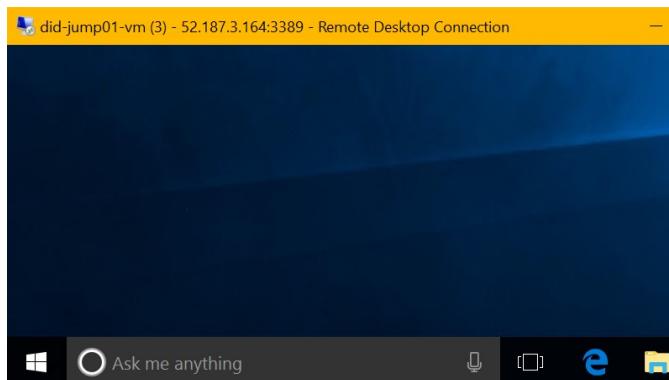
23. Select **Enabled** under **Boot diagnostics** setting.
24. Select **Enabled** under **Guest OS diagnostics** setting.
25. Let Microsoft Azure create a new storage account to store diagnostics log for you.
26. Click **OK**.



27. On the **Summary** blade, review all information again. Make sure this jump virtual machine does not reside in the same private virtual network.
28. Click **OK**.



29. Wait around 5-10 minutes to complete provisioning the jump virtual machine.
30. RDP to the new jump virtual machine to verify.



Now you have completed this lab. We will configure Azure VPN in the next lab.

## Lab 2.2 – Setting up Point-to-site VPN gateway

In **Lab 2.1**, you successfully provision a new jump virtual machine because you are not going to directly RDP to your virtual machines in the private network. You will need to RDP to the jump virtual machine, then be authenticated with Point-to-site VPN gateway before RDP to things in the private network. This lab is going to walk you through step to establish a point-to-site VPN gateway between your jump virtual machine to the private virtual network. This lab is going to walk you through steps to create a new VPN gateway and connect jump virtual machine to the private network.

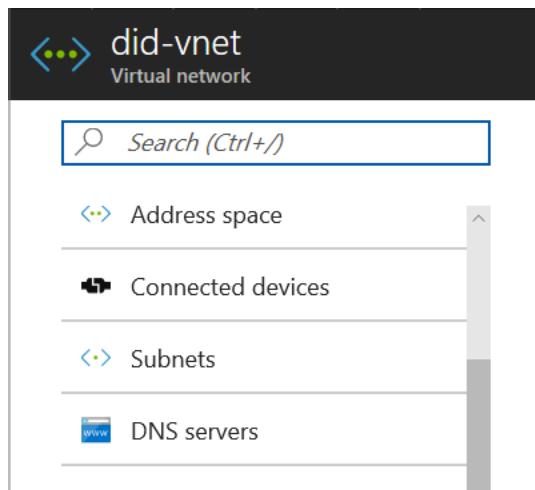
---

Note that we do not set up private connection between two virtual networks.

---

Perform the following steps to complete the lab:

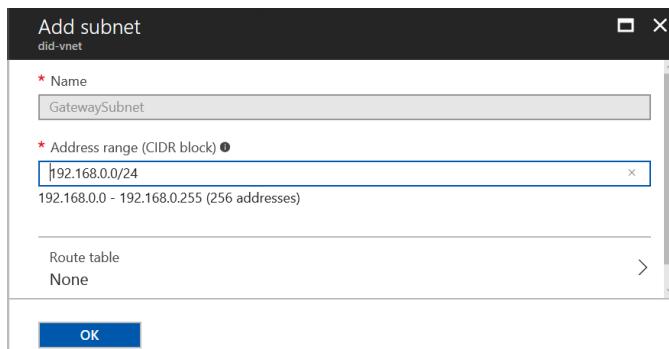
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual network**
3. Currently you have two virtual networks. We need to create a VPN gateway for your private network in order for the jump virtual network to connect to.
4. On the **did-vnet** blade, click **Subnets**.



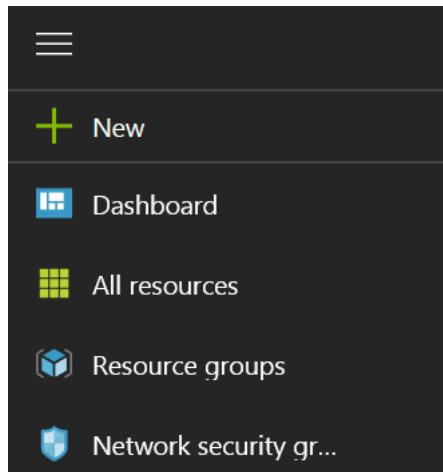
5. Click **Gateway subnet**.

NAME	ADDRESS RANGE	AVAILABLE ADDRES...
ad-subnet	192.168.1.0/24	250
db-subnet	192.168.2.0/24	250
web-subnet	192.168.3.0/24	249

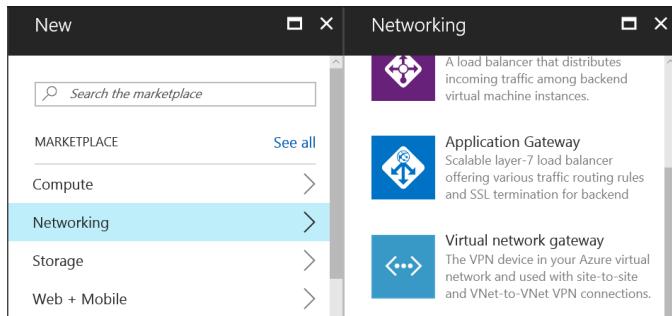
6. On the **Add subnet** blade, you are allowed to enter your address range only. The name is automatically populated. In this setup, we use the address range **192.168.0.0/24**
7. Click **OK**.



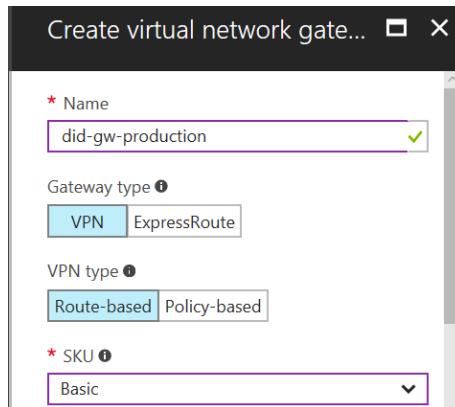
8. Go back to the Azure Management portal, from the left panel click (+ New).



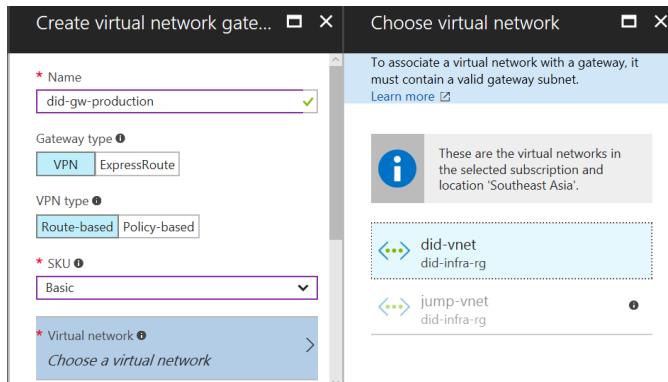
9. Click **Networking**. Select **Virtual network gateway**.



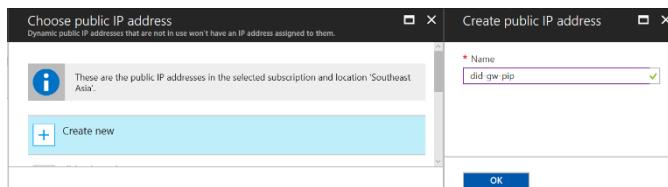
10. On the **Create virtual network gateway** blade, enter the name of the new virtual private gateway.
11. Select **VPN** under **Gateway type** setting. We do not use ExpressRoute connection (refer to *Chapter 3, ExpressRoute* section)
12. Select **Route-based** under **VPN type** setting.
13. Select **Basic** under **SKU** setting.



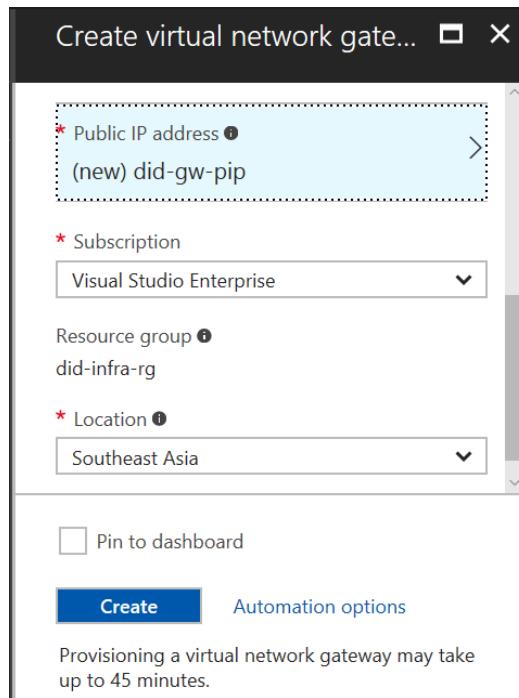
14. Click **Virtual network** setting, select **did-vnet**.



15. Click **Public IP address** setting, click **Create new**. On the **Create public IP address** blade, enter name of the new public IP address.
16. Click **OK**.



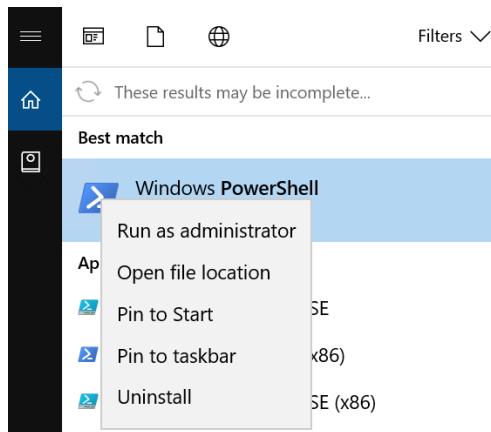
17. Select the same subscription you used during the lab under **Subscription** setting.
18. Select location under **Location**.
19. Click **Create**.



20. Note from Microsoft Azure that the virtual network gateway creation may take up to 45 minutes.
21. You can verify by going to **More services** then search for **Virtual network gateway**.

Virtual network gateways			
TS Consulting (ninthuanlive.onmicrosoft.com)			
<span style="font-size: 1.5em;">+</span> Add		Columns	Refresh
<b>Subscriptions:</b> 1 of 2 selected – Don't see a subscription? <a href="#">Switch directories</a>			
<input type="text" value="Filter by name..."/>	<input type="button" value="Visual Studio Enterprise"/>	<input type="button" value="All locati"/>	
1 items			
NAME	VIRTUAL NETWO...	GATEWAY TYPE	RESOURCE...
 did-gw-production	did-vnet	VPN	did-infra-rg

22. RDP to your jump virtual machine.
23. Click **Start** icon and enter PowerShell. Run it as an administrator.



24. You may be asked by **User Account Control**. Just click **Yes** to go through.
25. Type the following command

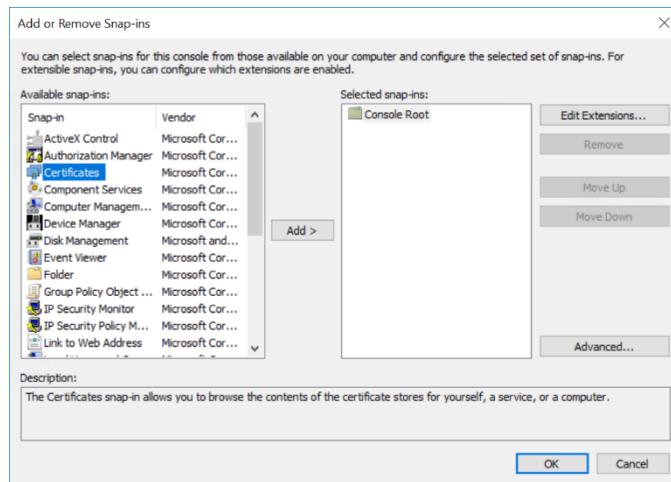
```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
```



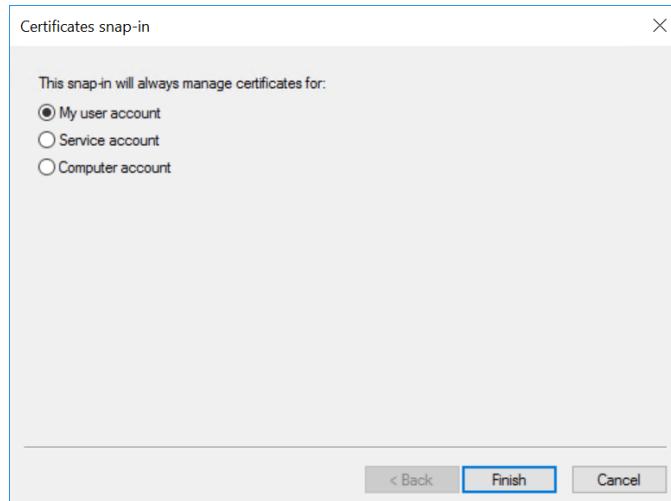
26. Keep PowerShell opening, run the following command to create a client certificate.

```
New-SelfSignedCertificate -Type Custom -KeySpec Signature -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2") -Subject "CN=P2SChildCert"
```

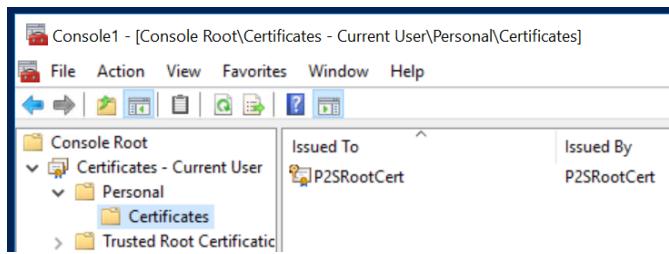
27. Press **Ctrl + R** and enter **mmc** to open **Microsoft Management Console**
28. Press **Ctrl + M** to add **Certificate** snap-in. Click **Certificates**. Click **Add**.



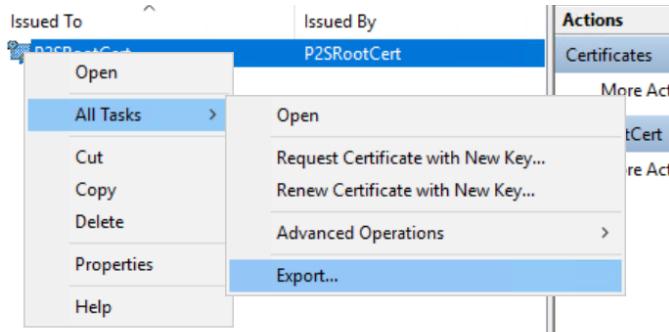
29. In **Certificates snap-in** windows, select **My user account**
30. Click **Next**.



31. Click **Finish**.
32. In **Add or Remove Snap-ins** windows, make sure the **Certificates (Local Computer)** is added.
33. Click **OK**
34. Expand **Certificates** then **Personal**. Click **Certificate folder** to verify the newly created certificate you created by PowerShell



35. Now you need to export public certificate file for Point-to-Site VPN. Right click on your newly created cert and select **All Tasks**. Click **Export**.



36. In **Welcome to the Certificate Export Wizard** page, click **Next**.
37. In **Export Private Key** page, select **No, do not export the private key**.
38. Click **Next**.
39. In **Export File Format** page, select **Base-64 encoded X.509 (.CER)**.
40. Click **Next**.

←  Certificate Export Wizard

**Export File Format**

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)  
 Base-64 encoded X.509 (.CER)  
 Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)  
     Include all certificates in the certification path if possible  
 Personal Information Exchange - PKCS #12 (.PFX)  
     Include all certificates in the certification path if possible  
     Delete the private key if the export is successful  
     Export all extended properties  
     Enable certificate privacy  
 Microsoft Serialized Certificate Store (.SST)

**Next**

**Cancel**

41. In **File to Export** page, browser to the location you want to store the file and type the file name. The extension is supposed to be **\*.cer**.
42. Click **Next**.

**File to Export**

Specify the name of the file you want to export

File name:

C:\cert\p2s.cer

**Browse...**

43. In **Completing the Certificate Export Wizard** page, review again all information you have. Click **Finish**.
44. A windows popup opens automatically informing you the successful exported certificate.

## Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\cert\p2s.cer
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

45. Go back to the Azure Management Portal. Navigate to open your virtual network gateway.
46. On the **did-gw-production** blade, click **Point-to-site configuration**
47. On the **Point-to-site configuration** blade, enter the address pool. Microsoft does not explain what this is. This is the reserved address which your jump virtual machine to connect to the private virtual network. In this case, we choose **10.0.0.0/24**

Save Discard Download VPN client

Connection health

Connections	0
Ingress (bytes)	0
Egress (bytes)	0

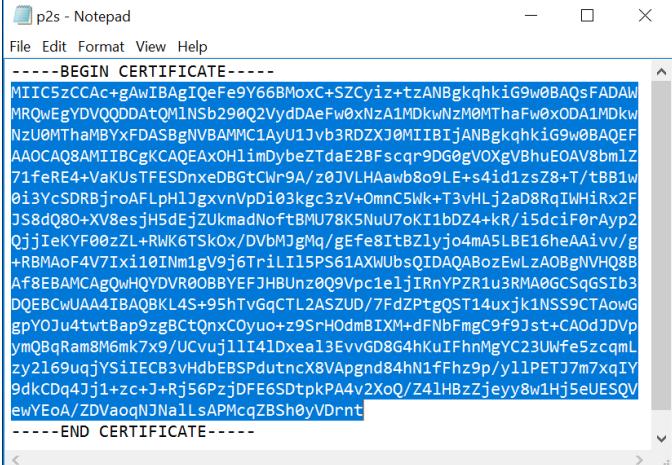
Address pool

10.0.0.0/24

Root certificates

NAME	PUBLIC CERTIFICATE DATA
p2s	MII... MIIC5zCCAc+gAwIBAgIQeFe9Y66BMoxC+SZCyiz+tzA... ...

48. Open the location where you specified to store the certificate file. Open it by Notepad and copy its content.

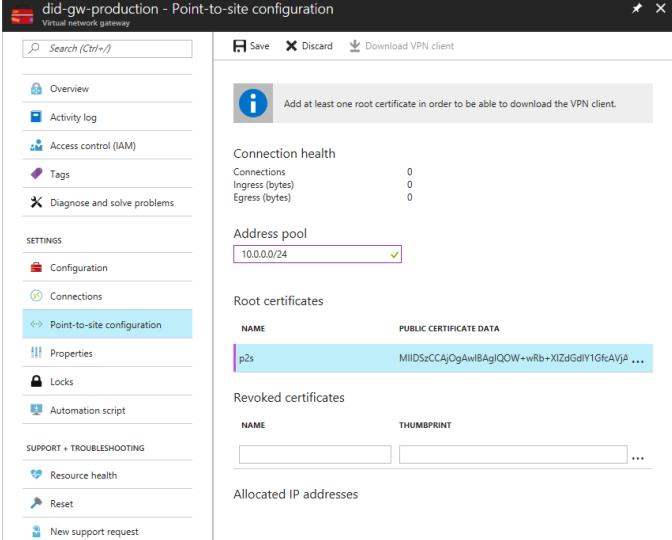


```

-----BEGIN CERTIFICATE-----
MIIC5zCACc+gAwIBAgIQeFe9Y66BMoC+SZCyiz+tzANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDAzQMLNsB290Q2VydDaeFw0xNzA1MDkwNzM0MThaFw0xODA1MDkw
NzU0MThaMBYxFDASBgNVBAMMC1AyU1jb3RDZJ0MIIBIjANBgkqhkiG9w0BAQE
AAOCQAQ8AMIIBCgKCAQEAx0HlimDybeZTdaE2Bfscqr9DG0gVOXevBhuEOAV8bm1z
71feR4+VaKUsTFESDnxDBGtCWr9A/z0JVLHaawb8o9LE+s4id1zsZ8+T/tBB1w
0i3YcSDRBjroAFLpHJgxvnVpDi03kgc3zV+0mnC5Wk+T3vHLj2aD8RqIWHiRx2F
JS8dq080+XV8esjH5dEjZUkmaDnoftBMU78k5NuU70kI1bDZ4+KR/i5dcI0rAyp2
QjjIeKYF00zL+RWK6TSkOx/DVbMjgMq/gFfe8ItBzlyjo4mA5LB16heAAivv/g
+RBMoF4V71xi10INm1gV9j6tril15PS61AXWUb5QIDAQABoZeWLzAOgNVHQ8B
Af8EBAMCAgQwHQYDVR0OBBYEFJHBUNz0Q9Vpc1eljIRnYPZR1u3RMA0GCSqGSIb3
DQEBCwUA4IBAQBL4S+95hTvGqCTL2ASZUD/7FdZPtg0ST14uxjk1N599CTAoWg
gpYOJu4twtBap9zgBctQnxCOyu+0SrH0dmBIXM+dFnBFmgC9f9Jst+CA0dJDVp
ymQ8aRam8M6mk7x9/Ucvuj11i41bxeal3EvvGD8G4hKu1FhnMgYC23UWfe5zcqML
zy2169uqjYSiIECB3vHdbEBSPdutncX8VAprnd84hN1fFhz9p/y11PETJ7m7xqIY
9dkCDq4j1+zc+j+R156PzjDFE65DtpkPA4v2XoQ/Z41HBzZjeyy8w1Hj5eUESQV
ewYEA/ZDVaoqNjNa11sAPMcqZBSH0yvDrnt
-----END CERTIFICATE-----

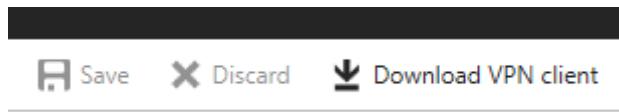
```

49. Paste the copied to the box under **Public certificate data** box. Enter the name for your cert.

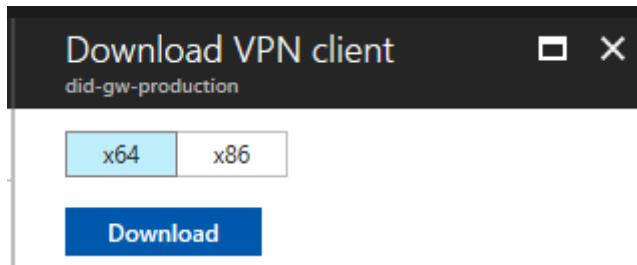


NAME	PUBLIC CERTIFICATE DATA
p2s	MiIDSzCCAj0AwIBAgIQOW+wRb+XIZdGdIV1GfcAVjA...

50. Leave **Revoked certificates** setting blank.
51. Click **Save**.
52. Wait around 5-10 minutes until the configuration is updated to establish point-to-site connection.
53. On the **Point-to-site configuration** blade, click **Download VPN client**.

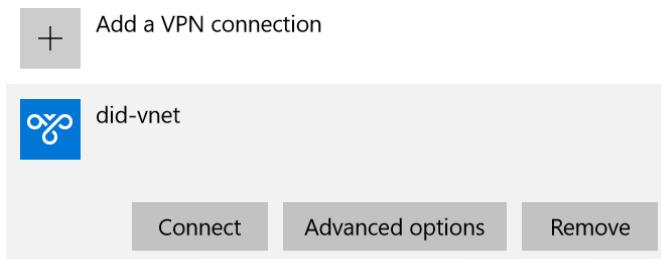


54. Select the appropriate VPN client package for your operating system. In this case, we select x64. Click **Download**.

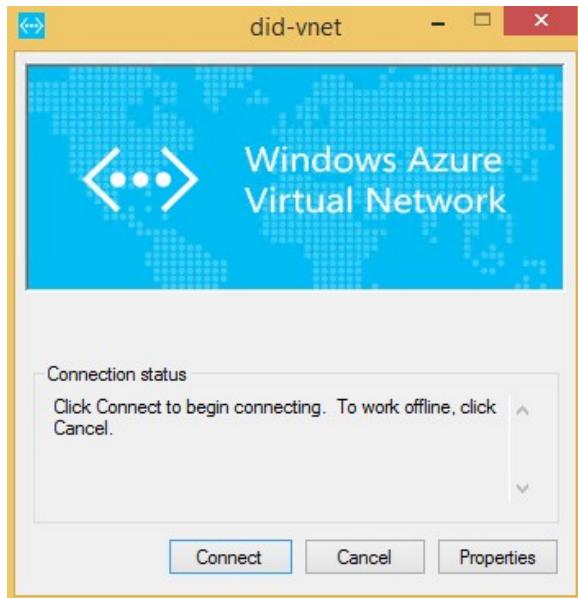


55. You need to download the VPN client (x64).exe file directly on the jump virtual machine and run it to install the VPN client. You are asked to confirm to install a VPN Client. You may need to restart the jump virtual machine after the VPN client is successfully installed. Copy VPN client from another machine to jump virtual machine would not work if the anti-virus blocked the download.
56. Open network setting on the jump virtual machine. You will see the new VPN named the same as your private virtual network.
57. Click **Connect**.

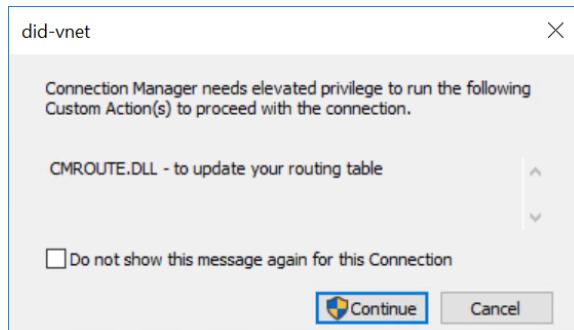
## VPN



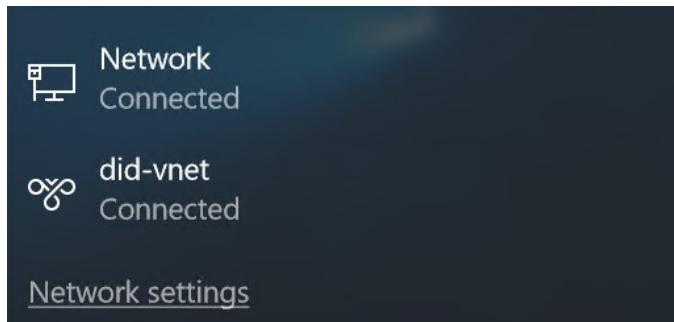
58. From the VPN client, click **Connect**.



59. You are asked to confirm to elevate privilege of Connection Manager by running CMROUTE.DLL to process the connection.
60. Click **Continue**.



61. The VPN client will check the client certificate you generated in step 26 with the public certificate you configured in step 49. It is successfully if the configuration is correct. Check from network setting.



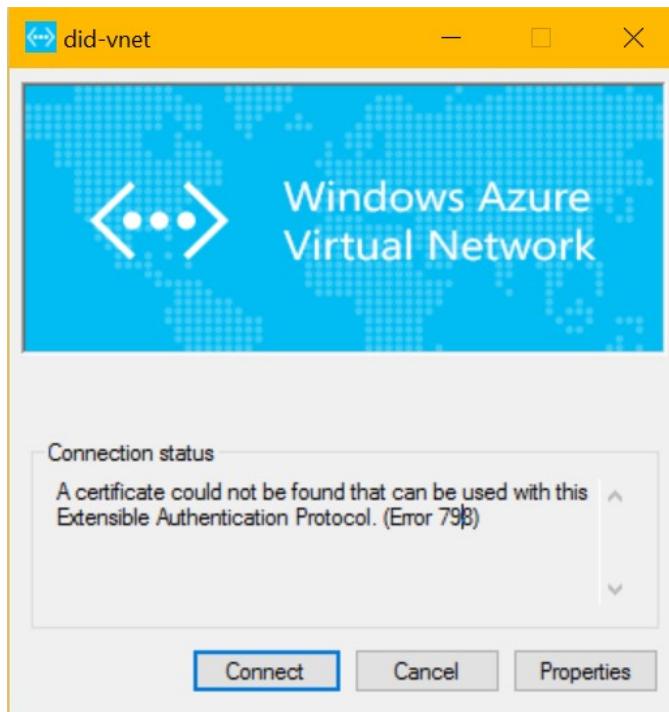
Now you have completed this lab.

## Lab 2.3 – Connect to private virtual network from your laptop

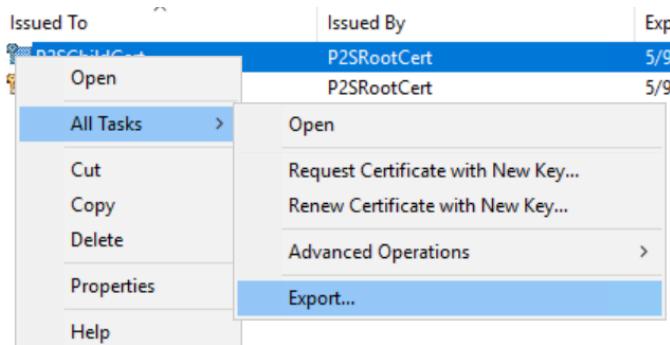
In **Lab 2.2**, you completed configuring Point-to-site VPN to allow your jump virtual machine connect to the private virtual network. In some cases, you want to connect from your personal laptop. In this case, you do not necessarily have to generate a new certificate. Instead, you need the client certificate you created in *Lab 2.2*. This lab is going to walk you through steps to connect to the private virtual network from your personal laptop.

Perform the following steps to complete the lab:

1. Install VPN client you downloaded from step 54 in Lab 2.2.
2. If you try to connect to the private virtual network without any valid client certificate installed on your laptop, you will get the error message “A certificate could not be found that can be used with this Extensible Authentication Protocol. (Error 798)”

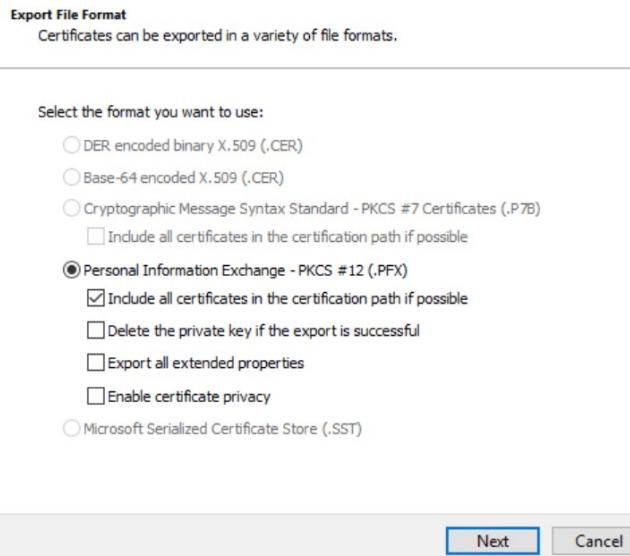


3. Go to the jump virtual machine to start exporting the client certificate.
4. Repeat step 27 – 34 in **Lab 2.3** to open Personal certificate console. There is a client certificate you created named **P2SChildCert**.



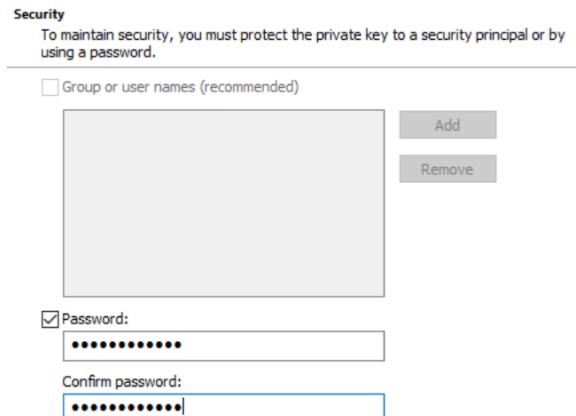
5. In **Welcome to the Certificate Export Wizard** page, click **Next**.
6. In **Export Private Key** page, select **Yes, export the private key**.

7. In **Export File Format** page, select **Personal Information Exchange – PKCS #12 (.PFX)**. Select **Include all certificates in the certification path if possible**.
8. Click **Next**.



9. In **Security** page, select **Password** and enter password to protect your key when you import to your laptop. This is a security practice to ensure if the certificate is lost to an attacker, he cannot import to his machine without knowing the password.

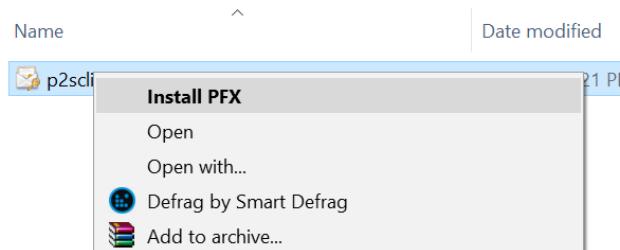
10. Click **Next**.



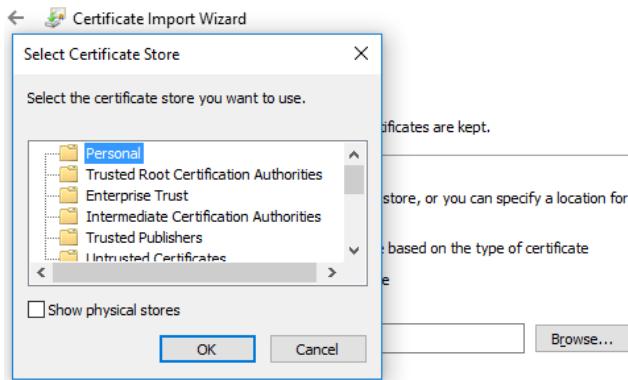
11. In **File to Export** page, browse to the folder you want to store the client certificate you are going to export. Make sure the file extension is **\*.pfx**.
12. Click **Next**.



13. In **Completing the Certificate Export Wizard** page, review information you just configured. Click **Finish**.
14. Copy the exported certificate to your laptop.
15. Right click on this certificate and select **Install PFX**.

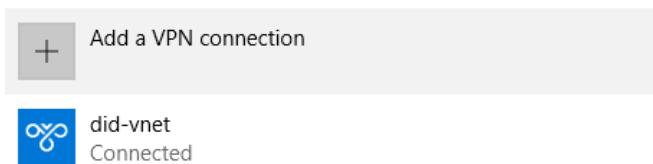


16. In **Welcome to the Certificate Import Wizard** page, select Current User.
17. In **File to Import** page, make sure you locate the exported client certificate. Click **Next**.
18. In **Private key protection** page, enter the password you set in step 10. Click **Next**.
19. In **Certificate Store** page, select **Place all certificates in the following store**. Click **Browser** and select **Personal**.



20. In **Completing the Certificate Import Wizard** page, click **Finish**.
21. You are asked to confirm to install two certificates to the trusted root certificate list. It is because the certificate you generated is not issued by any corporate authority. Click **Yes** twice to go through this security warning.
22. Now try to connect to the private virtual network with VPN client. Make sure two certificates are successfully installed in **Personal** store.

## VPN



Now you have completed this lab.

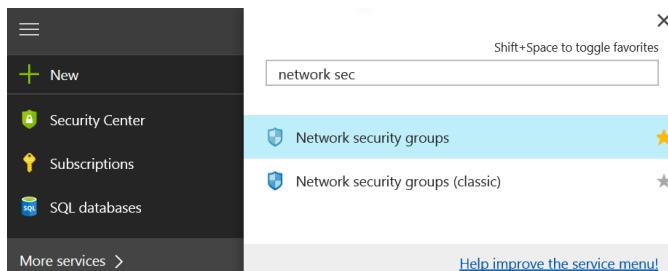
## Lab 2.4 – Blocking RDP from the Internet with Network Security Group

Previously you successfully installed the jump virtual machine, established Point-to-site connection on both jump virtual machine and your personal laptop. However, we can still RDP to any virtual machine in the private virtual network from the Internet. This is considered unsecure configuration. What we need to do is block RDP to the Internet. That said,

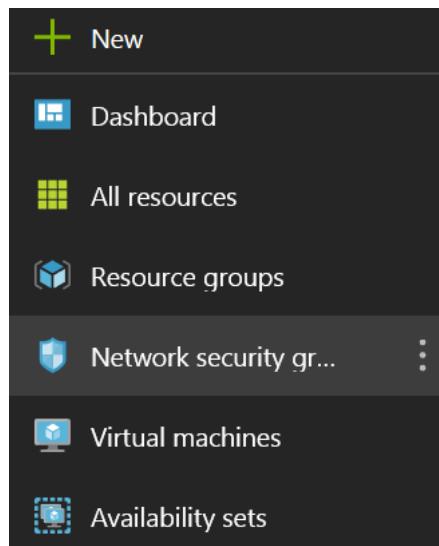
you must RDP to the jump virtual machine first, before establishing VPN connection to any virtual machine in the private virtual network. This lab is going to walk you through steps to configure a network security group to block Internet-bound RDP.

Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **More services** to add **Network security groups** navigation.



3. Go back to the left panel and click **Network security groups**.



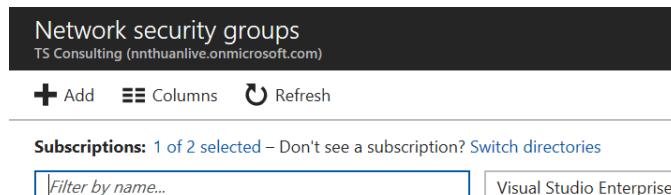
4. On the **Network security groups** blade, click **Add**

Network security groups  
TS Consulting (n nthuanlive.onmicrosoft.com)

**+** Add **Columns** **⟳** Refresh

**Subscriptions:** 1 of 2 selected – Don't see a subscription? [Switch directories](#)

Visual Studio Enterprise



5. On the **Create network security group** blade, enter the name for the new network security group. This name should be meaningful. Let's say it is a group of rules for your DMZ.
6. Select your subscription under **Subscription** setting.
7. Select **Use existing** under **Resource group** setting. Select **did-infra-rg** we planned to group all network and infrastructure components.
8. Click **Create**.

Create network security gro... □ X

**\* Name**  
 ✓

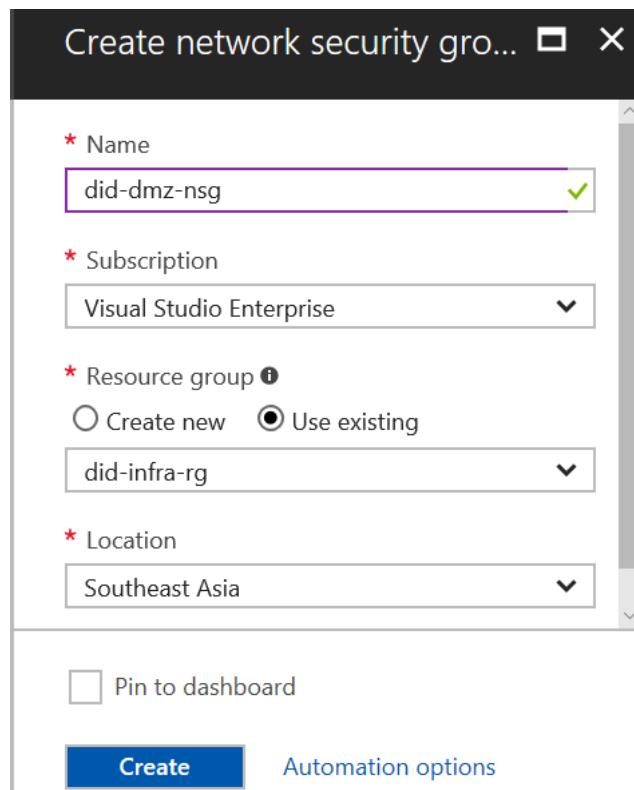
**\* Subscription**  
 ▼

**\* Resource group  ⓘ**  
 Create new  Use existing  
 ▼

**\* Location**  
 ▼

Pin to dashboard

**Create** **Automation options**



9. Wait a few minutes until the network security group is successfully created.

- Click **did-dmz-nsg** to start configuring rule. Because we need to block all incoming request containing RDP packet, we have to create a new inbound security rule.
- On the **did-dmz-nsg** blade, click **Inbound security rules**.

- On the **Inbound security rules** blade, click **Default rules** to see all the hidden default rules.
- By default, there are three inbound rules with low priority.
  - AllowVnetInbound**: this rule allows inbound network traffic to pass across virtual networks.
  - AllowAzureLoadBalancerInBound**: this rule allows inbound network traffic to pass from Azure Load Balancer to any destination.
  - DenyAllInBound**: this rule is to deny all inbound network traffic from any resource to any resource.

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
65000	AllowVnetInbound	VirtualNetwork	VirtualNetwork	Custom (Any/Any)	Allow
65001	AllowAzureLoadBalancerInBo...	AzureLoadBalancer	Any	Custom (Any/Any)	Allow
65500	DenyAllInBound	Any	Any	Custom (Any/Any)	Deny

---

You might be afraid of **DenyAllInBound** rule because it blocks all inbound rules including RDP or any type of protocol. Fundamentally it does. However, because **DenyAllInBound** rule is set at lower

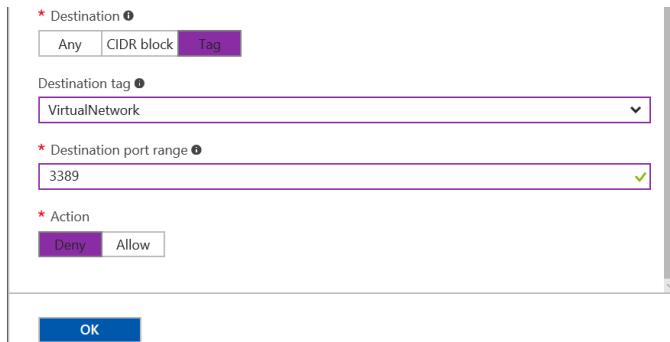
priority than **AllowVnetInBound** when Azure processes to check the rule, it prioritizes **AllowVnetInBound** first. All other rules with lower priority is not processed after then. It means if **AllowVnetInBound** rule is processed, **DenyAllInBound** rule is not effective.

---

14. On the **Inbound security rule** blade, click **Add**.
15. On the **Add inbound security rule** blade, enter name of the rule for blocking RDP.
16. Set the priority around **300** under **Priority** setting. 300 is not a must but I would recommend you this number in order to reserve higher priority (lower number) for further critical rules if any.
17. Click **Advanced**.
18. Select **Tag** under **Source** setting.
19. Select **Internet** under **Source tag** setting.
20. Select **Any** under **Protocol** setting.
21. Enter **3389** under **Source port range**. This is the default RDP port.



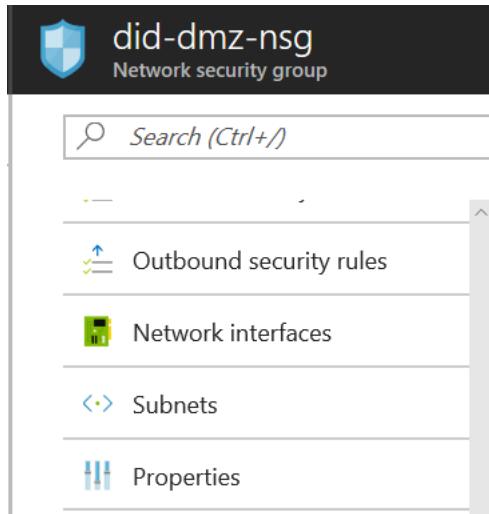
22. Select **Tag** under **Destination** setting.
23. Select **VirtualNetwork** under **Destination tag**.
24. Enter **3389** under **Destination port range** setting.
25. Select **Deny** under **Action** setting.
26. Click **OK**.



27. Wait a few minutes until the new inbound rule is created successfully.
28. Check the list of inbound rules. You have completed creating a straightforward rule to deny all RDP inbound network packet from the Internet to your virtual network.

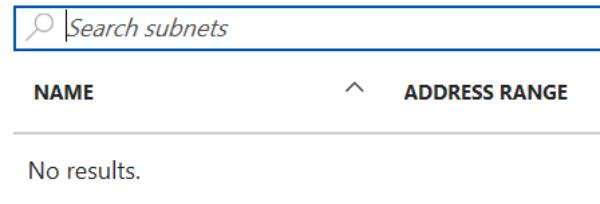
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
300	BlockRDP	Internet	VirtualNetwork	Custom (Any/3389)	<b>Deny</b>

29. Now you need to associate the network security group to all subnets you have.
30. On the **did-dmz-nsg** blade, click **Subnets**.



31. On the **Subnets** blade, click **Associate**.

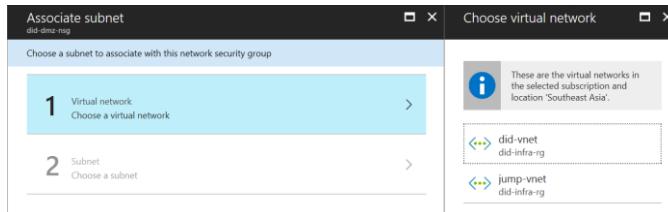
## ⊕ Associate



Search subnets

NAME	ADDRESS RANGE
No results.	

32. On the **Associate subnet** blade, click **Virtual network** then select your private virtual network



Associate subnet  
did-dmz-rg

Choose a subnet to associate with this network security group

1 Virtual network  
Choose a virtual network

2 Subnet  
Choose a subnet

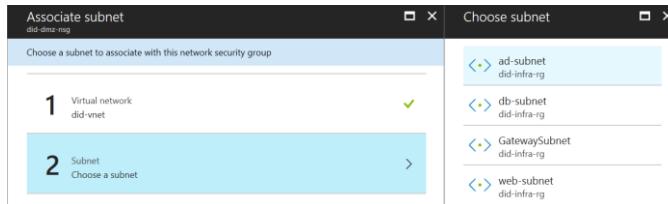
Choose virtual network

These are the virtual networks in the selected subscription and location 'Southeast Asia'.

did-vnet  
did-infra-rg

jump-vnet  
did-infra-rg

33. Click **Subnet** then select **ad-subnet**



Associate subnet  
did-dmz-rg

Choose a subnet to associate with this network security group

1 Virtual network  
did-vnet

2 Subnet  
Choose a subnet

Choose subnet

ad-subnet  
did-infra-rg

db-subnet  
did-infra-rg

GatewaySubnet  
did-infra-rg

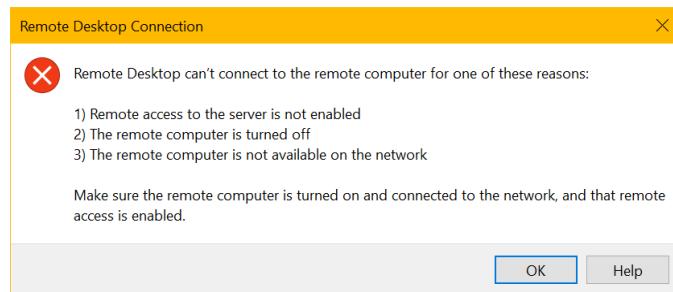
web-subnet  
did-infra-rg

34. Click **OK**.

35. Repeat step 31 – 33 to associate your network security group to **db-subnet** and **web-subnet**.

NAME	ADDRESS RANGE	VIRTUAL NETWORK
ad-subnet	192.168.1.0/24	did-vnet
db-subnet	192.168.2.0/24	did-vnet
web-subnet	192.168.3.0/24	did-vnet

36. Let's do a test by RDP from the Internet without VPN connection to any of your virtual machine. You will encounter an error message from RDP.



37. Now if you disassociate your network security group out of a subnet, you will be able to RDP.

NAME	ADDRESS RANGE	VIRTUAL NETWORK	
ad-subnet	192.168.1.0/24	Dissociate	...
db-subnet	192.168.2.0/24	did-vnet	...
web-subnet	192.168.3.0/24	did-vnet	...

38. Try one more time by RDP to your jump virtual machine then RDP to any of virtual machine in the private virtual network.

Now you have completed this lab. Blocking RDP from the Internet to your virtual network is recommended to make your system more secure. In the next lab, we will explore on how to allow RDP from the Jump virtual machine.

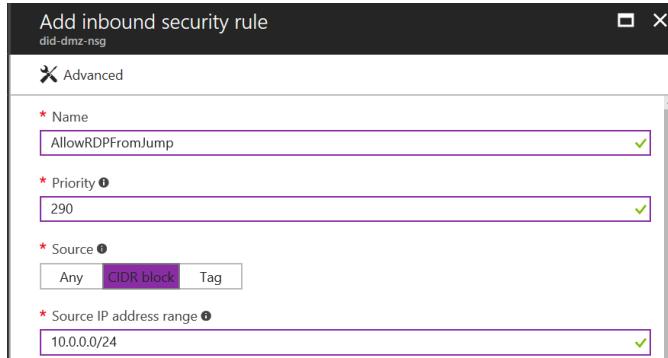
## Lab 2.5 – Allowing RDP from the Jump virtual machine

From now on, you are no longer able to RDP to the private virtual network (did-vnet) because RDP is blocked even each virtual machine has a public IP address. However, you still need to RDP to your SharePoint virtual machines from the jump virtual machine. This lab is going to walk you through step to create a new inbound rule to allow only the jump virtual machine to RDP to your SharePoint virtual machine.

Perform the following steps to complete the lab:

1. From **did-dmz-nsg** you created, click **Inbound security rule** on the blade to create a new inbound rule.
2. On the **Add inbound security rule** blade, enter name of the new rule (e.g. **AllowRDPFromJump**)

3. Set the priority lower than the **BlockRDP** you created.
4. Select **CIDR block** under **Source** setting.
5. Under **Source IP address range**, enter the client address pool you configured from step 47 in *Lab 2.2*.



6. Select **RDP** under **Service** setting.
7. The configurations under **Protocol** and **Port range** settings are automatically populated.
8. Select **Allow** under **Action** setting.
9. Click **OK**.

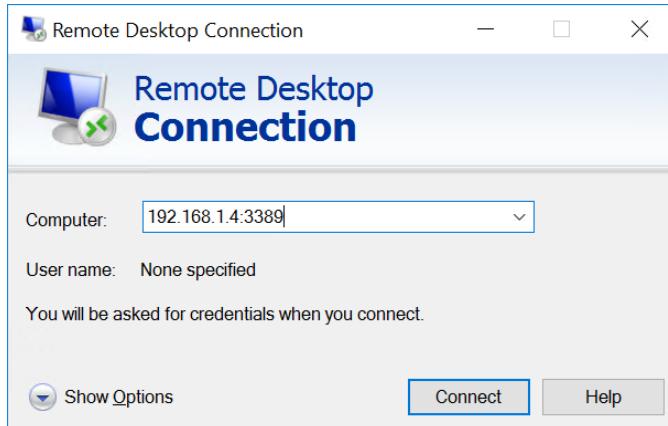


10. Verify your newly created rule. From the below screen, it is easy to understand that RDP network packet is permitted from the address range **10.0.0.0/24** which is configured to your jump virtual machine after successfully connected to the private virtual network.

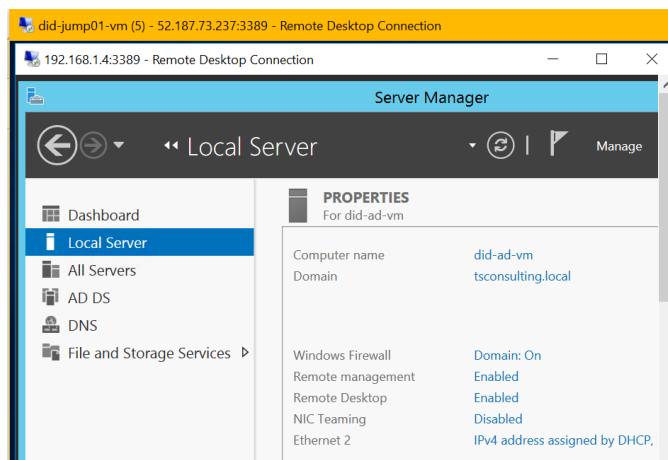
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
290	AllowRDPFromJump	10.0.0.0/24	Any	RDP (TCP/3389)	Allow
300	BlockRDP	Internet	VirtualNetwork	Custom (Any/3389)	Deny

11. Now it is the time for test. From the jump virtual machine, RDP to one of the SharePoint virtual machine. Make sure you use private IP

address of the target virtual machine, not the virtual machine name, public IP address or even FQDN (Full Qualified Domain Name).



12. Remember to use your domain account (e.g. `tsconsulting\thuansoldier`) to log into.



Now you have completed this lab.

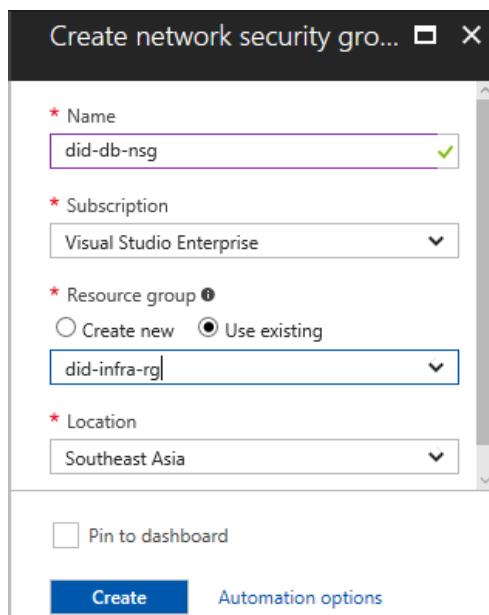
## Lab 2.6 – Allowing SQL Service to your database virtual machine

Previously, you created two inbound security rules to block all incoming Internet-bound network traffic on port 1433 and only allows RDP from the jump virtual machine. This results a big challenge to an attacker because he must gain the jump virtual machine's account to RDP to your jump virtual

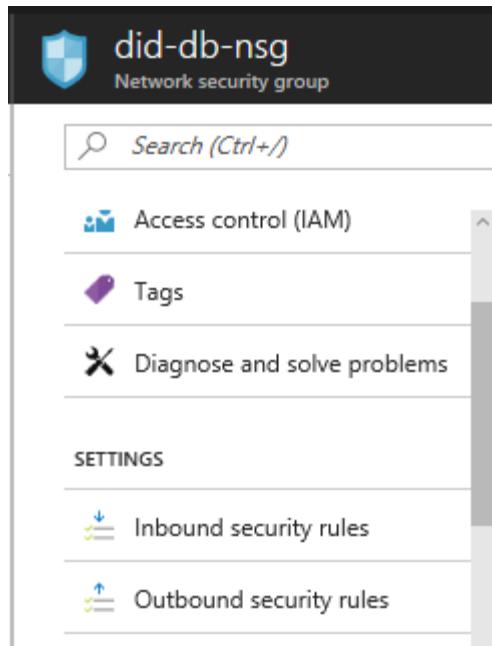
machine, before connecting to the private virtual network through Point-to-Site VPN gateway. In this lab, we will continue working with Azure network security group. This lab is going to walk you through steps to create a new network security group and inbound security rule to allow SQL service on port 1433 from the SharePoint web front-end virtual machines to the database virtual machine.

Perform the following steps to complete the lab:

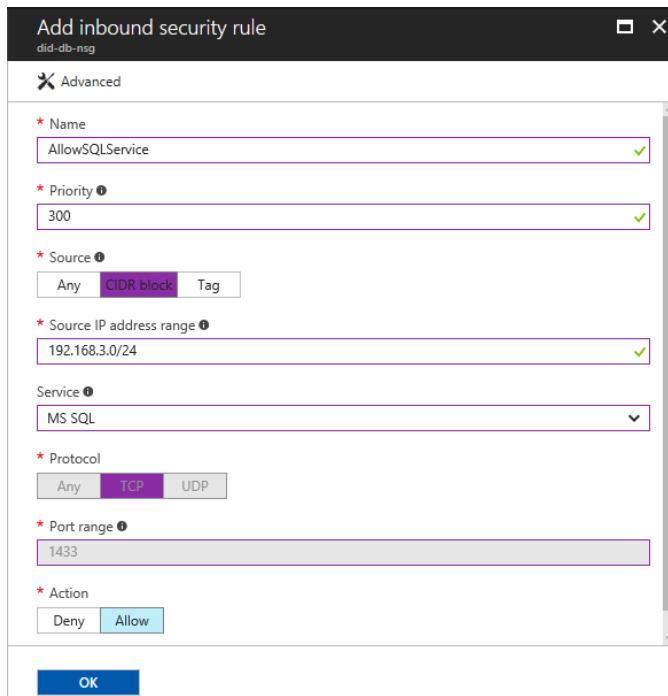
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Network security groups**
3. On the **Network security groups** blade, click **Add**
4. On the **Create network security group** blade, enter the name for the new network security group. This name should be meaningful.
5. Select your subscription under **Subscription** setting.
6. Select **Use existing under Resource group** setting. Select **did-infra-rg** we planned to group all network and infrastructure components.
7. Select your location under **Location** setting.
8. Click **Create**.



9. Wait a few minutes until the network security group is successfully created.
10. Click **did-db-nsg** to start configuring rule. Because we need to only allow network packet on the port 1433 from web front-end virtual machines to database virtual machine so we need to create an inbound rule.
11. On the **did-db-nsg** blade, click **Inbound security rules**.



12. On the **Inbound security rule** blade, click **Add**.
13. On the **Add inbound security rule** blade, enter name of the rule for allowing SQL service (e.g. **AllowSQLService**)
14. Enter the priority value under **Priority** setting.
15. Select **CIDR block** under **Source** setting.
16. Enter subnet address space of web front-end virtual machines under **Source IP address range** setting. In the lab, it is **192.168.3.0/24**
17. Select **MS SQL** under **Service** setting.
18. The configurations under **Protocol** and **Port range** settings are automatically populated.
19. Select **Allow** under **Action** setting.
20. Click **OK**.



21. Check the list of inbound rules.

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
300	AllowSQLService	192.168.3.0/24	Any	MS SQL (TCP/1433)	Allow

39. Now you need to associate the network security group to all subnets you have.  
 40. On the **did-db-nsg** blade, click **Subnets**.  
 41. On the **Subnets** blade, click **Associate**.

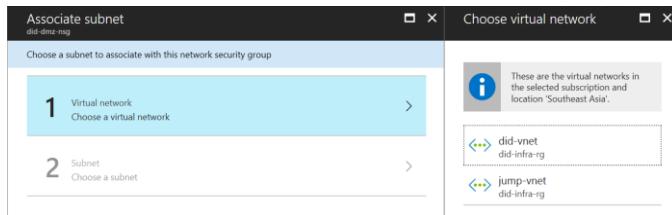
**Associate**

---

*Search subnets*

NAME	ADDRESS RANGE
No results.	

42. On the **Associate subnet** blade, click **Virtual network** then select your private virtual network



43. Click **Subnet** then select **db-subnet**
44. Click **OK**.

If you receive the warning that your network security group will replace the previous one. Do not mind this because you are just doing an experiment in Azure Network Security Group to make sure you have hands-on experience. In the real-world scenario, you just need to create only one network security group that contain three rules we have finished so far in **Lab 2.4**, **Lab 2.5** and **Lab 2.6**. From this lab, you can see that one subnet cannot have multiple network security group. A recommended practice is to create network security group per subnet. Remember creating a new inbound rule to block RDP from the Internet and allow RDP from the jump virtual machine.

## Lab 2.7 – Routing to Defense System

In *Chapter 3, Routing to Defense* section system you were introduced User Defined Routing to create your custom route to force network traffic to a defense system for better monitoring and inspection. Traffic coming from the web front-end virtual machines to the database virtual machine need to go through a defense system first. Similarly, outgoing network traffic from the database virtual machines to the web front-end virtual machines are better to be protected. This lab is going to walk you through steps to use User Defined Routing to force traffic among virtual machines.

Perform the following steps to complete the lab:

1. Open Barracuda Evaluation site at <https://www.barracuda.com/purchase/evaluation> to request a trial evaluation. Under **Select a product**, make sure to choose Barracuda NextGen Firewall F Azure.

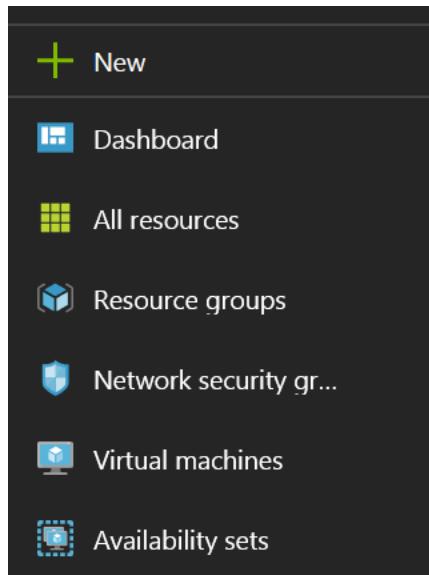
Barracuda Essentials for Office 365  
Barracuda Cloud Archiving Service

**Public Cloud Solutions**

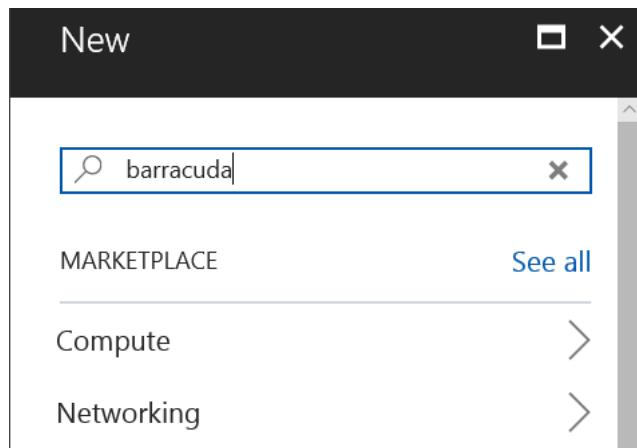
Barracuda Application Security Control Center AWS  
Barracuda Application Security Control Center Azure  
Barracuda Email Security Gateway AWS  
Barracuda Email Security Gateway Azure  
Barracuda Email Security Gateway vCloud Air  
Barracuda Load Balancer ADC AWS  
Barracuda Message Archiver AWS  
Barracuda Message Archiver vCloud Air  
Barracuda NextGen Control Center Azure  
Barracuda NextGen Control Center for AWS  
Barracuda NextGen Firewall F AWS  
**Barracuda NextGen Firewall F Azure**  
Barracuda NextGen Firewall F Google Cloud Platform  
Barracuda NextGen Firewall F vCloud Air  
Barracuda Web Application Firewall AWS  
Barracuda Web Application Firewall Azure  
Barracuda Web Application Firewall vCloud Air

Please Choose ▾ Last Name

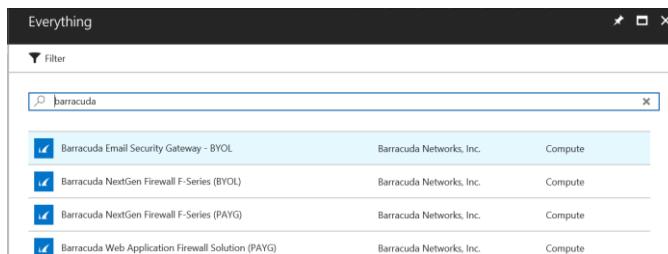
2. Complete the form with your personal information. After your registration, Barracuda will send you a confirmation email including serial number and license token.
3. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
4. From the left panel, click **New**.



5. On the **New** blade, enter **Barracuda** into search box then press **Enter**

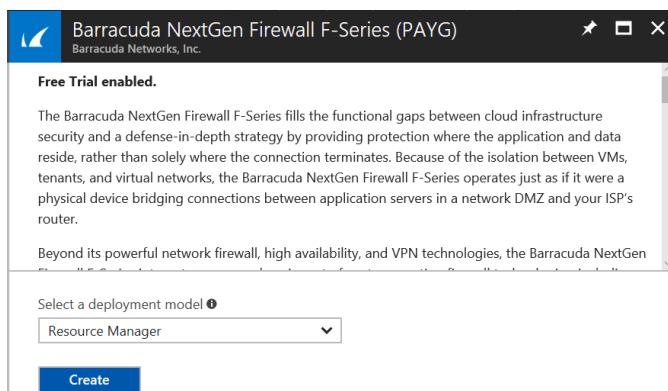


6. On the **Everything** blade, select **Barracuda NextGen Firewall F-Series (PAYG)**

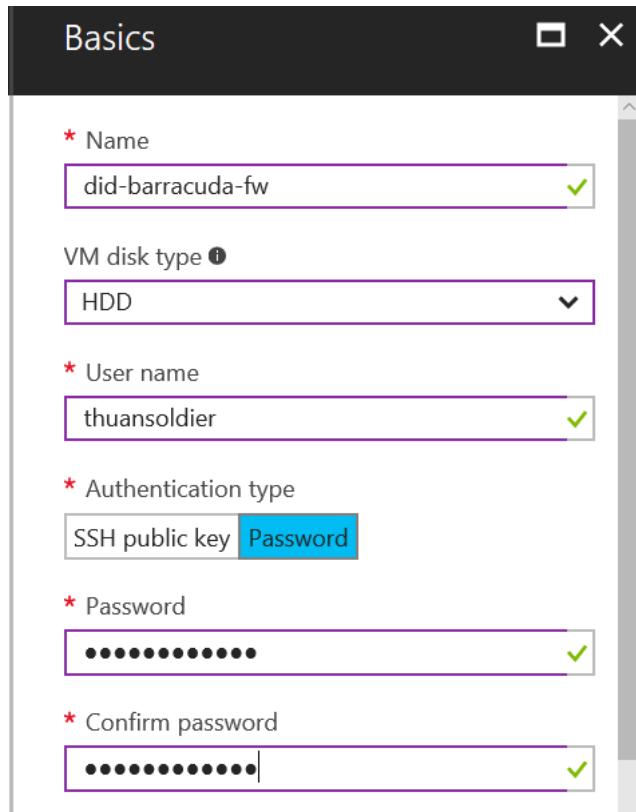


7. On the **Barracuda NextGen Firewall F-Series (PAYG)** blade, make sure the deployment model is **Resource Manager**.

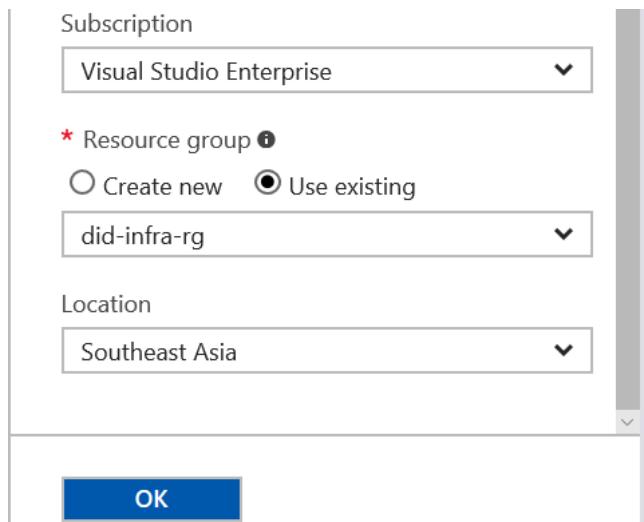
8. Click **Create**.



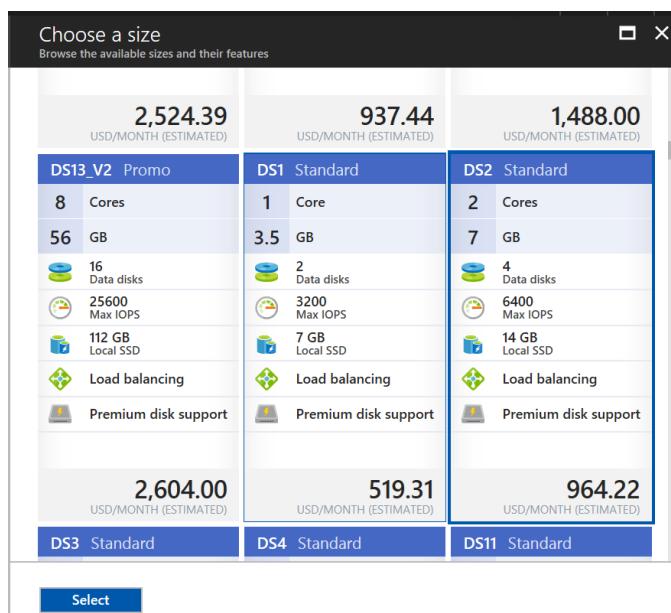
9. On the **Basics** blade, enter name of the new Barracuda firewall under Name setting.
10. Select **HDD** under **VM disk type** setting.
11. Enter username under **User name** setting.
12. Select **Password** under **Authentication type** setting.
13. Enter your password and confirm it.



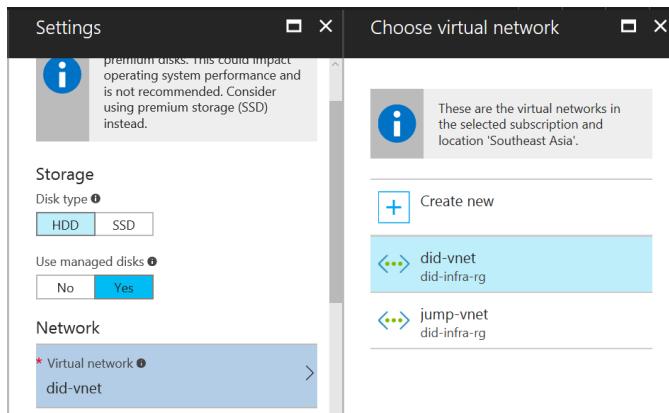
14. Select your subscription under **Subscription** setting.
15. Select **Use existing** under **Resource group** setting, select **did-infra-rg** from the drop-down list.
16. Select your location under **Location** setting.
17. Click **OK**.



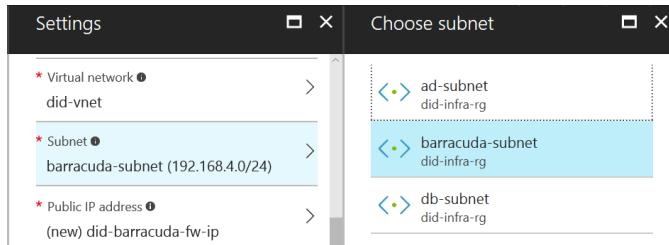
18. On the **Choose a size** blade, search for DS2 standard and select it.
19. Click **Select**



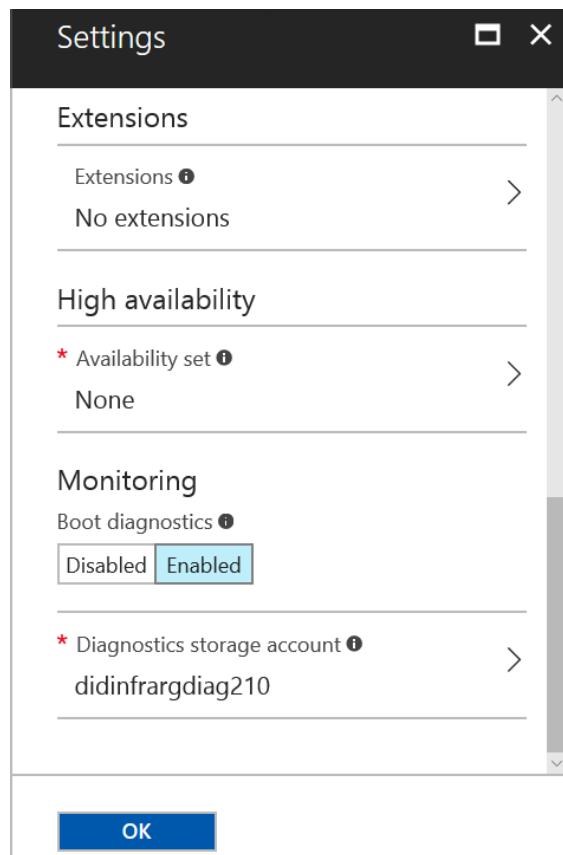
20. On the **Settings** blade, select **HDD** under **Disk type** setting.
21. Select **Yes** under **Use managed disks** setting.
22. Click **Virtual network** setting, select your private virtual network.



23. Click **Subnet** setting. Select a dedicated subnet for your Barracuda firewall. If you have not created that subnet, refer to *Lab 1.4* to create a new subnet.



24. Leave **Public IP address** setting and **Network security group (firewall)** by default. The network security group created for Barracuda contains some special rules you can explore after creating the firewall.
25. Keep **Extensions** and **High availability** setting by default.
26. Select **Enabled** under **Boot diagnostics** setting.
27. Keep **Diagnostics storage account setting** by default if you do not want to select an existing storage account.
28. Click **OK**.



29. On the **Summary** blade, review all information again.
30. Click **OK**.

Summary

Validation passed

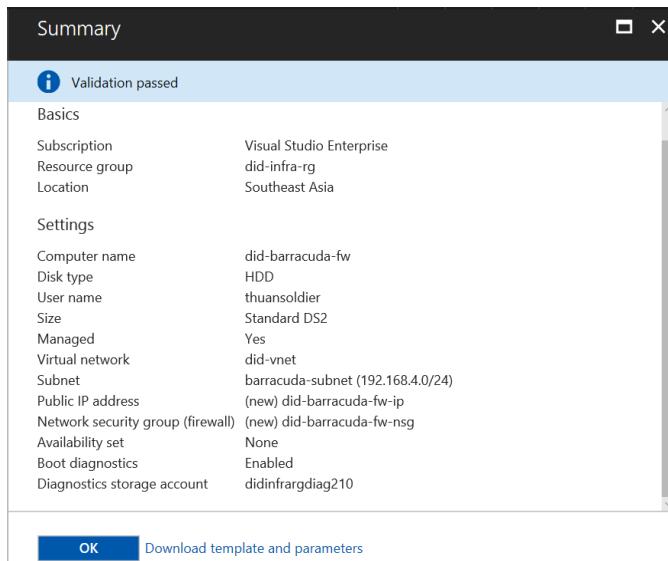
Basics

Subscription	Visual Studio Enterprise
Resource group	did-infra-rg
Location	Southeast Asia

Settings

Computer name	did-barracuda-fw
Disk type	HDD
User name	thuansoldier
Size	Standard DS2
Managed	Yes
Virtual network	did-vnet
Subnet	barracuda-subnet (192.168.4.0/24)
Public IP address	(new) did-barracuda-fw-ip
Network security group (firewall)	(new) did-barracuda-fw-nsg
Availability set	None
Boot diagnostics	Enabled
Diagnostics storage account	didinfrargdiag210

OK Download template and parameters



31. On the **Purchase** blade, review Barracuda price and some terms of use.
32. Click **Purchase**.

Purchase

Offer details

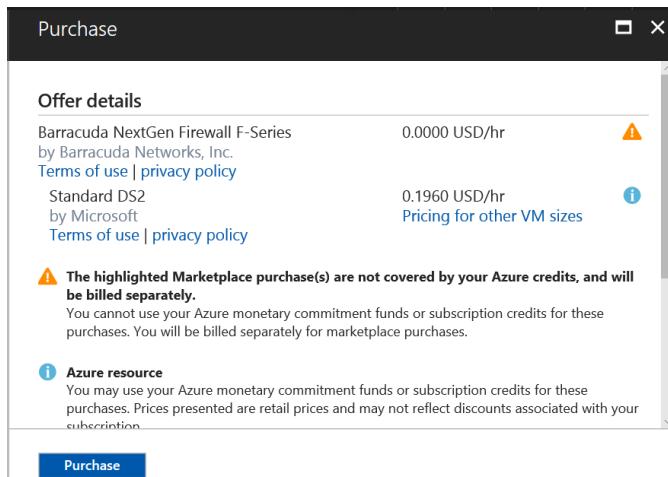
Barracuda NextGen Firewall F-Series by Barracuda Networks, Inc.	0.0000 USD/hr	⚠
Standard DS2 by Microsoft	0.1960 USD/hr	ⓘ

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

**⚠ The highlighted Marketplace purchase(s) are not covered by your Azure credits, and will be billed separately.**  
You cannot use your Azure monetary commitment funds or subscription credits for these purchases. You will be billed separately for marketplace purchases.

**ⓘ Azure resource**  
You may use your Azure monetary commitment funds or subscription credits for these purchases. Prices presented are retail prices and may not reflect discounts associated with your subscription.

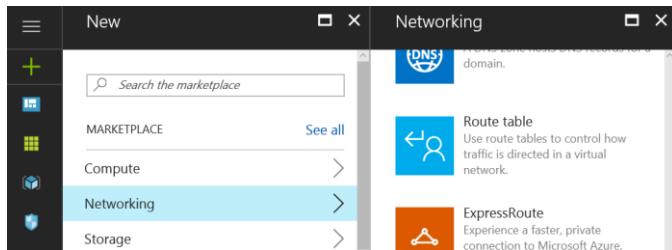
Purchase



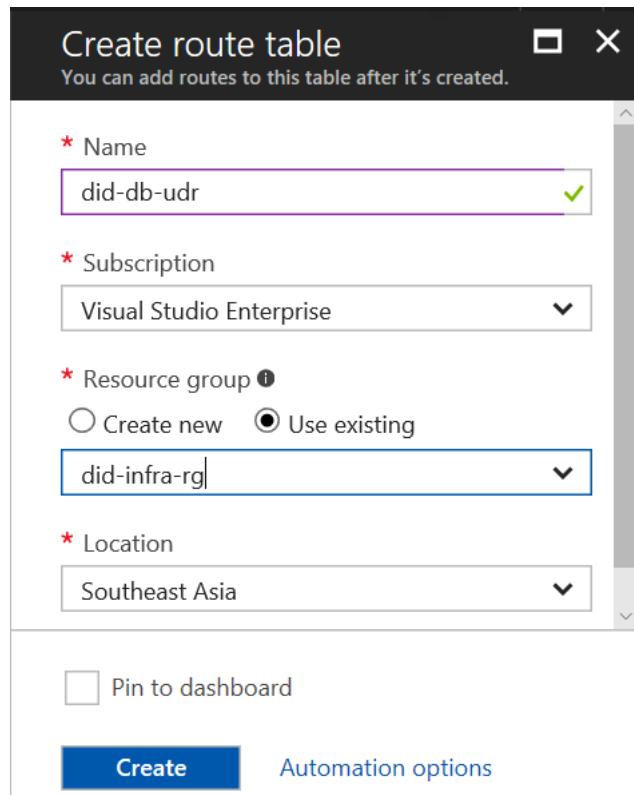
33. Go to the list of virtual machines to verify your newly created Barracuda firewall

NAME	STATUS	RESOURCE GROUP
did-ad-vm	Running	did-ad-rg
did-barracuda-fw	Running	did-infra-rg
did-db-vm	Running	did-db-rg
did-jump01-vm	Running	did-infra-rg
did-web01-vm	Running	did-web-rg
did-web02-vm	Running	did-web-rg

34. Go to the Azure Management Portal. Click **New** from the left panel. Click **Networking**. Select **Route table**.



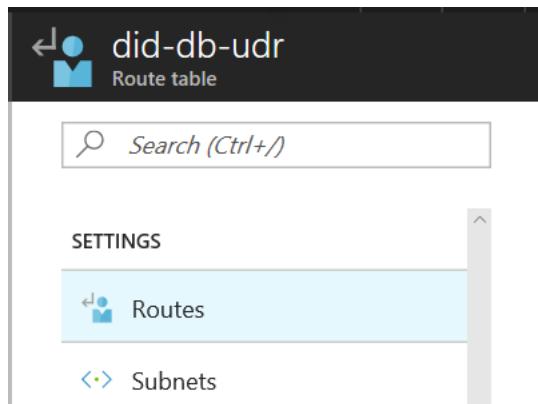
35. On the **Create route table** blade, enter name of the new route under **Name** setting.
36. Select subscription under **Subscription** setting.
37. Select **Use existing** under **Resource group**. Select **did-infra-rg** from the drop-down list.
38. Select your location under **Location** setting.
39. Click **Create**.



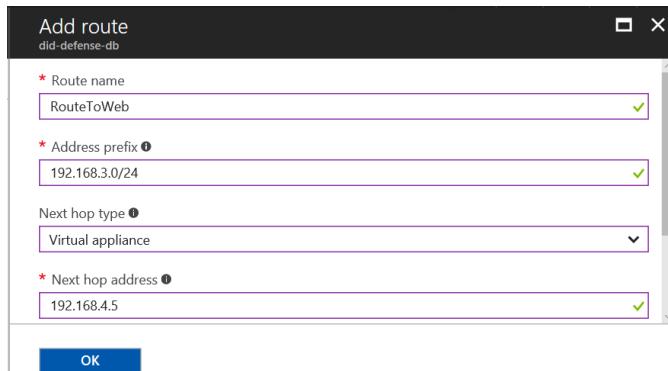
40. Open your newly created route table. You can add **Route tables** navigation to the left panel to easily manage it.

The screenshot shows the 'Route tables' blade in the Azure portal. It displays a list of route tables, with 'did-db-udr' selected. The blade includes a 'Subscriptions' section, a 'Filter by name...' input, and a 'Visual Studio Enterprise' dropdown.

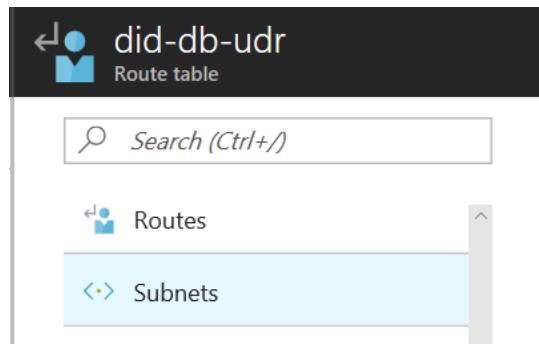
41. On the **did-db-udr** blade, click **Route**.



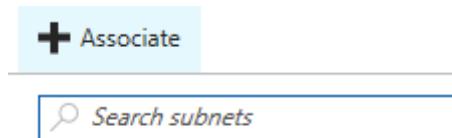
42. Click **Add**.
43. On the **Add route** blade, enter name of the new route under Route name setting.
44. Enter address range the route applies to. This is the range of your web front-end virtual machines.
45. Select **Virtual appliance** under **Next hop type** because you are using Barracuda.
46. Enter private IP address of the Barracuda virtual machine under **Next hop address**.
47. Click **OK**.



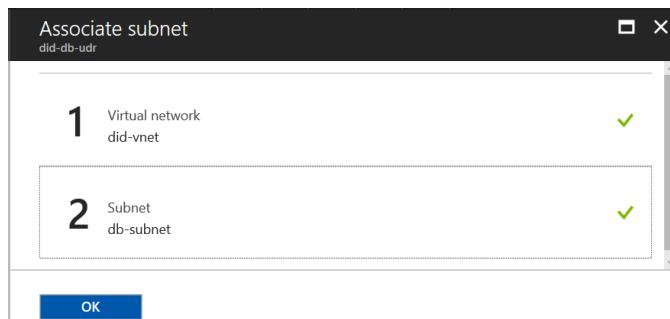
48. On the **did-db-udr – Routes** blade, click **Subnets**.



49. Click **Associate**.



50. On the **Associate subnet** blade, click **Virtual network** setting and select your private virtual network.  
51. Click **Subnet** setting and select web front-end subnet.  
52. Click **OK**.



53. Repeat from step 34 – 39 in this lab to create a route table to contain the route forcing traffic to database subnet to have to be gone through the firewall.

NAME	RESOURCE...	LOCATION
did-db-udr	did-infra-rg	Southeast Asia
did-web-udr	did-infra-rg	Southeast Asia

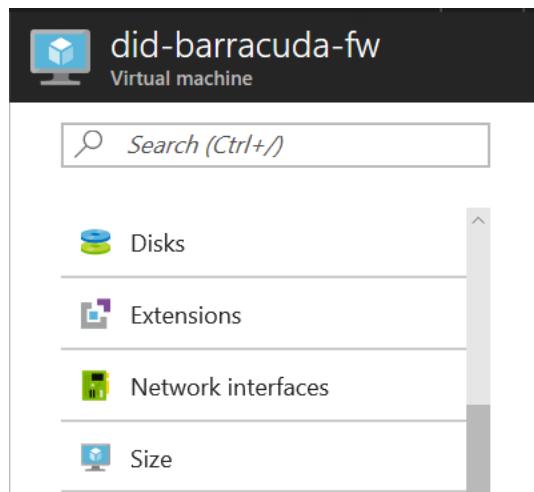
54. Repeat from step 40 – 47 in this lab to create a custom route for database subnet.

NAME	ADDRESS PREFIX	NEXT HOP
RouteToDB	192.168.2.0/24	192.168.4.5

55. Repeat from step 48 – 52 to associate the newly created route table to the web front-end subnet

NAME	ADDRESS RANGE	VIRTUAL NETWORK	SECURITY GROUP
web-subnet	192.168.3.0/24	did-vnet	did-dmz-nsg

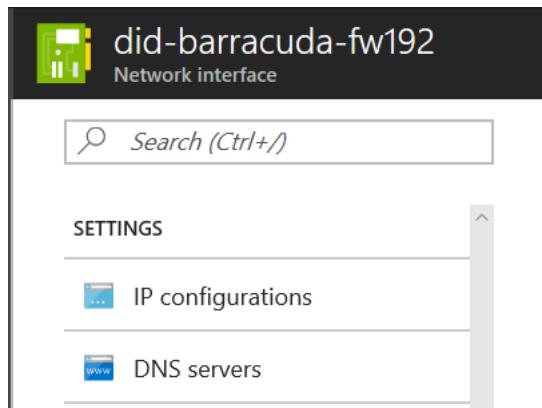
56. The last step is to enable IP Forwarding on Barracuda virtual machine. Otherwise, Barracuda does not forward network packet it receives to the destination.
57. Click your Barracuda virtual machine. On the **did-barracuda-fw** blade, click **Network interfaces**.



58. On the **Network interfaces** blade, click your network interface.

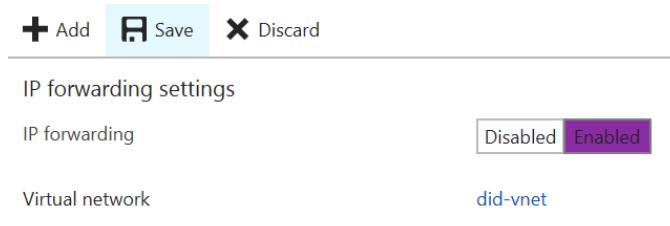
NAME	PUBLIC IP ADDRE...	PRIVATE IP ADD...	SECURITY GROUP
did-barracuda-fw192	52.187.14.198	192.168.4.5	did-barracuda-fw-n... ...

59. On your network interface blade, click **IP configurations**



The screenshot shows the Barracuda Firewall's Network interface configuration screen. The title bar says 'did-barracuda-fw192' and 'Network interface'. A search bar at the top says 'Search (Ctrl+/)'. Below it is a 'SETTINGS' section with two items: 'IP configurations' and 'DNS servers'. At the bottom is a toolbar with 'Add', 'Save' (which is highlighted in blue), and 'Discard' buttons.

60. Select **Enabled** in **IP forwarding** setting.
61. Click **Save**.



The screenshot shows the 'IP forwarding settings' page. It has a 'Virtual network' dropdown set to 'did-vnet' and an 'IP forwarding' switch that is currently set to 'Enabled' (highlighted in purple). There are 'Add', 'Save', and 'Discard' buttons at the top.

62. Now network traffic among your web front-end virtual machines and database virtual machines are routed to Barracuda firewall first.
63. You should configure more route table for network traffic for your Active Directory virtual machine.

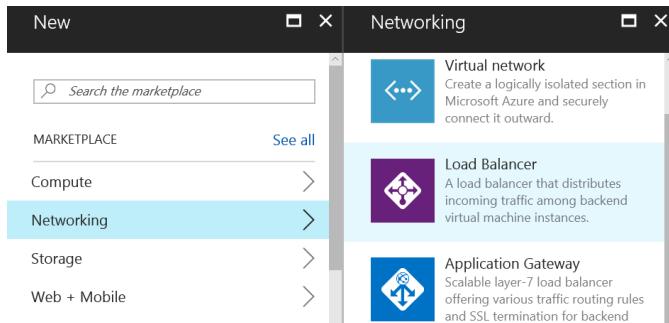
Now you have completed this lab.

## Lab 2.8 – Deploying Azure Load Balancer

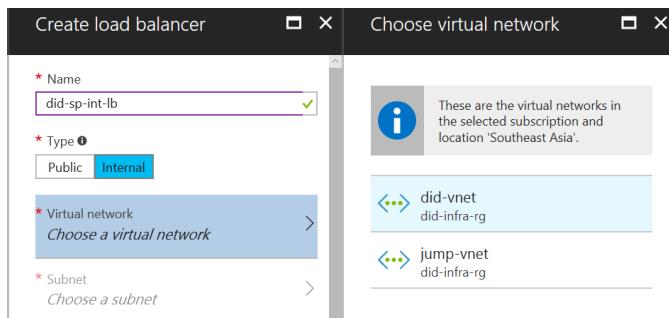
In Chapter 3, Network Availability section, we discussed about availability and how Azure could help. Azure Load Balancer works at Layer 4 (TCP, UDP) in the OSI model to distribute network traffic to virtual machines. In the context of this book, we aim to provide availability for network traffic among the web front-end virtual machines. This lab is going to walk you through steps to deploy Azure Load Balancer to distribute network traffic between two web front-end virtual machines we already created and configured previously.

Perform the following steps to complete the lab:

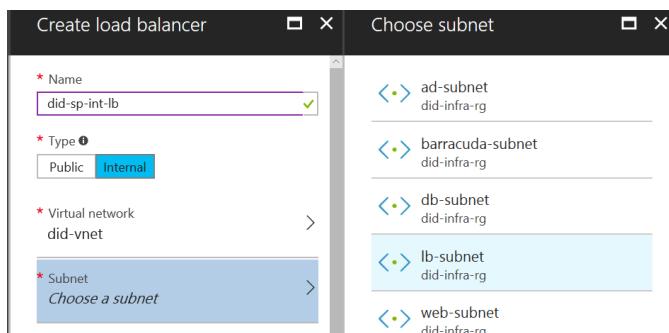
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **New**.
3. Click **Load Balancer**.



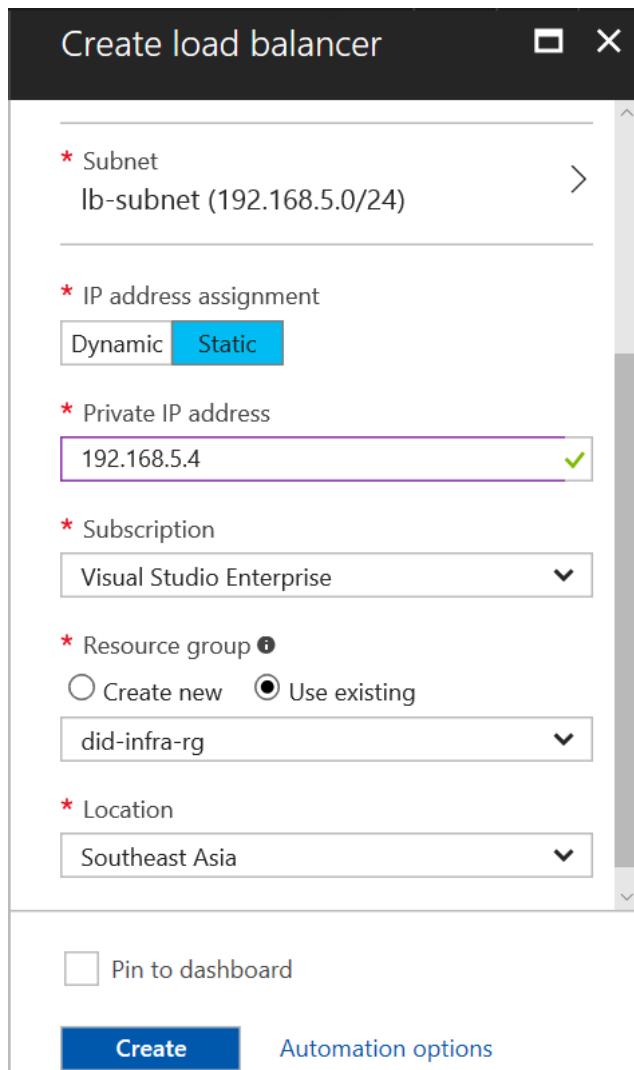
4. On the **Create load balancer** blade, enter name of the new load balancer.
5. Select **Internal** under **Type** setting.
6. Click **Virtual network** and select your private virtual network.



7. Click **Subnet** setting, select a dedicated subnet for your load balancer. If you have not created it yet, refer to *Lab 1.4*.



8. Select **Static** under IP address assignment setting.
9. Enter the private IP address under **Private IP address** setting.
10. Select your subscription under **Subscription** setting.
11. Select **Use existing** under **Resource group** setting. Select **did-infra-rg** from the drop-down list.
12. Select your location under **Location** setting.
13. Click **Create**.



14. Open your newly created load balancer. You can find it from **More services**. If you need to quickly navigate to it, add its navigation to the left panel.

The screenshot shows the 'Load balancers' blade in the Azure portal. At the top, it displays 'Load balancers' and 'TS Consulting (nnthuanlive.onmicrosoft.com)'. Below this are three buttons: 'Add', 'Columns', and 'Refresh'. A 'Subscriptions' section indicates '1 of 2 selected – Don't see a subscription?'. A 'Filter by name...' input field is present. The main list shows '1 items' with a single entry: 'did-sp-int-lb'.

NAME
did-sp-int-lb

15. Click the newly created load balancer. On the **did-sp-int-lb** blade, click **Backend pool**.

The screenshot shows the 'did-sp-int-lb' blade in the Azure portal. At the top, it displays the load balancer name and 'Load balancer'. A search bar is present. The left sidebar has a 'Tags' section and a 'Diagnose and solve problems' section. The 'SETTINGS' section is expanded, showing 'Frontend IP pool', 'Backend pools' (which is highlighted in blue), and 'Health probes'.

SETTINGS
Frontend IP pool
Backend pools
Health probes

16. Click **Add**.

<span style="font-size: 2em; font-weight: bold;">+</span> Add	
<span style="font-size: 1.5em; font-weight: bold;">Search backend address pools</span>	
VIRTUAL MACHINE	STATUS
No results.	

17. On the **Add backend pool** blade, enter name of the new backend pool under **Name** setting.
18. Select **Availability set** under **Associated to** setting.
19. Select the existing web front-end availability set.

**Add backend pool**  
did-sp-int-lb

<b>Name</b>	Web-BackendPool	✓
<b>IP version</b>	IPv4	
<b>Associated to</b>	Availability set	▼
<b>Availability set</b>	web-av-set number of virtual machines: 2, resource group: did-web-rg	▼

20. Click **Add a target network IP configuration**.
21. Select the first web front-end virtual machine from the drop-down list under **Target virtual machine** setting.
22. Select the network interface of **did-web01-vm** virtual machine under **Network IP configuration** setting.

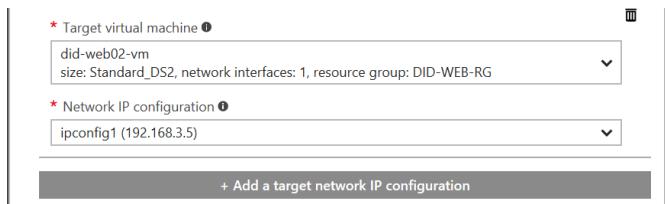
Target network IP configurations

Only VMs within the current availability set can be chosen. Once a VM is chosen, you can select a network IP configuration related to it.

<b>Target virtual machine</b>	did-web01-vm size: Standard_DS2, network interfaces: 1, resource group: DID-WEB-RG	▼
<b>Network IP configuration</b>	ipconfig1 (192.168.3.4)	▼
<b>+ Add a target network IP configuration</b>		

23. Click **Add a target network IP configuration** to add the second web front-end virtual machine.

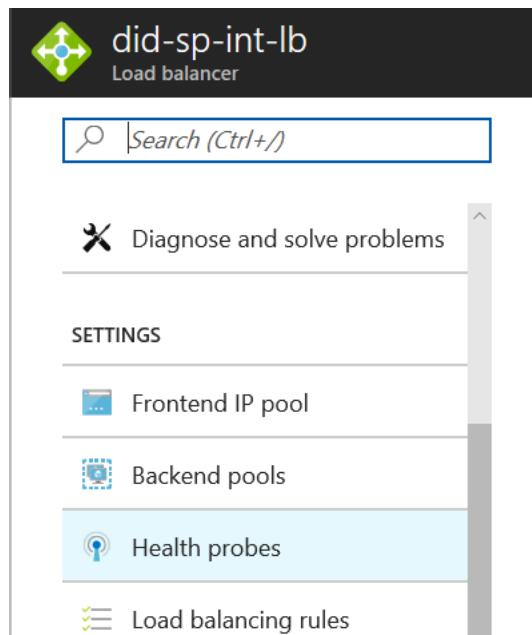
24. Select the second web front-end virtual machine from the drop-down list under **Target virtual machine** setting.
25. Select the network interface of **did-web02-vm** virtual machine under **Network IP configuration** setting.
26. Click **OK**.



27. Verify the list of added virtual machines in your backend pool.

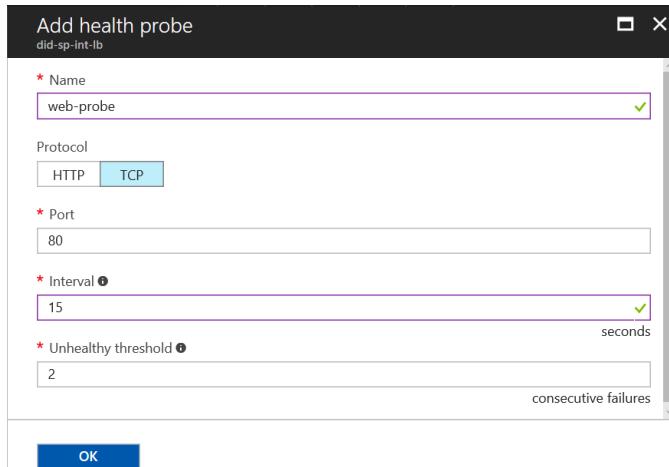
VIRTUAL MACHINE	STATUS	NETWORK INTERFACE	PRIVATE IP ADDRESS
▼ Web-BackendPool (2 virtual m...)			
did-web01-vm	Running	did-web01-vm120	192.168.3.4
did-web02-vm	Running	did-web02-vm884	192.168.3.5

28. On the **did-sp-int-lb** blade, click Health probes to create a probe to monitor the load balancer's health.

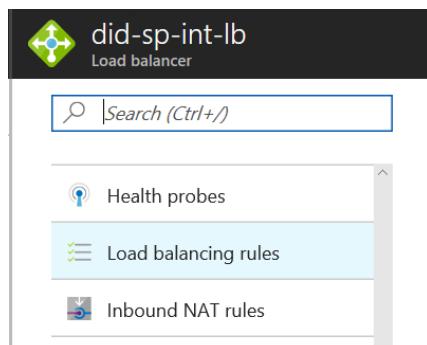


29. Click **Add**.
30. On the Add health probe blade, enter name of the new probe for your web front-end layer.
31. Select **TCP** under **Protocol** setting
32. Enter port **80** under **Port** setting. If you use secure protocol such as **HTTPS**, the port is supposed to be **443**.
33. Enter interval value under **Interval** setting.
34. Enter the threshold value under **Unhealthy threshold** setting. This is to determine the number of consecutive probe failure before the load balancer considers that the web front-end virtual machine is unhealthy.

35. Click **OK**.

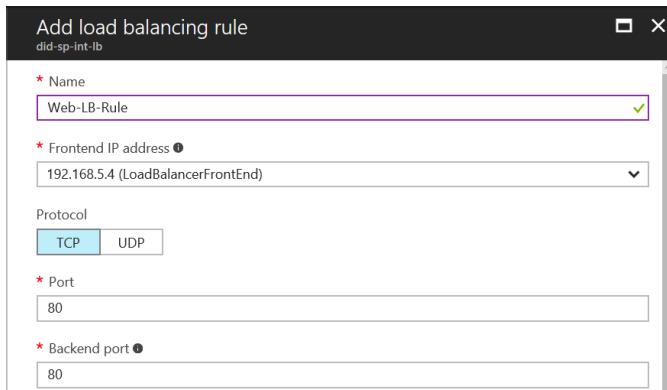


36. On the **did-sp-int-lb** blade, click **Load balancing rules**.

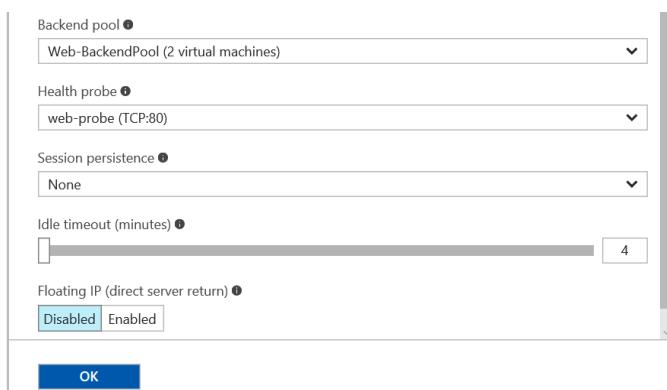


37. Click **Add**.

38. On the **Add load balancing rule** blade, enter name of the new load balancing rule for web front-end layer.
39. The private IP address of your load balancer is automatically selected under **Frontend IP address** setting.
40. Select **TCP** under **Protocol** setting.
41. Enter port value under **Port** setting.
42. Enter port value under **Backend port** setting



43. Your backend pool you created is automatically selected under **Backend pool** setting.
44. Your health probe you created is automatically selected under **Health probe** setting.
45. Select **None** under **Session persistence** setting.
46. Configure the minute value under **Idle timeout (minutes)** setting.
47. Select **Disabled** under **Floating IP (direct server return)** setting.
48. Click **OK**.



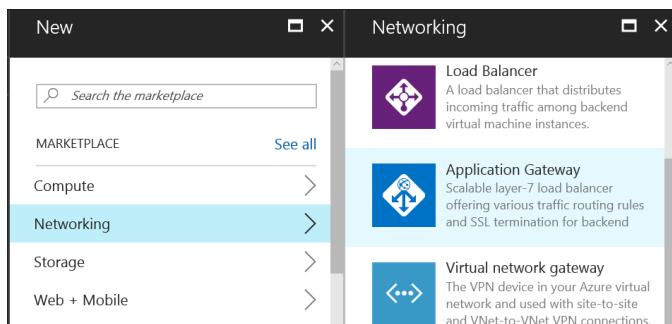
Now you have completed this lab. We will do the test after creating an Azure Application Gateway to publish SharePoint site over the Internet through this gateway.

## Lab 2.9 – Deploying Azure Application Gateway

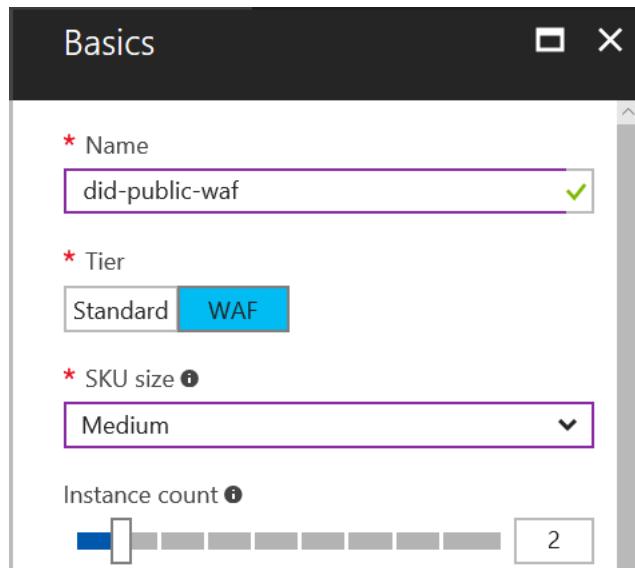
You previously created an internal load balancer to distribute network traffic among two web front-end virtual machines. The load balancer does not interface with Internet so the SharePoint website is not accessible when you connect from the Internet. In Chapter 3, Network Availability section we mentioned Azure Application Gateway which is a web application firewall working at Layer 7 in the OSI model. The Azure Application Gateway also provide HTTP-based load balancing functionality. This lab is going to walk you through steps to deploy a new Azure Application Gateway into your existing SharePoint environment.

Perform the following steps to complete the lab:

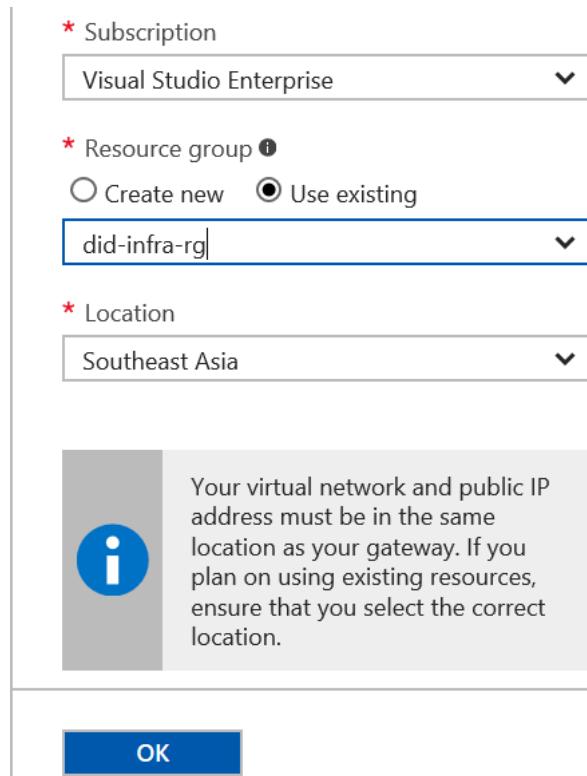
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **New**.
3. Click **Application Gateway**



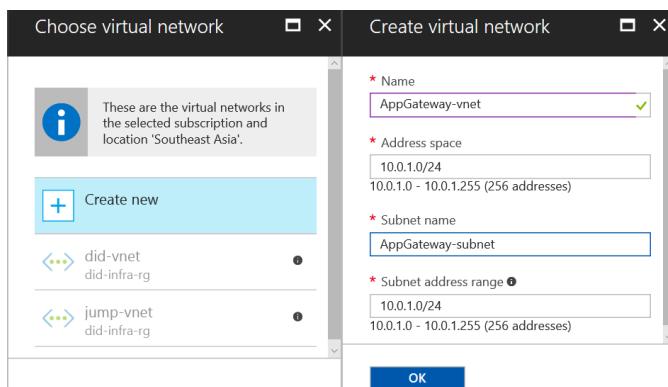
4. On the **Basics** blade, enter name of the new application gateway under **Name** setting.
5. Select **WAF** under **Tier** setting to take fully advantages of web application firewall including OWASP rules.
6. Select **Medium** under **SKU size** setting.
7. Configure the number of instances under **Instance count** setting. Keep it by default as **2** for evaluation purpose.



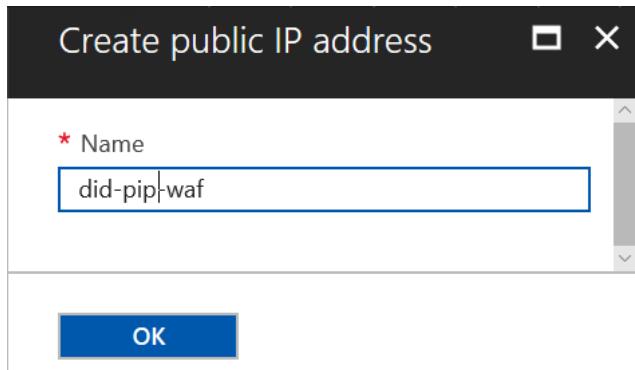
8. Select your subscription under **Subscription** setting.
9. Select **Use existing** under **Resource group** setting. Select **did-infra-rg** from the drop-down list.
10. Select your location under **Location** setting. Pay attention to the warning message that your virtual network and public IP address must be in the same location as your gateway.
11. Click **OK**.



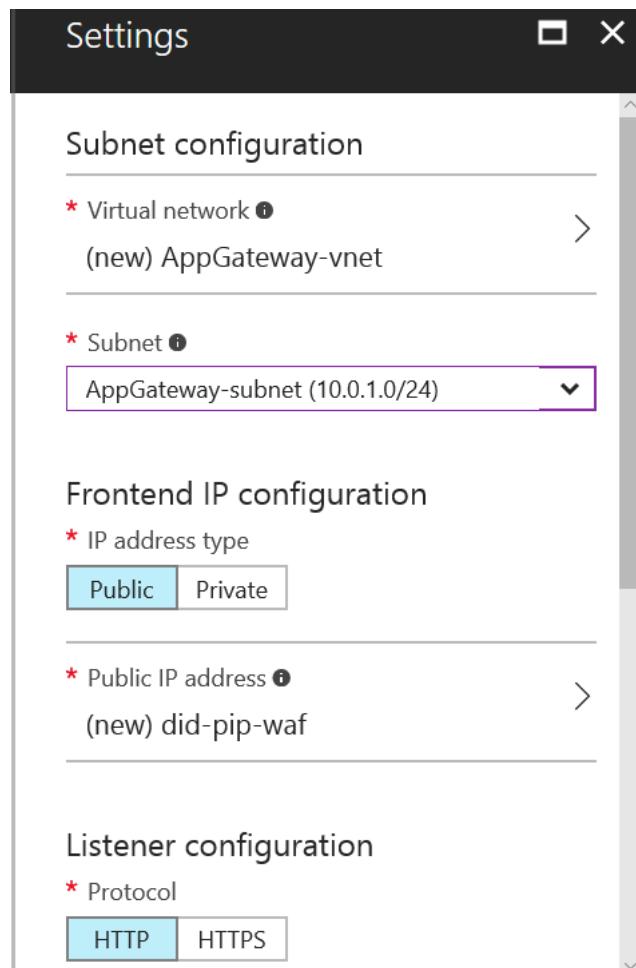
12. On the **Setting** blade, click **Virtual network** setting. Choose a dedicated virtual network. If you have not created it yet, refer **Lab 1.3** to create a new virtual network for your application gateway.
13. You can directly create a new virtual network including subnet by clicking **Click new** on the **Choose virtual network** blade.
14. Click **OK**.



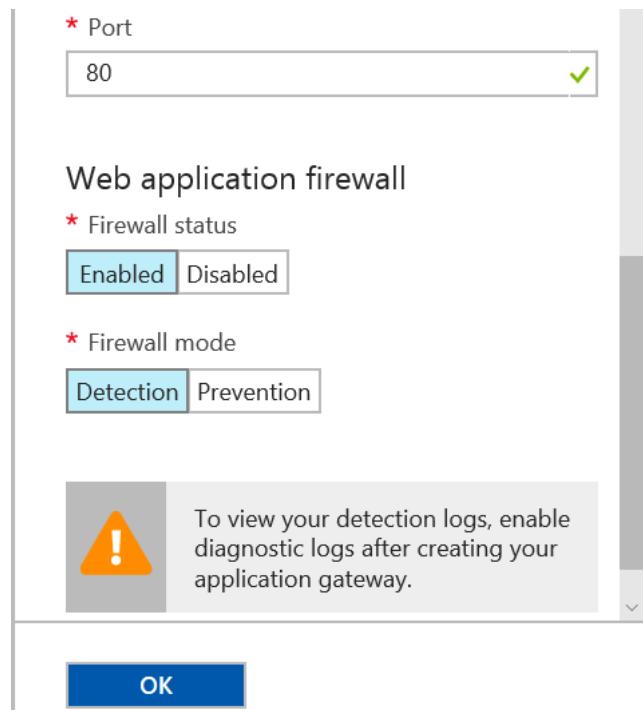
15. Select **Public** under **IP address type** because you are creating a public-facing application gateway.
16. Click **Public IP address** setting. On the **Choose public IP address** setting, click **Create new**.
17. On the **Create public IP address** blade, enter name of the new public IP address for the new application gateway.
18. Click **OK**.



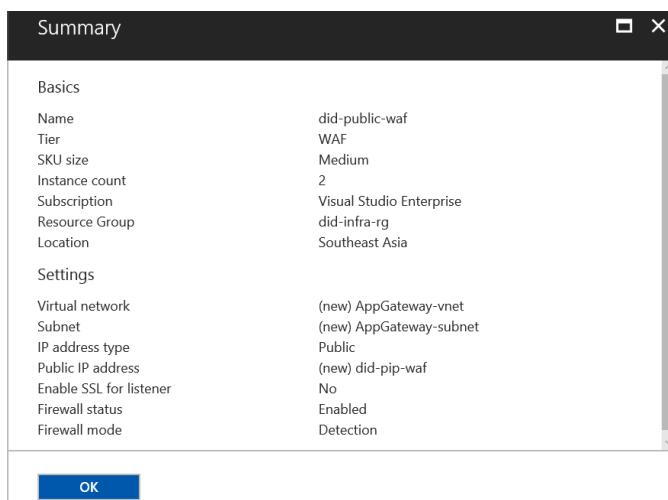
19. Select **HTTP** under **Protocol** setting.



20. Enter port 80 under **Port** setting.
21. Select **Enabled** under **Firewall** status.
22. Select **Detection** under **Firewall** mode. This configuration allows you to review log to perform deep assessment when your firewall receives attacks.
23. Click **OK**.



24. On the **Summary** blade, review information of your application gateway.
25. Click **OK**.



26. Open your application gateway from **More services**.

Application gateways  
TS Consulting (nnthuanlive.onmicrosoft.com)

**+** Add   **Columns**   **Refresh**

**Subscriptions:** 1 of 2 selected – Don't see a subscription? [Switch directories](#)

1 items

NAME	PUBLIC IP ADDR...	PRIVATE IP ADD...	RESOURCE...
 did-public-waf	52.187.73.156	-	did-infra-rg

27. On the **did-public-waf** blade, click **Backend pools**.

 **did-public-waf**  
Application gateway

 Configuration

 Web application firewall

 Backend pools

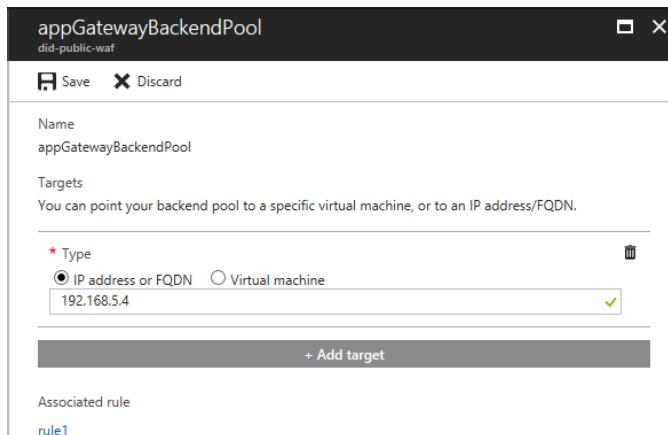
 HTTP settings

28. There is a default backend pool. Click it.

**+** Add

NAME	RULES ASSOCIATED
appGatewayBackendPool	1

29. On the **appGatewayBackendPool** blade, click **Add target**.



30. Select **IP address or FQDN** under **Type** setting.
31. Enter the front-end IP address of your internal load balancer.
32. Click **Save**.
33. Now you can test by opening the public IP address of the application gateway on your browser. Enter your SharePoint administrator account (`tsconsulting\sp_admin`) when being asked.

Now you have completed this lab.

## Lab 3 – Virtual Machine and Storage Protection

In Chapter 4, we explored some built-in features Microsoft Azure provides to help protect virtual machine and storage. In Lab 3, we will aim to secure virtual machine and storage by implementing storage encryption, disk encryption, Microsoft antimalware and automated hardening configuration.

### Lab 3.1 – Implementing Disk Encryption

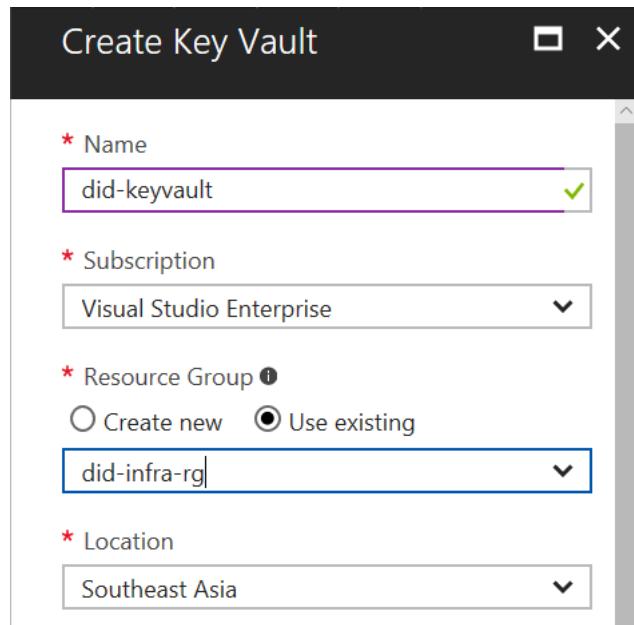
In *Chapter 4, Disk Encryption* section, you were introduced Azure Disk Encryption which allows you to secure disk storing OS and VM. In practical scenario, Disk Encryption works with Azure Key Vault to store secret key. This lab is going to walk you through steps to enable Disk Encryption.

Perform the following steps to complete the lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Azure Key Vault**. If it has not been added yet, click More services and search for **Key vaults**.

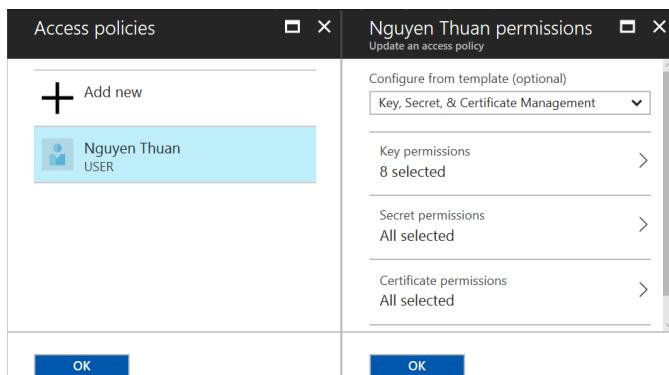
The image shows a screenshot of the Azure Management Portal. At the top, there is a search bar with the placeholder text 'Shift+Space to toggle favorites'. A user has typed 'key va' into the search bar. To the right of the search bar is a close button (an 'X'). Below the search bar, a blue header bar is visible with the text 'Key vaults' and a star icon for favoriting. The main content area is titled 'Key vaults' and shows the text 'TS Consulting (nnthuanlive.onmicrosoft.com)'. Below this, there are three buttons: a plus sign for 'Add', a grid icon for 'Columns', and a circular arrow for 'Refresh'. A horizontal line separates this from the next section. The next section is titled 'Subscriptions' and shows 'All 2 selected'. It includes a link 'Don't see a subscription? Swap' and a 'Filter by name...' input field.

3. On the **Key vaults** blade, click **Add**.
4. On the **Create Key Vault** blade, enter name of the new key vault under **Name** setting.
5. Select your subscription under **Subscription** setting.
6. Select **Use existing** under **Resource Group** setting. Select **did-infra-rg** from the drop-down list.
7. Select your location under **Location** setting.

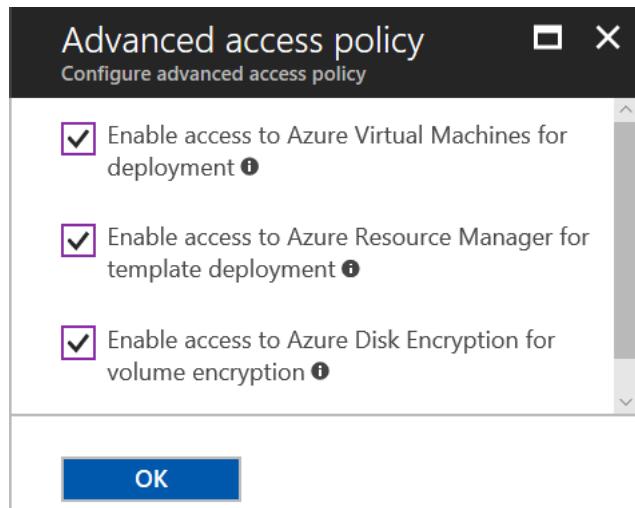


8. Keep **Pricing tier** setting by default with **Standard** tier.
9. Click **Access policies** to specify who to manage key vault.
10. On the **Access policies** blade, choose the user you want.
11. On the permission blade, select **Key, secret, & Certificate Management** under **Configure from template (optional)** setting.

12. Click **OK**.



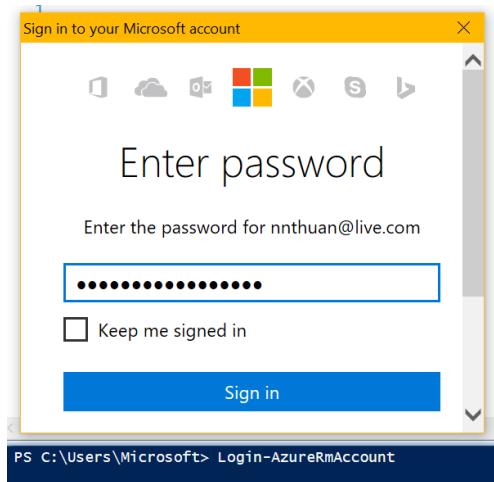
13. Click **Advanced access policy** setting. On the **Advanced access policy** blade, select three options.
14. Click **OK**.



15. Click **Create**.
16. Wait a few minutes until the creation process is completed.

NAME	TYPE	RESOUR...
 did-keyvault	Key vault	did-infra-rg

17. Open PowerShell ISE and run **Login-AzureRM** to log into your Azure. You are prompted to provide Azure subscription account.



18. Make sure PowerShell returns your Azure information before you move on.

```
PS C:\Users\Microsoft> Login-AzureRmAccount

Environment          : AzureCloud
Account             : nnthuan@live.com
TenantId            : 03987603-0fc0-4103-bd94-cdfffbefb2226
SubscriptionId      : 2dd8cb59-ed12-4755-a2bc-356c212fbafc
SubscriptionName    : Visual Studio Enterprise
CurrentStorageAccount :
```

19. Open the Azure Disk Encryption Prerequisite file provided by Microsoft from this URL  
<https://raw.githubusercontent.com/Azure/azure-powershell/master/src/ResourceManager/Compute/Commands.Compute/Extension/AzureDiskEncryption/Scripts/AzureDiskEncryptionPreRequisiteSetup.ps1>. Copy the code and paste into PowerShell ISE.
  20. The PowerShell asks you several information including key vault information you created from the beginning.
  21. Copy **addClientID**, **addClientSecret**,  
**diskEncryptionKeyVaultUrl**, **keyVaultResourceId** from the PowerShell screen into a NotePad file before you press Enter.

22. Copy the following PowerShell code snipping with correct value you copied, including virtual machine name and resource group that the virtual machine you need to encrypt its disks.

```
$vmName = 'did-ad-vm'
$resourceGroupName = 'did-ad-rg'
$aadClientID = '9fc8a638-a495-43e9-b951-aa7b9109836c'
$aadClientSecret = '045d7535-3c58-4c28-acd9-064a12f09134'
$diskEncryptionKeyVaultUrl = 'https://did-
keyvault.vault.azure.net/'
$keyVaultResourceId = '/subscriptions/2dd8cb59-ed12-4755-
a2bc-356c212fbafc/resourceGroups/did-infra-
rg/providers/Microsoft.KeyVault/vaults/did-keyvault'

Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName
$resourceGroupName -VMName $vmName -AadClientID
$aadClientID -AadClientSecret $aadClientSecret -
DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $keyVaultResourceId
```

23. You are asked to confirm to encrypt the disk on the target virtual machine. Click **Yes**.



24. Wait around 10-15 minutes until the encryption process is completed.
25. You can verify by checking encryption status in **DISK ENCRYPTION** column.

NAME	STATUS	DISK ENCRYPTION
did-ad-vm	Running	Enabled

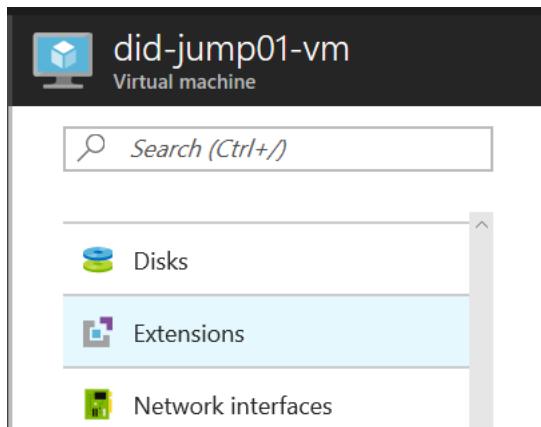
Now you have completed this lab.

## Lab 3.2 – Installing Microsoft Antimalware Extension

Microsoft Azure offers number of different extensions for your virtual machine. One of them that you need to pay attention to is Microsoft Antimalware. In Chapter 4, Antimalware for Virtual machine section, you were introduced this extension. This lab is going to walk you through steps to enable Microsoft Antimalware for your virtual machine (namely the jump virtual machine) via Azure Management Portal.

Perform the following steps to complete the lab:

26. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
27. From the left panel, click **Virtual machines**.
28. Click **did-jump01-vm** virtual machine.
29. On the **did-jump01-vm** blade, click **Extensions**.

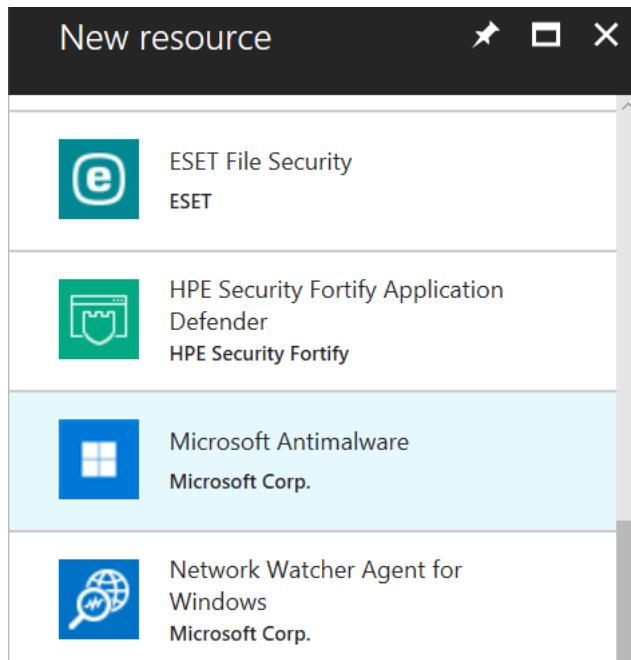


30. On the **Extensions** blade, there is one extension named **IaaS Diagnostics** which has been already installed during your virtual machine provisioning.
31. Click **Add**

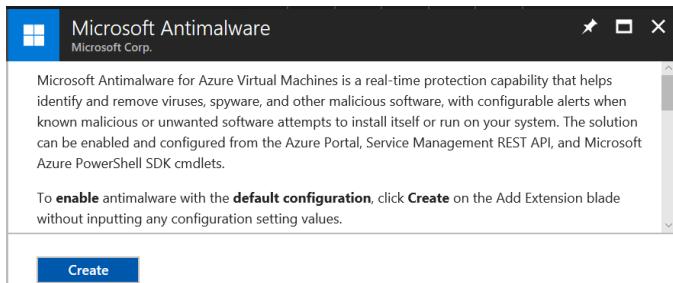
A screenshot of the 'Add extension' blade. The table shows one item: 'IaaS Diagnostics' (Type: Microsoft.Azure.Diagnostics.I... Status: Provisioning succeeded).

NAME	TYPE	V...	STATUS
IaaS Diagnostics	Microsoft.Azure.Diagnostics.I...	1.*	Provisioning succeeded

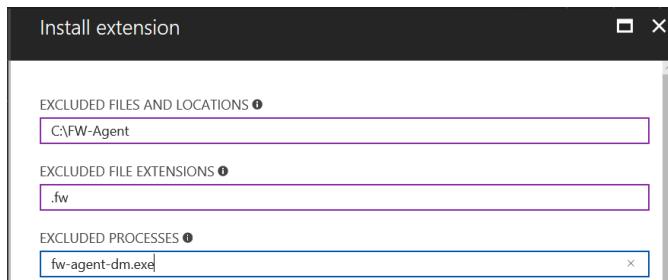
32. On the **New resource** blade, click **Microsoft Antimalware**.



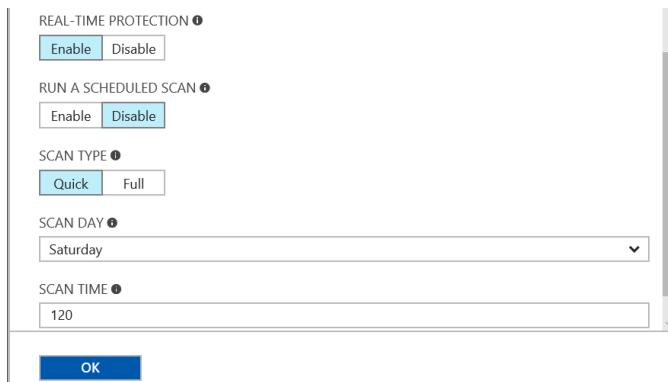
33. On **Microsoft Antimalware** blade, click **Create**.



34. On the **Install extension** blade, you need to set up some specific configurations for your Antimalware.
35. Enter excluded file and location you do not want Microsoft Antimalware client application scan under **EXCLUDED FILE AND LOCATION** setting.
36. Enter excluded file extensions under **EXCLUDED FILE EXTENSIONS** setting.
37. Enter excluded processes under **EXCLUDED PROCESSES** setting.



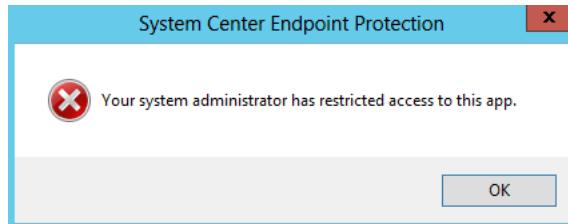
38. Select **Enable** under **REAL-TIME PROTECTION** setting.
39. Select **Enable** or **Disable** under **RUN A SCHEDULED SCAN** setting. If you select **Disable**, you can still configure a schedule directly from the Antimalware tool.
40. Select **Quick** or **Full** under **SCAN TYPE** setting.
41. Set you date you wish the Antimalware tool to scan and scan time under **SCAN TIME** setting. You can hover your mouse on the tooltip icon to understand this setting.
42. Click **OK**.



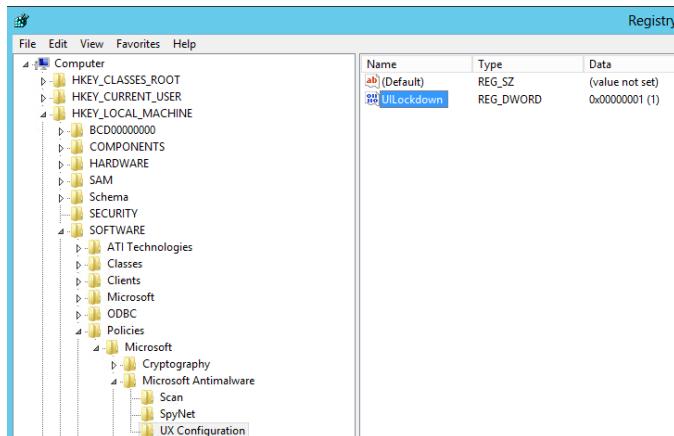
43. Wait around 5 – 10 minutes until the installation is complete.
44. If the OS is Windows Server 2016, the Antimalware client is Windows Defender. If the OS is Windows Server 2012, it is System Center Endpoint Protection.



45. By default, Microsoft Antimalware does not provide Graphic User Interface (GUI) version in Windows Server 2012. When you open you will receive the error message below:

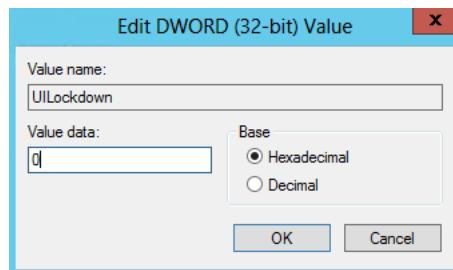


46. However, you can enable GUI version. Go to registry path:  
*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policy\Microsoft Antimalware\UX Configuration*



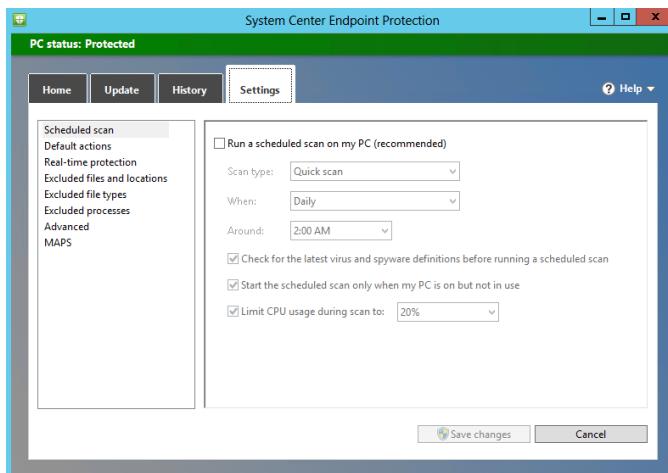
22. Click double on **UILockdown** key. Change the value under **Value data** setting from **1** to **0**.

23. Click **OK**.



24. Open **System Center Endpoint Protection** again.

25. You can configure your antimalware from the GUI version in **Settings** tab.



Now you have completed this lab.

## Lab 3.3 – Automating hardened configuration

During the time working with the Government Cloud operation team, I was responsible for deploying hardening scripts for Windows Server 2008 and 2012 after virtual machines were successfully provisioned. This type of deployment is to make sure that all security configuration is consistently applied to every virtual machine in your system. In Microsoft Azure, you can RDP to every virtual machine to run a hardening script. However, this takes time and is not considered a practical deployment. This lab is going to walk you through steps to automate hardening script deployment using Azure Desired State Configuration (DSC).

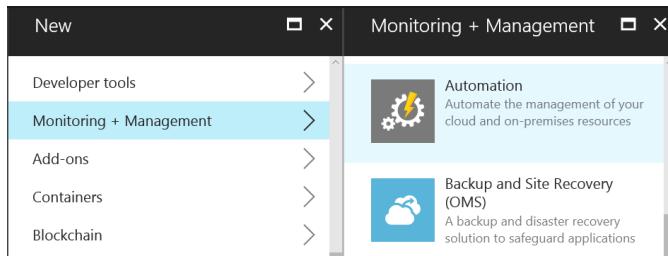
---

Before this lab, I highly recommend you to learn DSC structure and how to write a workable DSC configuration file with PowerShell.

---

Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **New**.
3. Click **Monitoring + Management**. Click **Automation**.



4. On the **Add Automation Account** blade, enter name of the new automation account.
5. Select your subscription under **Subscription** setting.
6. Select **Use existing** under **Resource group** setting. Select **did-infra-rg** from the drop-down list.
7. Select your location under **Location** setting.
8. Select **Yes** under **Create Azure Run As account** setting.
9. Click **Create**.

Add Automation Account X

\* Name i  
 ✓

\* Subscription

\* Resource group i  
 Create new  Use existing

\* Location

\* Create Azure Run As account i

Pin to dashboard

Create

The Run As account feature will be available after the account is created.

10. You can add **Automation Accounts** navigation to the left panel.
11. Click to open your automation account

Automation Accounts  
TS Consulting (nnthuanlive.onmicrosoft.com)

**Subscriptions:** 1 of 2 selected – Don't see a subscription? [Switch](#)

[Visual Studio Enterprise](#)

No grouping		
NAME	TYPE	RESOUR...
 <a href="#">did-auto-account</a>	Automation...	<a href="#">did-infra-rg</a>

12. On the **did-auto-account** blade, click **Modules Gallery**.

**did-auto-account**  
Automation Account

SHARED RESOURCES

 [Hybrid worker groups](#)

 [Schedules](#)

 [Modules](#)

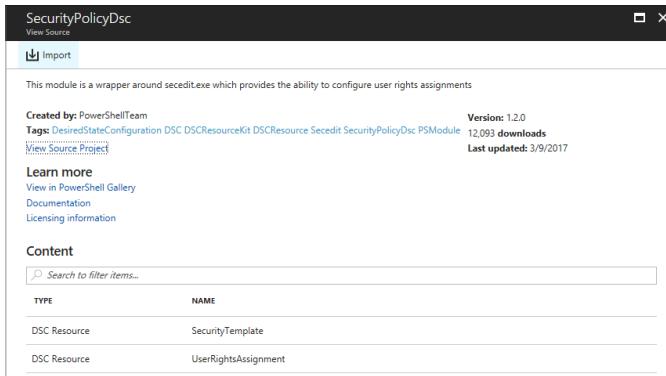
 [Modules Gallery](#)

 [Credentials](#)

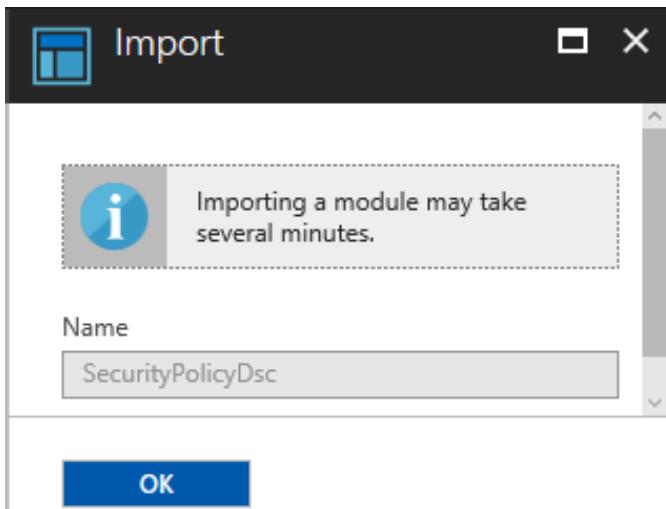
13. On the **Modules Gallery** blade, enter security on the search box and press **Enter**.
14. In the result, click **SecurityPolicyDsc** to add the module to your automation account.



15. On the **SecurityPolicyDsc** blade, click **Import**.



16. On the **Import** blade, click **OK**.



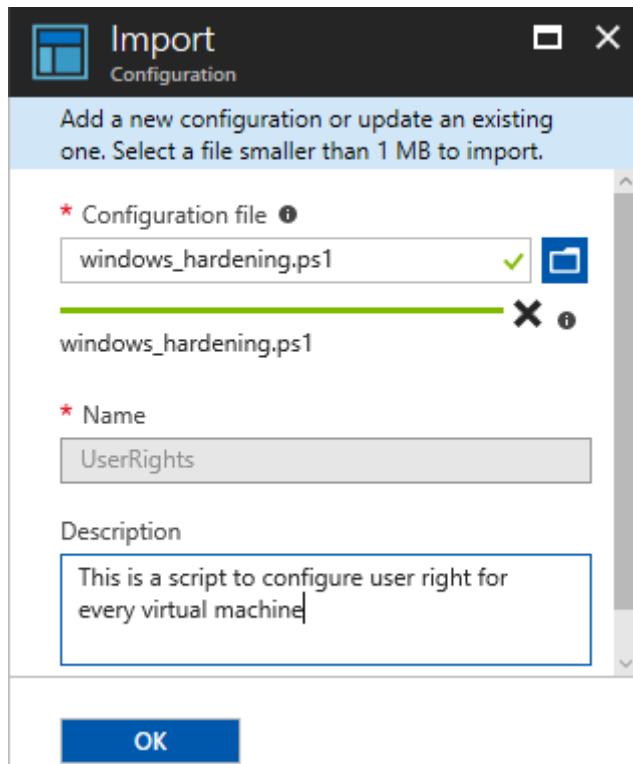
17. Click **Modules** to review all available modules, including the one you just imported.

NAME	LAST MODIFIED	STATUS
Azure	4/15/2017 4:46 AM	Available
Azure.Storage	4/15/2017 4:52 AM	Available
AzureRM.Automation	4/15/2017 4:50 AM	Available
AzureRM.Compute	4/15/2017 4:50 AM	Available
AzureRM.Profile	4/15/2017 4:49 AM	Available
AzureRM.Resources	4/15/2017 4:51 AM	Available
AzureRM.Sql	4/15/2017 4:51 AM	Available
AzureRM.Storage	4/15/2017 4:52 AM	Available
Microsoft.PowerShell.Core	4/15/2017 4:46 AM	Available
Microsoft.PowerShell.Diagnostics	4/15/2017 4:47 AM	Available
Microsoft.PowerShell.Management	4/15/2017 4:47 AM	Available
Microsoft.PowerShell.Security	4/15/2017 4:48 AM	Available
Microsoft.PowerShell.Utility	4/15/2017 4:48 AM	Available
Microsoft.WSMAN.Management	4/15/2017 4:49 AM	Available
Orchestrator.AssetManagement.Cmdlets	4/15/2017 4:51 AM	Available
SecurityPolicyDsc	5/22/2017 9:20 PM	Available

18. Click **DSC configurations**.
19. Click **Add a configuration**.

NAME
No DSC configurations found.

20. On the **Import** blade, click folder icon to browse to your DSC configuration file. This is your hardening PowerShell script. The name is automatically populated from the pre-defined parameter in the script.
21. Click **OK**.



22. Click on your newly added script

Recent configurations		
NAME	AUTHORIZING STATUS	LAST MODIFIED
UserRights	Published	5/22/2017 9:35 PM

23. On the blade, click **Compile**.

UserRights	
Configuration	
Essentials	
Resource group	Account
<a href="#">did-infra-rg</a>	did-auto-account
Location	Subscription name
southeastasia	<a href="#">Visual Studio Enterprise</a>
Subscription ID	Status
2dd8ccb9-ed12-4755-a2bc-356c212fbafc	Published
Last published	Configuration source
5/22/2017 9:35 PM	<a href="#">View configuration source</a>

24. Azure asks you to confirm to compile your DSC configuration.  
Click **Yes**.

Compile DSC Configuration

Are you sure you want to compile this configuration? Any node configurations generated will be automatically placed on the Azure Automation DSC pull server. If node configurations with the same name exist on the pull server, they will be overwritten.

**Yes** **No**

25. You can check from the blade the compiling status.

Deployments to Pull Server

Compilation jobs

STATUS	CREATED	LAST UPDATED
Starting	5/22/2017 9:38 PM	5/22/2017 9:39 PM

26. After the compiling process is finished, you can check the status.

Deployments to Pull Server

Compilation jobs

STATUS	CREATED	LAST UPDATED
✓ Completed	5/22/2017 9:41 PM	5/22/2017 9:43 PM

27. go back to your automation blade, click DSC nodes to start adding your virtual machine.  
28. Click **Add Azure VM**.

did-auto-account - DSC nodes

Automation Account

CONFIGURATION MANAGEMENT

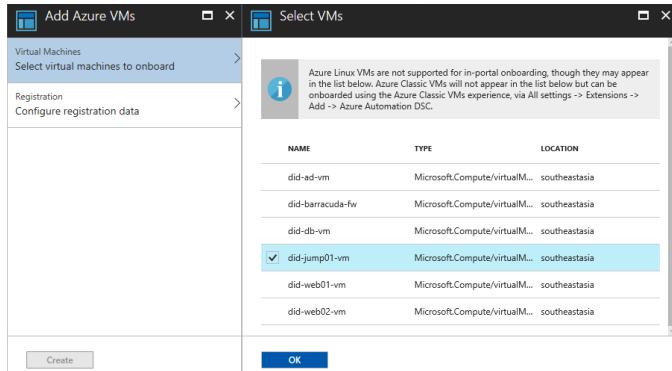
- DSC nodes**
- DSC configurations
- DSC node configurations

**+ Add Azure VM** **+ Add on-prem VM** **Learn more** **Refresh**

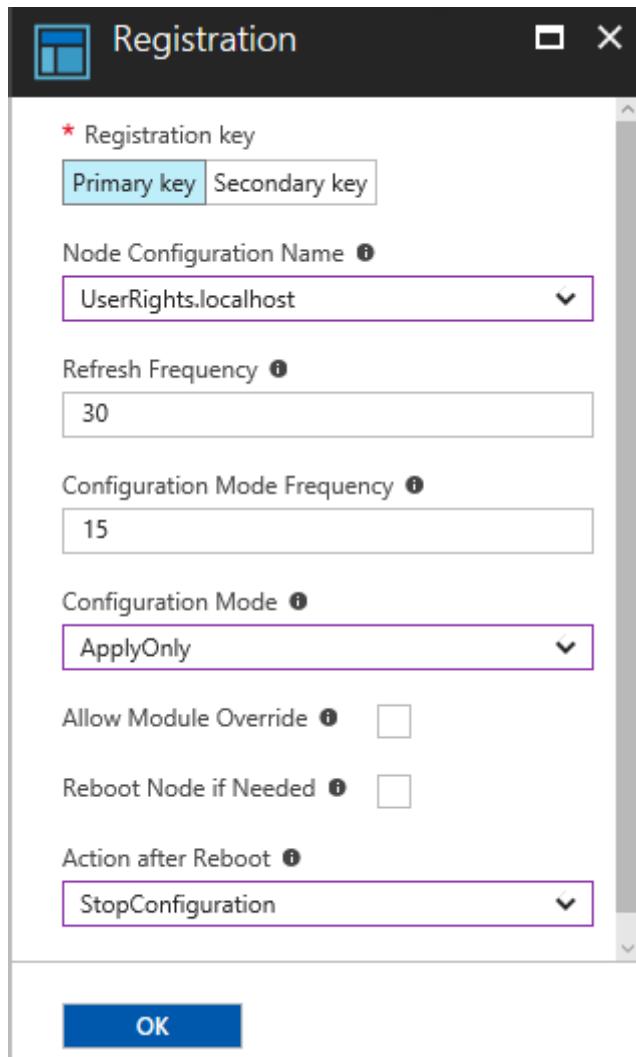
DSC nodes

No DSC nodes found.

29. On the **Add Azure VMs** blade, click **Virtual Machines** setting.  
Select the jump virtual machine as an example.
30. Click **OK**



31. Click **Registration** setting. On the **Registration** blade, select **Primary key** under **Registration key** setting.
32. Select your DSC configuration under **Node Configuration Name** setting.
33. Keep **Refresh Frequency** and **Configuration Mode Frequency** settings by default.
34. Select **ApplyOnly** under Configuration Mode setting.
35. Keep **Allow Module Override** and **Reboot Node if Needed** settings by default.
36. Select **StopConfiguration** under **Action after Reboot** setting.



37. Click **Create**.
38. During the process, **Microsoft.PowerShell.DSC** extension is automatically installed on the jump virtual machine.

NAME	TYPE	V...	STATUS	...
IaaSAntimalware	Microsoft.Azure.Security.IaaS...	1.*	Provisioning succeeded	...
IaaSDiagnostics	Microsoft.Azure.Diagnostics.I...	1.*	Provisioning succeeded	...
Microsoft.PowerShell...	Microsoft.PowerShell.DSC	2.*	Provisioning succeeded	...

39. RDP to the jump virtual machine to verify your hardening configuration which is successfully applied.

Now you have completed this lab. You need to add other virtual machines to apply your corporate hardening security configuration.

## Lab 4 – Manage your Identity

In Chapter 5, you were introduced number of different ways to manage your identity in the Azure Management Portal. As an Azure administrator, you do need to protect your account. If it is compromised, the attacker can destroy your infrastructure which hugely damages your entirely business. In Lab 4, we will configure role-based access control along with several techniques to mitigate brute-force attack.

### Lab 4.1 – Configure role-based access control

Role-Based Access Control helps you classify privilege you need to assign to individual account or group in your Azure Management Portal. This lab is going to walk you through steps to configure role-based access control for virtual machines.

Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. Navigate to the list of virtual machines and click any of them.
3. On the blade, click **Access control (IAM)**.
4. On the **Access control (IAM)** blade, click **Add**

did-jump01-vm - Access control (IAM)

Virtual machine

Search (Ctrl+F)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Availability set

Disks

Extensions

Network interfaces

Size

Name

Type

3 items (1 Users, 1 Groups, 1 Apps)

NAME	TYPE
did-auto-account_ckiHAu4BKRCQyU4T6rT9NjsNlabpf	App

CONTRIBUTOR

	Subscription admins	Group
--	---------------------	-------

OWNER

	TH	thuansg.1506	thuansg.1506@gmail.com	User
--	----	--------------	------------------------	------

5. On the **Add permissions** blade, select **Virtual Machine Contributor** under **Role**.
6. Select an account from the existing list.
7. Click **Save**.

Add permissions

Role

Select

biz  
biz@collapoint.onmicrosoft.com

Selected members:

CG Chris Green  
chris@nnthuanlive.onmicrosoft.com [Remove](#)

[Save](#) [Discard](#)

8. Verify from the list of access control in the selected virtual machine.

NAME	TYPE	ROLE	SCOPE
CONTRIBUTOR			
did-auto-account_c	App	Contributor	Inherited (Subscription)
thuansg.1506	User	Owner	Inherited (Subscription)
OWNER			
Subscription admins	Group	Owner	Inherited (Subscription)
Chris Green	User	Virtual Machine Co...	Assigned
VIRTUAL MACHINE CONTRIBUTOR			

9. If you want to review all assigned accounts in your virtual machine, click **Roles**.
10. On the **Roles** blade, click a role to see all assigned accounts.

NAME	USERS	GROUPS
Owner	1	1
Contributor	1	0
Reader	0	0
Virtual Machine Contributor	1	0
Dev/Test Lab User	0	0
Log Analytics Contributor	0	0
Log Analytics Reader	0	0
Monitoring Contributor Service Role	0	0
Monitoring Reader Service Role	0	0
User Access Administrator	0	0

USER	ACCESS
Chris Green chris@nnthuanlive.onmicrosoft.com	Assigned

Now you have completed this lab.

## Lab 4.2 – Enabling Multi-Factor Authentication for Microsoft Account

Multi-factor authentication is a security countermeasure to the brute-force attack. Without a second authentication step, the attacker cannot be successfully authenticated into your Azure Management portal. This lab is going to walk you through steps to enable multi-factor authentication for Microsoft account which is commonly used to log into Azure Management Portal.

Perform the following steps to complete this lab:

1. Log into the **Account** page to manage your security setting of Microsoft account here <https://account.microsoft.com/>
2. Navigate to **Security** page (<https://account.microsoft.com/security>)
3. Find the link to more security options at the bottom. You can browse this URL (<https://account.live.com/proofs/manage/additional?mkt=en-US&refd=account.microsoft.com&refp=security>)
4. You are asked to log into again before having access to the **Additional security options** page.
5. Under **Two-step verification**, click **Set up two-step verification**.

## Two-step verification

---

Two-step verification is an advanced security feature that makes [it right for you](#).

### [Set up two-step verification](#)

6. On the **Set up two-step verification** page, click **Next**.

## Set up two-step verification

Two-step verification adds an extra layer of protection to your account. After you've turned it on, we'll ask you to enter an additional security code when you sign in. We'll provide this security code only to you.

In the following steps, we'll help you:

1. Make sure you have up-to-date security info where you can receive security codes.
2. Set up an authenticator app if you have a smartphone. (With an authenticator app, you can get security codes even if your phone isn't connected to a cellular network.)
3. Create app passwords for apps and devices (such as Xbox 360, Windows Phone 8 (or earlier), or mail apps on your other devices) that don't support two-step verification codes.

 Next

Cancel

7. On the **Set up an identity verification app** page, select a mobile device you want to install the app on.
8. Click **Next**.

# Set up an identity verification app

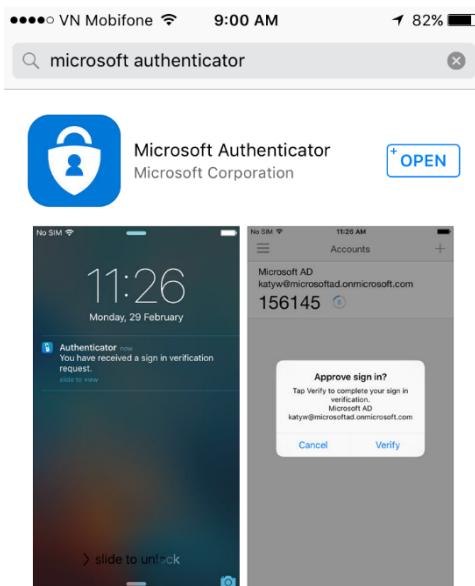
What mobile device do you want to install the app on?

- Windows Phone
- Android
- iPhone, iPad or iPod touch
- Other

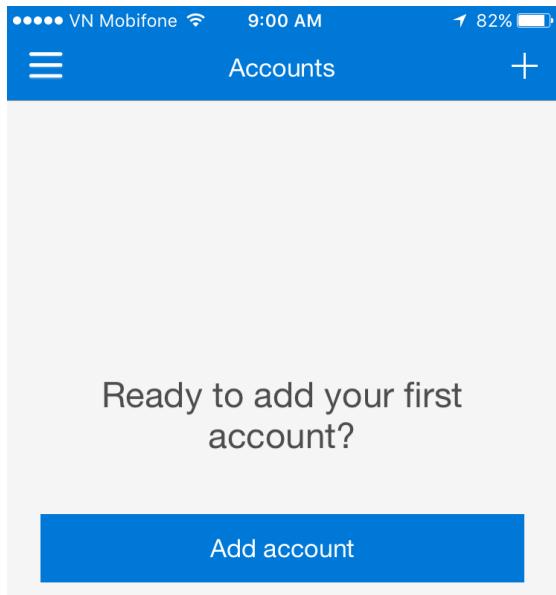
Next

Skip

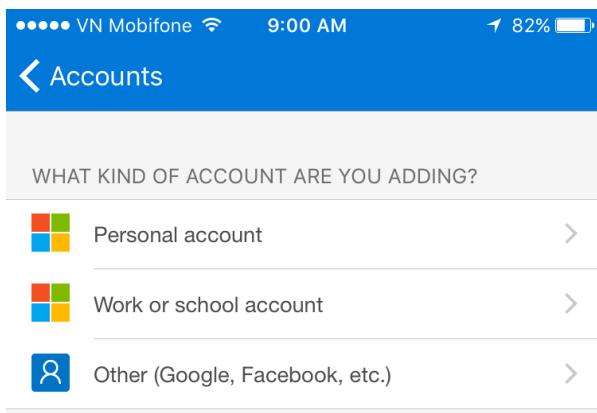
9. On the **Set up Microsoft Authenticator app** page, click the link to Microsoft Authenticator on the App Store to install the app. You can search for Microsoft Authenticator app on the App Store.



10. After you install the app, open the app. Click **Add account**.



11. Choose **Personal account**.



12. Use your Microsoft account when you are asked. Click **Next** to go to password page. Enter your password.

Cancel

## Sign in

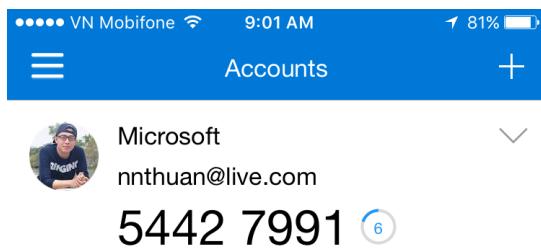
Use your Microsoft account.

[What's this?](#)

nnthuan@live.com

Next

- Once everything is successfully set up, your Microsoft account appears on the app.



- On the **Set up Microsoft Authentication** page, click **Next**.

### Set up Microsoft Authenticator app

- [Install the app from the App Store.](#) (This link will open in a new tab.)
- Open the app.
- Add your personal Microsoft account information.
- When you're done setting it up, tap or click **Next** below.

The next time you sign in to your account, you can verify your identity with the app.

Next

Skip

Don't have an iOS device? [Go back to pick a different device.](#)

- On the **Set up your smart phone with an app password** page, you are given an app password under the step 4 to use for other devices.

## Set up your smart phone with an app password

If you use a Windows Phone 8 (or earlier), you need to replace the Microsoft account password on your phone with an app password (Mail and the Store) don't accept security codes.

### Update your Windows Phone 8 (or earlier) with an app password

1. On your phone, open **Settings**
2. Tap **email+accounts**
3. Tap your Microsoft account.
4. Replace your password with the following app password:  
bbndinxpsxcgjwjr
5. Tap the **Done** icon

If you don't have your phone with you now, you can set it up with an app password later by visiting the security info page.

[Next](#)

16. On **Some other apps and devices need an app password too** page, click **Finish**.
17. Now you need to test by browsing Azure Management portal and use your Microsoft account to log into.



## Protect your account

Because you've turned on two-step verification, you need to approve request 46NGL on your Microsoft Authenticator app.

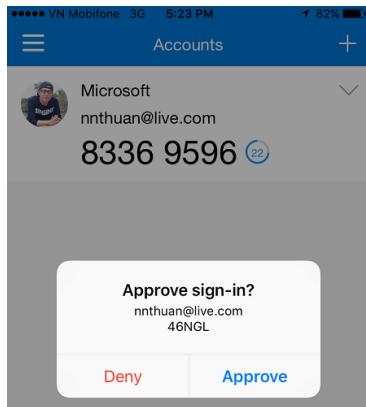
 Waiting for you to approve request 46NGL

I sign in frequently on this device. Don't ask me to approve requests here.

[Having trouble?](#)

[Cancel](#)

18. Open Microsoft Authenticator app on your phone, there is an approval pop-up that asks you approve the authentication request. The request ID in the pop-up matches 100% with the one displaying in the above page.



19. Tap on **Approve** to complete the sign-in request.

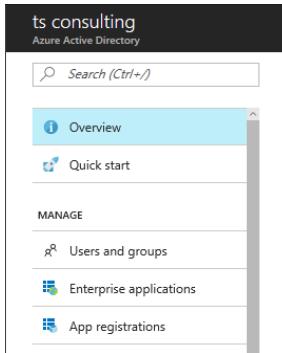
Now you have completed this lab. As said, you cannot force a Microsoft account to use multi-factor authentication. In the next lab, we will configure to force accounts created by Azure AD to use multi-factor authentication.

## Lab 4.3 – Enabling Multi-Factor Authentication for Azure AD account

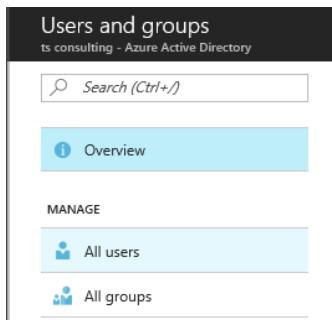
You may have not only Microsoft account but also Azure AD account to manage your Azure resources. This lab is going to walk you through steps to enable multi-factor authentication for an Azure AD account.

Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **More services** to add **Azure Active Directory** navigation if it has not been added yet.
3. On your Azure Active Directory subscription blade, click **Users and groups**.



4. On the **Users and groups** blade, click **All users**



5. Click **Multi-Factor Authentication**

NAME	USER NAME	
 biz	biz@collapoint.onmicrosoft.com	...
 Chris Green	chris@nnthuanlive.onmicrosoft.com	...
 collapoint@outlook.com	collapoint@outlook.com	...

6. On the multi-factor authentication page, you can see the list of all accounts including Azure AD and Microsoft Live ID in your Azure subscription. You can only manage Azure AD. All Microsoft accounts are greyed.

## multi-factor authentication users service settings

Before you begin, take a look at the [multi-factor auth deployment guide](#).

View:

<input type="checkbox"/> DISPLAY NAME ▾	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/> biz	biz@collapoint.onmicrosoft.com	Disabled
<input type="checkbox"/> Chris Green	chris@nnthuanlive.onmicrosoft.com	Disabled
<input type="checkbox"/> collapoint@outlook.com	collapoint@outlook.com	Disabled
<input type="checkbox"/> h.pham	h.pham@lancaster.ac.uk	Disabled
<input type="checkbox"/> Jackie Chan	jackie@nnthuanlive.onmicrosoft.com	Disabled
<input type="checkbox"/> Nguyen Thuan	nnthuan@live.com	Disabled
<input type="checkbox"/> sh_tuanpa@hotmail.com	sh_tuanpa@hotmail.com	Disabled
<input type="checkbox"/> thuan	thuan@outlook.com	Disabled
<input type="checkbox"/> Thuan Nguyen (Azure)	thuan@nnthuanlive.onmicrosoft.com	Enforced
<input type="checkbox"/> thuansg.1506	thuansg.1506@gmail.com	Disabled

### 7. Select an Azure AD account. Click **Enable** under **quick steps**.

<input type="checkbox"/> DISPLAY NAME ▾	USER NAME	MULTI-FACTOR AUTH STATUS	
<input type="checkbox"/> biz	biz@collapoint.onmicrosoft.com	Disabled	Thuan Nguyen 
<input type="checkbox"/> Chris Green	chris@nnthuanlive.onmicrosoft.com	Enabled	thuan@nnthuanlive.onmicrosoft.com
<input type="checkbox"/> collapoint@outlook.com	collapoint@outlook.com	Disabled	quick steps
<input type="checkbox"/> h.pham	h.pham@lancaster.ac.uk	Disabled	<a href="#">Enable</a>
<input type="checkbox"/> Jackie Chan	jackie@nnthuanlive.onmicrosoft.com	Disabled	<a href="#">Manage user settings</a>
<input type="checkbox"/> Nguyen Thuan	nnthuan@live.com	Disabled	
<input type="checkbox"/> sh_tuanpa@hotmail.com	sh_tuanpa@hotmail.com	Disabled	
<input type="checkbox"/> thuan	thuan@outlook.com	Disabled	
<input checked="" type="checkbox"/> Thuan Nguyen (Azure)	thuan@nnthuanlive.onmicrosoft.com	Disabled	
<input type="checkbox"/> thuansg.1506	thuansg.1506@gmail.com	Disabled	

### 8. You are asked to confirm your configuration. Click **enable multi-factor auth**.



#### About enabling multi-factor auth

Please read the [deployment guide](#) if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: <https://aka.ms/MFASetup>

[enable multi-factor auth](#)

[cancel](#)

### 9. Once the update is successful. Click **close**.



Updates successful

Multi-factor auth is now enabled for the selected accounts.

[close](#)

10. At the first time of login, if multi-factor authentication is enabled, Azure asks you to set up your own authentication method.
11. Click **Set it up now**.



thuan@nnthuanlive.onmicr...

Your admin has required that you set up this account for additional security verification.

[Set it up now](#)

[Sign out and sign in with a different account](#)

[More information](#)

12. On the **Additional security verification** page, select the authentication method. There are three options: **Authentication phone**, **Office phone** and **Mobile app**.
13. Select your preferred method. In this lab, **Authentication phone** option is used. Select your country code and your phone number.
14. Click **Contact me**.

## Additional security verification

Secure your account by adding phone verification to your password. [View video](#)

### Step 1: How should we contact you?

▾

▾

Method

- Send me a code by text message  
 Call me

[Contact me](#)

15. Enter your verification code which is sent to your phone number then click **Verify**.
16. You are given an app password which can be used for other apps such as Outlook, Apple Mail. Copy the app password to a secure location.
17. Click **Done**.

## Additional security verification

Secure your account by adding phone verification to your password. [View video](#)

### Step 3: Keep using your existing applications

In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. [Learn more](#)

Get started with this app password:

khccftssgcyzfhj 

**Done**

18. Try to log into Azure Management Portal again to verify your configuration.

How do you want us to verify your account?



thuan@nnthuanlive.onmicrosoft.com

Text me at +84 0000000000

We've sent you a text message with a verification code.

**Sign in**

[Use a different verification option](#)

[Sign out and sign in with a different account](#)

[More information](#)

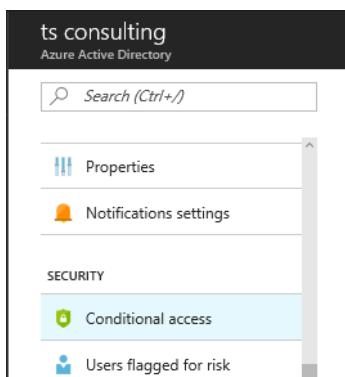
Now you have completed this lab.

## Lab 4.4 – Forcing Multi-Factor Authentication with Conditional Access

With Microsoft account, there is no way as of this article to force to use multi-factor authentication during login time to Azure Management portal. However, if your account is created and managed by Azure AD you can create an enforcement policy to force people in your organization to set up multi-factor authentication before they can log into Azure. This lab is going to walk you through steps to create an enforcement policy of multi-factor authentication to apply to a group of Azure AD accounts.

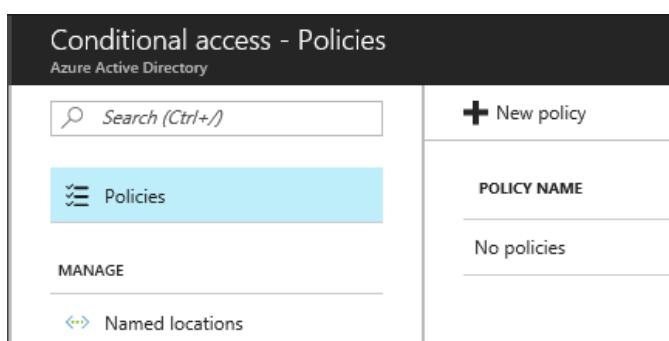
Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Azure Active Directory**
3. Click **Conditional access**.



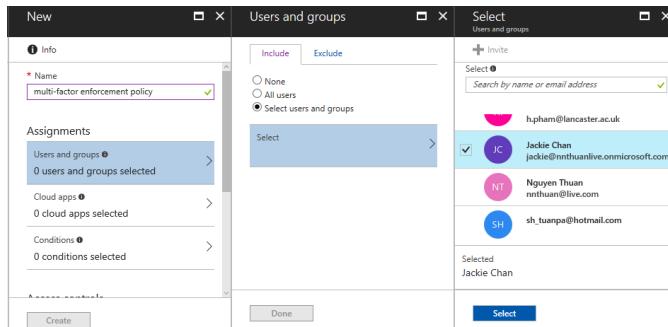
The screenshot shows the Azure Active Directory interface. The top navigation bar has 'ts consulting' and 'Azure Active Directory'. The left sidebar has a search bar and links for 'Properties', 'Notifications settings', 'SECURITY' (which is expanded to show 'Conditional access' and 'Users flagged for risk'), and 'Users flagged for risk'. The main content area is currently empty.

4. On the **Conditional access** blade, click **Policies**.
5. Click **New policy**.

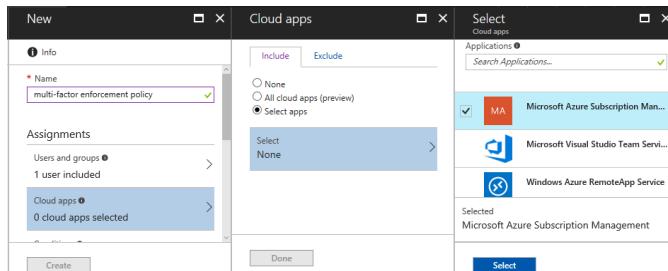


The screenshot shows the 'Conditional access - Policies' blade. The top navigation bar has 'Azure Active Directory'. The left sidebar has a search bar and links for 'Policies' (which is selected and highlighted in blue), 'MANAGE', and 'Named locations'. The right panel has a 'New policy' button and a table with a single row for 'POLICY NAME' containing the text 'No policies'.

6. On the New blade, enter name of the new policy under **Name** setting.
7. Under **Assignments** setting, click **Users and groups**.
8. Select **Select users and groups** in **Include** tab.
9. Click **Select**.
10. Click user you want to apply the new policy.
11. Click **Select**.



12. Click **Done** after the user is added.
13. Click **Cloud apps**.
14. Select **Select apps** in **Include** tab.
15. Select **Microsoft Azure Subscription Management**. Click **Select**.



16. Click **Done** after the app is added.
17. Leave **Condition** settings by default. We will explore different condition types in the next lab.
18. Click **Grant** under **Access controls**.
19. On the **Grant** blade, click **Grant access**.
20. Select **Require multi-factor authentication**.
21. Select **Require one of the selected controls (preview)**.
22. Click **Select**.

23. Keep **Session** setting by default.
24. Select **On** under **Enable policy** setting.
25. Click **Create**.

26. Wait a few minutes until the policy is successfully created.

POLICY NAME	ENABLED
multi-factor enforcement policy	<input checked="" type="checkbox"/>

27. Use the added account to log into Azure Management Portal.
28. At the first time, this account is asked to set up an authentication method.



jackie@nnthuanlive.onmicro...

Your admin has required that you set up this account for additional security verification.

[Set it up now](#)

[Sign out and sign in with a different account](#)

[More information](#)

29. Refer **Step 11** in *Lab 4.4* to complete the setup.

Now you have completed this lab.

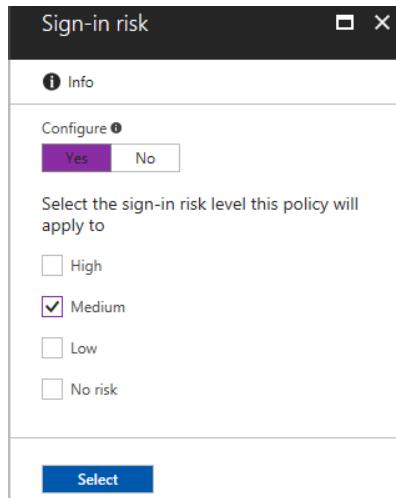
## Lab 4.5 – Protecting your Identity with Conditional Access

In the previous lab, you created an enforcement policy to force multi-factor authentication to a given Azure AD account. Conditional Access not only provides you such a feature but also several conditions to assist you to protect your Azure AD account. This lab is going to walk you through steps to create several conditions to protect an Azure AD account.

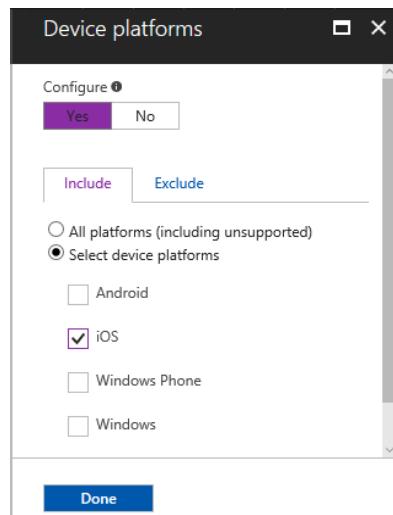
Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Azure Active Directory**
3. Click **Conditional access**.
4. Click your policy you created in *Lab 4.4*.
5. Click **Conditions**.
6. On the **Conditions** blade, there are four types of condition you can set to control access.
7. **Sign-in risk** provides you four levels of risk Microsoft defines: **High**, **Medium**, **Low** and **No Risk**. These levels are based on the detection capability in both Real-time and Offline mode to track an Azure AD identity. For example, if your account is signed in from an anonymous IP address, the risk level is **Medium**.

8. On the **Sign-in risk** blade, select **Yes** under **Configure** setting.
9. Select a risk level you want your policy to apply to. Click **Select**.



10. Click **Device platform** blade. Select **Yes** under **Configure** setting.
11. Click **Select device platform** and select a platform you want in **Include** tab. For example, I only grant access for all users using iOS because this is the complied device in my company.



12. Click **Locations** setting. Click **All trusted IPs** to limit IP address you want to allow. Click **Configure all trusted locations**.

13. You are redirected to the **multi-factor authentication** page.  
Under **service settings** tab, enter IP address you need.
14. Click **save**.

## multi-factor authentication

users    service settings

app passwords [\(learn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps  
 Do not allow users to create app passwords to sign in to non-browser apps

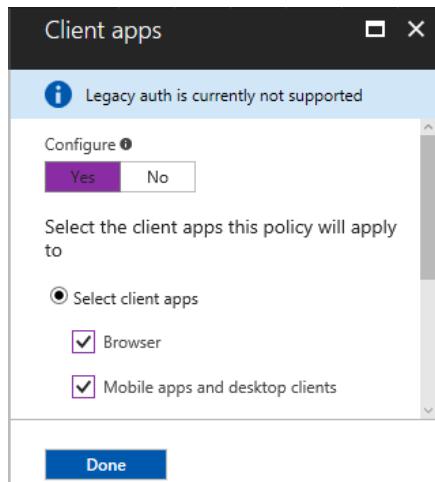
trusted ips [\(learn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/24

15. On the **Update successful** page, click **close**.
16. Click **Client apps** setting. Select **Yes** under **Configure** setting.
17. Select client apps you want.
18. Click **Done**.



19. Click **Grant** setting to verify your control. In this lab, it is **Grant access**.
20. Make sure **On** is selected under **Enable policy** setting.

Now you have completed this lab. You have successfully configured to grant access to added accounts that meet the conditions.

## Lab 5 – Monitoring your Azure resources

In Chapter 6, you were introduced the importance of monitoring in security. You also explored monitoring capabilities Microsoft Azure offers you to monitor your Azure resources. In Lab 5, we will experience each monitoring tool we discussed.

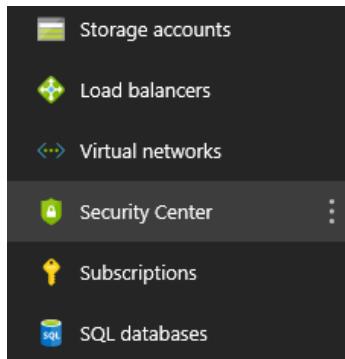
### Lab 5.1 – Overview of Azure resources in Azure Security Center

Azure Security Center provides you the one-stop shop to oversee and monitor all security related threats and vulnerabilities on your Azure resources. This lab is going to walk you through steps to experience Azure Security Center Overview

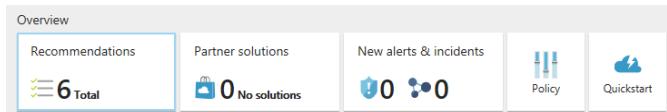
Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.

- From the left panel, click **Security Center**. If you do not see it, click **More services** to add **Security Center** navigation.



- The **Overview** provides you the overall landscape of security in your Azure subscription.
- On the **Overview** blade, under **Overview** section, Azure Security Center displays the number of recommendations based on its security measurement.



- Click **Recommendations** to see all of the security recommendations per your resource type.

Recommendations					
<span>Filter</span>					
DESCRIPTION	RESOURCE	STATE	SEVERITY		
Install Endpoint Protection	3 virtual mac...	Open	High	...	
Add a Next Generation Firewall	did-ad-vm-ip	Open	High	...	
Apply system updates	did-db-vm	Open	High	...	
Apply disk encryption	4 virtual ma...	Open	High	...	
Enable encryption for Azure Storage Ac...	6 storage ac...	Open	High	...	
Restrict access through Internet facing...	did-ad-vm	Open	Medium	...	
Add a vulnerability assessment solution	did-ad-vm	Open	Medium	...	
Remediate OS vulnerabilities (by Micros...	4 virtual ma...	Open	Low	...	

- With each recommendation, Microsoft Azure assists you to configure directly from Security Center or a link to the guidance. For example, click **Install Endpoint Protection**.

7. On the **Install Endpoint Protection** blade, you can see all of your virtual machines that do not have endpoint protection extensions installed. Stick a virtual machine then click **Install on 1 VMs**.

VIRTUAL MACHINE	STATE	SEVERITY	...
did-ad-vm	Open	High	...
did-db-vm	Open	High	...
did-web02-vm	Open	High	...

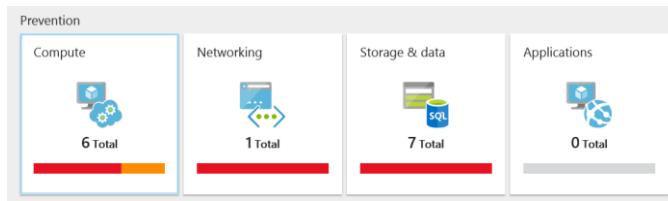
8. There are two extensions which offer endpoint protection solution on your virtual machine: **Deep Security Agent** and **Microsoft Antimalware**.

Deep Security Agent TrendMicro	>
Microsoft Antimalware Microsoft Corp	>

9. Click **Microsoft Antimalware**
10. On the **Microsoft Antimalware** blade, click **Create**.
11. Configure the Microsoft Antimalware setting similar to what you did in *Lab 3.2*.
12. You can try another action, such as **Add a Next Generation Firewall**. Microsoft Azure will recommend you one of four high-end firewall solutions.

Barracuda Networks, Inc. Barracuda NextGen Firewall F-Series (BYOL)	>
Check Point Check Point vSEC - 2 NIC	>
Cisco Systems, Inc. Cisco ASA v - BYOL 4 NIC	>
Fortinet FortiGate NGFW Single VM	>

13. Under **Prevention**, there are four resource types currently Microsoft Azure supports in security monitoring.



14. There are also prevention recommendations for each type. For example, click **Networking** to see what you are missing.

**Networking**  
SECURITY HEALTH

**NETWORKING RECOMMENDATIONS TOTAL**

RECOMMENDATION	ENDPOINTS	PROGRESS
NGFW not installed	1 of 1 endpoints	<div style="width: 100%;"> </div>
Restrict access through Intern...	1 of 1 virtual machines	<div style="width: 100%; background-color: orange;"> </div>

**Internet facing endpoints**

ENDPOINT NAME	IP	NSG	NGFW
did-ad-vm	13.76.211.20	<span style="color: orange;">⚠</span>	<span style="color: red;">!</span>

**Networking topology**

NAME	NSG
did-vnet	●
AppGateway-vnet	●
gth2docker01	●
jump-vnet	●

15. Click on an orange highlighted item to check security health.

The screenshot shows the 'Virtual machine security health' blade for a VM named 'did-ad-vm'. It displays the following information:

- Virtual machine info:**
  - VIRTUAL MACHINE: did-ad-vm
  - RESOURCE GROUP: DID-AD-RG
  - SUBSCRIPTION: Visual Studio Enterprise
  - VIRTUAL IP: 13.76.211.20
- Security Solutions:**
  - PREVENTION STATUS: High severity
  - NETWORK SECURITY GROUP: [did-dmz-nsg](#)
- Recommendations:**

DESCRIPTION	RESOURCE	STATE	SEVERITY	...
Restrict access through Internet facing...	did-ad-vm	Open	⚠️ Medium	...

16. From the recommendation, consider applying network security group for the resource. In the example above, the **did-ad-vm** virtual machine still allows Internet inbound network traffic which is not good in defense in depth strategy. Refer to Lab 2 to create a network security group with a rule to restrict Internet inbound network traffic then apply it to the **ad-subnet**.

Now you have completed this lab.

## Lab 5.2 – Installing Qualys Vulnerability Assessment on your Virtual machine

One of the recommendations you often see in Azure Security Center is vulnerability assessment solution on your virtual machine. Microsoft has engaged Qualys to provide an assessment for Azure virtual machines. This lab is going to walk you through steps to install Qualys vulnerability assessment on a virtual machine.

Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Security Center**.
3. Under **PREVENTION**, click **Partner solutions**.

4. Click **recommendations** hyperlink.

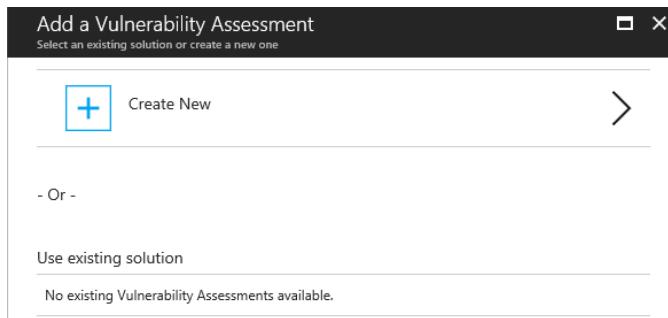
5. On the **Recommendations** blade, click **Add a vulnerability assessment solution**.

DESCRIPTION	RESOURCE	STATE	SEVERITY	...
Install Endpoint Protection	3 virtual mac...	Open	🔴 High	...
Add a Next Generation Firewall	did-ad-vm-ip	Open	🔴 High	...
Apply system updates	did-db-vm	Open	🔴 High	...
Apply disk encryption	4 virtual ma...	Open	🔴 High	...
Enable encryption for Azure Storage Ac...	7 storage ac...	Open	🔴 High	...
Restrict access through Internet facing...	did-ad-vm	Open	⚠ Medium	...
Add a vulnerability assessment solution	did-ad-vm	Open	⚠ Medium	...
Provide security contact details	1 subscriptions	Open	⚠ Medium	...
Remediate OS vulnerabilities (by Micros...	4 virtual ma...	Open	🟡 Low	...

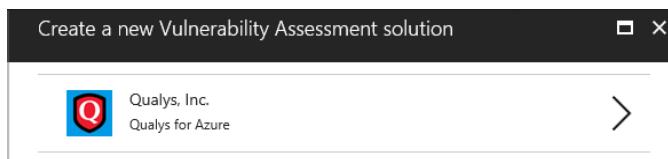
6. Select your virtual machine. Click **Install on 1 VMs**.

VIRTUAL MACHINE	SUBSCRIPTION NAME	STATE	SEVERITY	...
did-ad-vm	Visual Studio Enterprise	Open	⚠ Medium	...

7. On the **Add a Vulnerability Assessment** blade, click **Create New**.



8. On the **Create a new Vulnerability Assessment** solution blade, click **Qualys for Azure**.



9. On the Qualys, Inc. vulnerability management blade, click **Sign up** for the solution. You are redirected to the Qualys registration account for Qualys solution for Azure. Click **Qualys Free Trial** and follow registration process to complete.
10. Enter name of the solution under **Name** setting.
11. Subscription is automatically selected. Select **Use existing** under **Resource group** setting. Select **did-infra-rg** from the drop-down list.
12. Select your location under **Location** setting.

Qualys, Inc. vulnerability ma... □ X

Create management - PREVIEW

Sign up for the solution

\* Name

did-QualysVa ✓

Subscription

Visual Studio Enterprise

\* Resource group  ⓘ

Create new  Use existing

did-infra-rg ▼

\* Location

Southeast Asia ▼

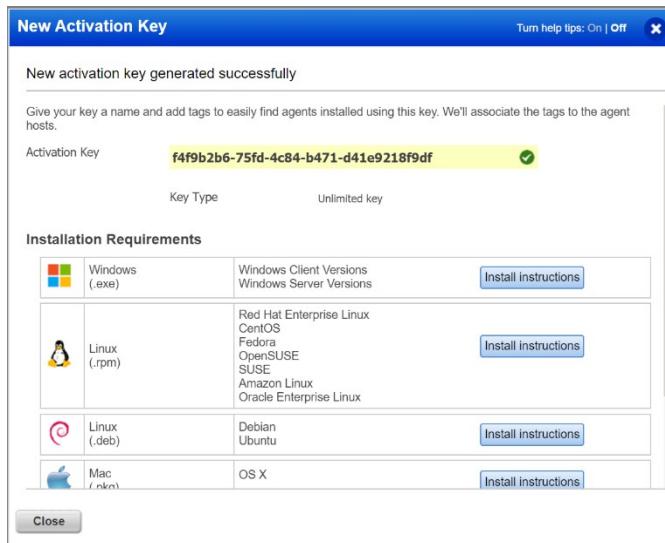
13. Login to Qualys portal. Click **Modules** from the left corner and select **Cloud Agent**.



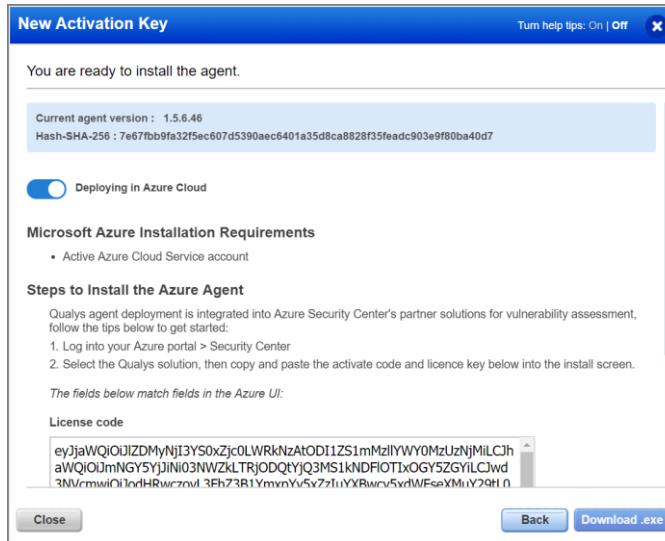
14. On the **Cloud Agent** page, there are two tabs: **Dashboard** and **Agent Management**. Click **Agent Management** tab.
15. On the **Agent Management** page, click **Agents** tab. Click **Install New Agent**.

16. On the **New Activation Key** page, enter the title of your new activation key.
17. Stick to **Vulnerability Management**.
18. Click **Generate**.

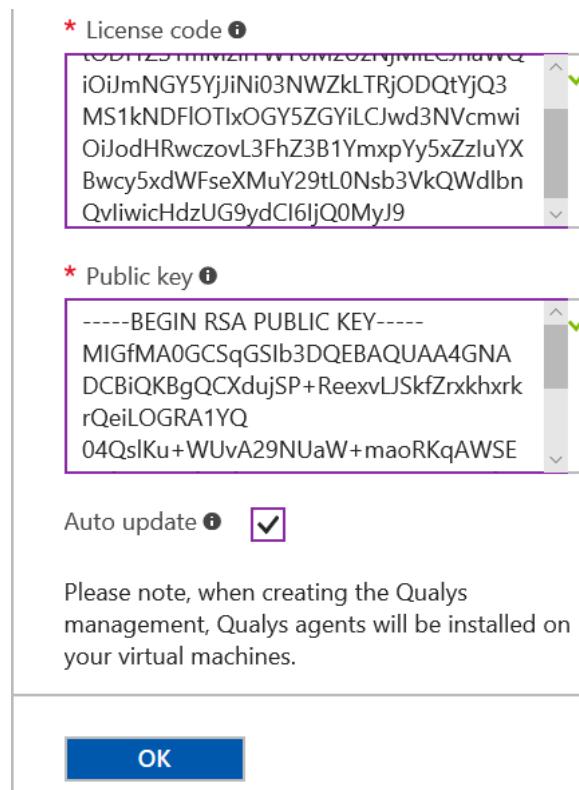
19. Copy the activation key into your secure note.
20. Click **Install instructions** for Windows under **Installation Requirements**.



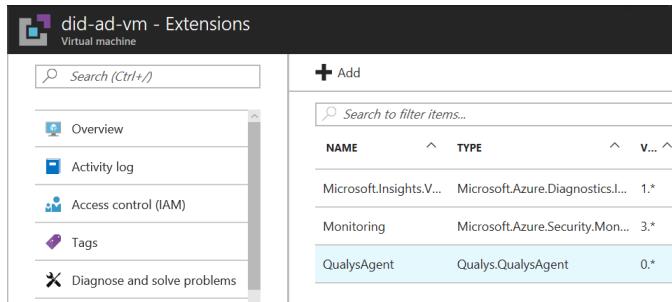
- Switch to the option **Deploying in Azure Cloud**.
- Copy code under **License code** and **Public key** which you need to enter in



- Paste copied code accordingly into **License code** box and **Public key** box.
- Stick **Auto update** if you want the agent is automatically installed on discovered unprotected resource in the target subscription.
- Click **OK**.



- Wait around 5 – 10 minutes until the agent deployment is complete on your target virtual machine.
- Once the deployment is finished, Qualys Agent extension is installed on your virtual machine.



- To verify if your setup is correct, you can navigate back to **Agent Management** page in the Qualys portal.
- Click **Activation Keys** tab.

The screenshot shows the 'Agent Management' section of a Qualys interface. The top navigation bar includes 'Dashboard', 'Agent Management', 'Agents', 'Activation Keys' (which is the active tab), and 'Configuration Profiles'. Below the navigation is a search bar with filters for 'Status: Active' and 'Enabled: Yes'. A button for 'Actions (1)' and a 'New Key' button are also present. The main table lists an activation key: 'did-azure-qualsy-agent' (f4f9b2b6-75fd-4c84-b471-d41e9218f9df), with 0 agents and a creation date of May 31, 2017.

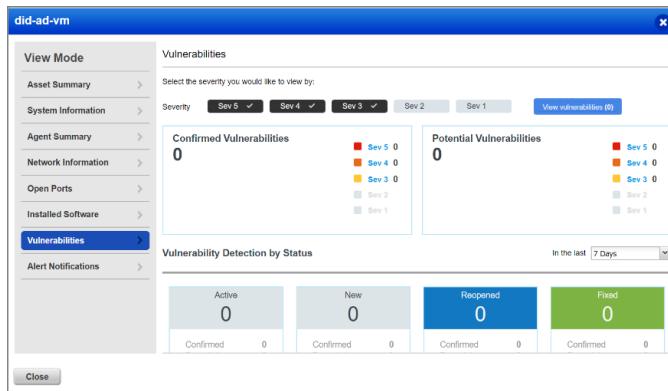
30. Click the activation key you just created.
31. On the **Key Info View** page, click **Agents**. You can see that your agent host with correct name is added.

The screenshot shows the 'Key Info View' page. The left sidebar has a 'View Mode' section with 'General Info', 'Agents' (which is selected and highlighted in blue), and 'Azure Info'. The main content area is titled 'Agents' and shows a table with one entry: 'Agent Host: did-ad-vm' and 'Version: 1.4.5.232'.

32. You can verify whether Qualys agent is automatically installed on another virtual machine.

The screenshot shows the 'Agent Management' section with the 'Agents' tab selected. It includes a 'Saved Searches' dropdown and a search bar. Below are buttons for 'Actions (0)', 'Install New Agent', and 'Activation Jobs'. The main table lists two agents: 'DID-JUMP01-VM' (IP: 10.0.0.4, MAC: fe80:0:0:98f7:a134:cce9:583a) and 'did-ad-vm' (IP: 192.168.1.4, MAC: fe80:0:0:6dae:3a86:3381:6b...).

33. You can click on each agent and look for Vulnerability report from Qualys.



Now you have completed this lab.

## Lab 5.3 – Configuring Security policy in Azure Security Center

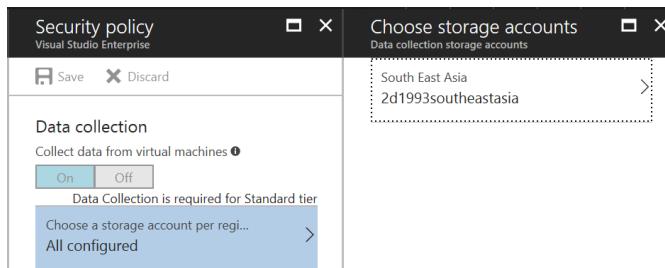
Security Policy in Azure Security Center allows you to check the Security Center tier you are applying for each subscription. It also allows you to set up prevention policy and email notification. This lab is going to walk you through steps to configure security policy in Azure Security Center.

Perform the following steps to complete this lab:

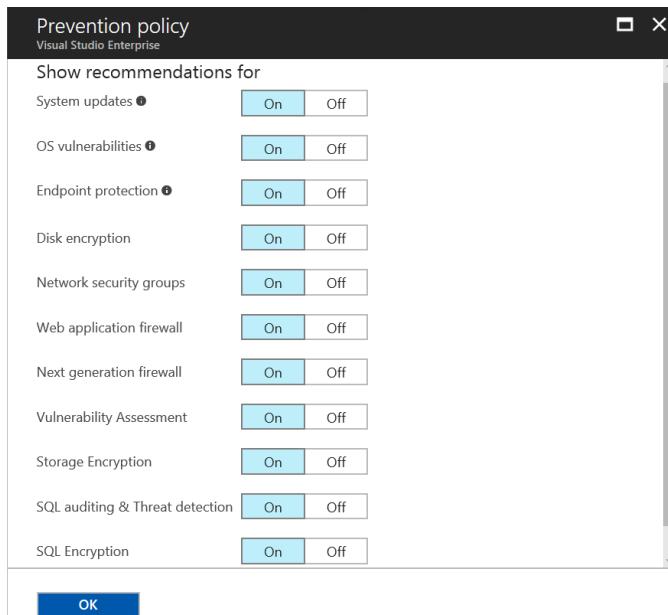
1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the **Security Center**, click **Security policy** under **GENERAL**.
3. On the **Security policy** blade, there is the list of all Azure subscriptions which Azure Security Center is enabled on.
4. Expand a subscription to see all resources which are being inherited into security policy of that subscription.
5. You can also see data collection enabled on each subscription.

NAME	INHERITANCE	DATA COLLECTION
Visual Studio Enterprise	---	On
did-ad-rg	Inherited	On
did-db-rg	Inherited	On
did-infra-rg	Inherited	On
did-web-rg	Inherited	On
securitydata	Inherited	On
Visual Studio Ultimate with MSDN	---	On
Hoang-Resouce	Inherited	On
gth2_docker_rg	Inherited	On
securitydata	Inherited	On

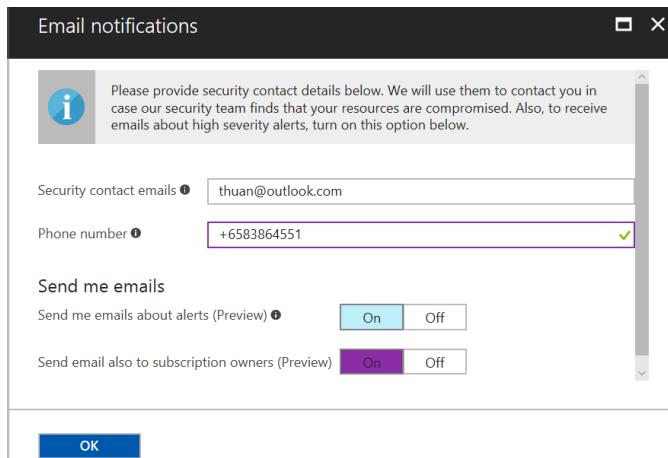
6. Click a subscription.
7. On the **Security policy** blade, if you are using Standard tier you cannot turn off data collection feature. The setting under **Data collection** is disabled.
8. You can see the storage account where data is collected into by clicking **Choose a storage account per region** setting.



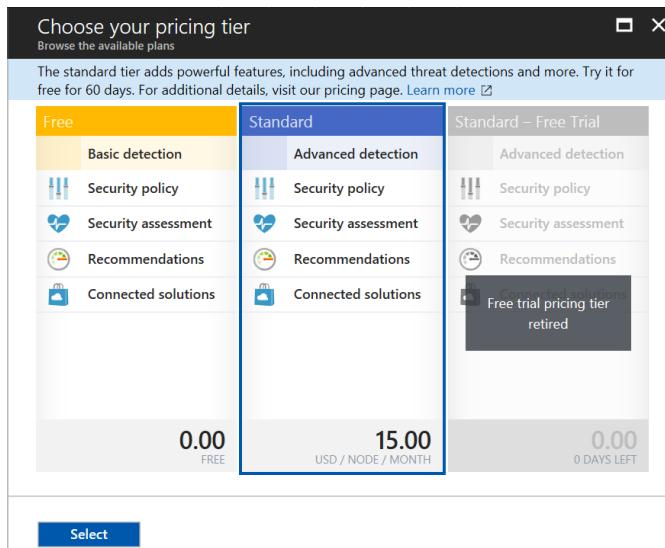
9. Under **Policy components**, you can set up prevention policy, email notifications or switch to different Security Center tier.
10. Click **Prevention policy** setting.
11. On the blade, there are 11 default policies you can turn on or off every time to not collect data. For example, if you do not want Azure Security Center to check and recommend you next generation firewall, simply click **Off**.
12. Click **OK** to complete the setup.



13. Click **Email notifications** setting.
14. On the blade, Microsoft allows you provide contact detail so if there is any critical security threat, Microsoft will contact you.
15. Click **OK** after entering your information and setting up.



16. Click **Pricing tier** setting. On the blade, select a tier you want to apply.
17. Click **Select**.



18. By default, policies on Azure resources under a subscription are inherited. You can stop inheritance and configure unique prevention policy by clicking a resource and selecting **Unique** under **Inheritance** setting.

Security policy  
did-ad-rg

Save Discard

Inheritance

Inherit policy settings from subscription or define this resource group as unique i

Inherited Unique

Data collection

Collect data from virtual machines i

On Off

Data Collection is required for Standard tier

Choose a storage account per regi... lock

All configured

19. Configure unique prevention policy for a given resource.

Now you have completed this lab.

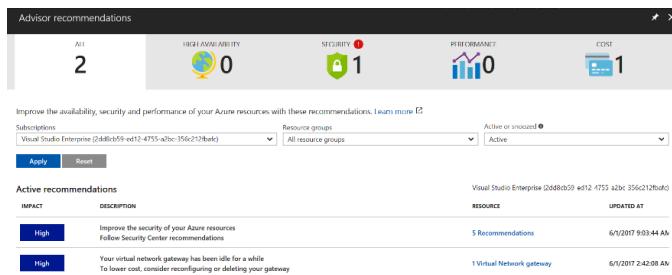
## Lab 5.4 – Exploring Azure Advisor

Azure Advisor focuses on analyzing your Azure resources in four factors: High Availability, Security, Performance and Cost. With Azure Advisor, you can better plan for Azure monitoring strategy. This lab is going to walk you through steps to explore Azure Advisor.

Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Advisor**. Add its navigation to the left panel if you have not done yet.
3. On the **Advisor recommendations** blade, Azure Advisor gives you a comprehensive look around the four factors. On the ALL tab, you can choose a subscription to get the list of

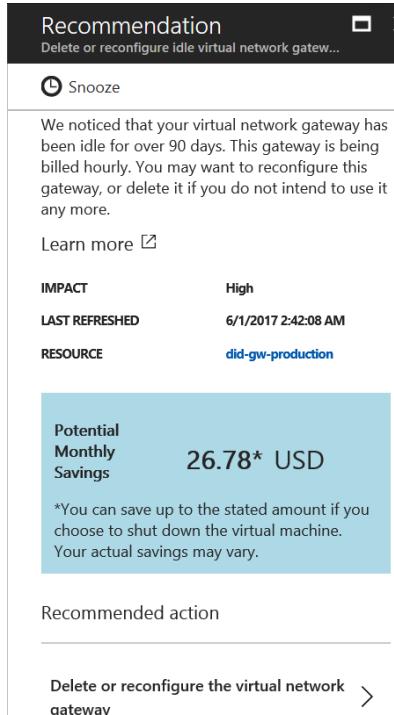
recommendations. Moreover, you can filter a specific resource group.



The screenshot shows the 'Advisor recommendations' interface. At the top, there are five metrics: HIGH AVAILABILITY (2), SECURITY (1), PERFORMANCE (0), and COST (1). Below this, a message says 'Improve the availability, security and performance of your Azure resources with these recommendations.' A 'Learn more' link is provided. The 'Active or ignored' dropdown is set to 'Active'. The 'Subscriptions' dropdown shows 'Visual Studio Enterprise (2d88cb59-ed12-4755-a2bc-356c212fbaf0)'. The 'Resource groups' dropdown shows 'All resource groups'. The 'Active' dropdown is also set to 'Active'. There are two 'Active recommendations' listed:

IMPACT	DESCRIPTION	RESOURCE	UPDATED AT
High	Follow Security Center recommendations	5 Recommendations	6/1/2017 9:03:44 AM
High	Your virtual network gateway has been idle for a while To lower cost, consider reconfiguring or deleting your gateway	1 Virtual Network gateway	6/1/2017 2:42:08 AM

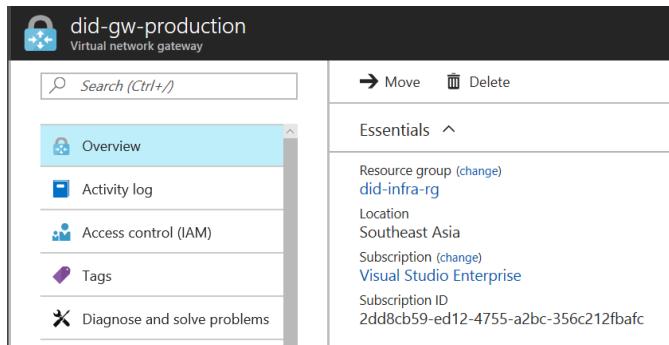
4. Under **Active recommendations**, click one to see what Azure Advisor recommends you.



The screenshot shows a 'Recommendation' dialog box. The title is 'Recommendation' and the sub-title is 'Delete or reconfigure idle virtual network gateway...'. There is a 'Snooze' button. The main text says: 'We noticed that your virtual network gateway has been idle for over 90 days. This gateway is being billed hourly. You may want to reconfigure this gateway, or delete it if you do not intend to use it any more.' Below this is a 'Learn more' link. The 'IMPACT' is 'High', 'LAST REFRESHED' is '6/1/2017 2:42:08 AM', and the 'RESOURCE' is 'did-gw-production'. A large callout box highlights 'Potential Monthly Savings' as '26.78\* USD'. A note below states: '\*You can save up to the stated amount if you choose to shut down the virtual machine. Your actual savings may vary.' At the bottom, it says 'Recommended action' and 'Delete or reconfigure the virtual network gateway' with a right-pointing arrow.

5. From the recommendation, Azure Advisor realizes that my virtual network gateway has been idle over 90 days. It also gives an estimate of saving money for my subscription. Besides, Azure Advisor recommends to consider deleting it or reconfiguring.
6. Click **Delete or reconfigure the virtual network gateway**.

7. You are directed to the virtual network gateway where you can delete if you do not need it.



did-gw-production  
Virtual network gateway

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Move Delete

Resource group (change)  
did-infra-rg

Location  
Southeast Asia

Subscription (change)  
Visual Studio Enterprise

Subscription ID  
2dd8cb59-ed12-4755-a2bc-356c212fbafc

8. You can try with another recommendation. Each recommendation includes the guidance and link to the recommended resource Azure Advise gives you.

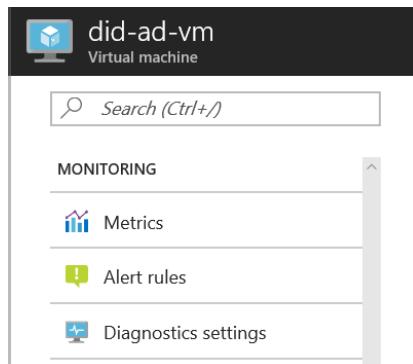
Now you have completed this lab.

## Lab 5.5 – Creating a virtual machine metric

To have an effective monitoring on virtual machine, you should set a metric with alert to timely get notification when the utilization exceeds the metric. This lab is going to walk you through steps to create a metric on a virtual machine.

Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Virtual machines**.
3. Click a virtual machine you need to add a metric.
4. On the blade, under **MONITORING**, click **Metrics**

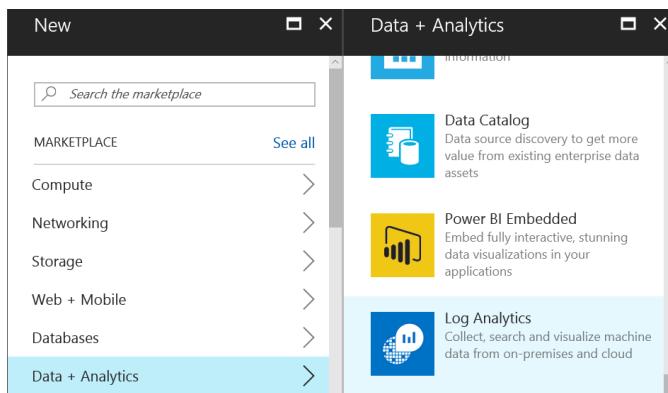


## Lab 5.6 – Setting up Azure Log Analytics

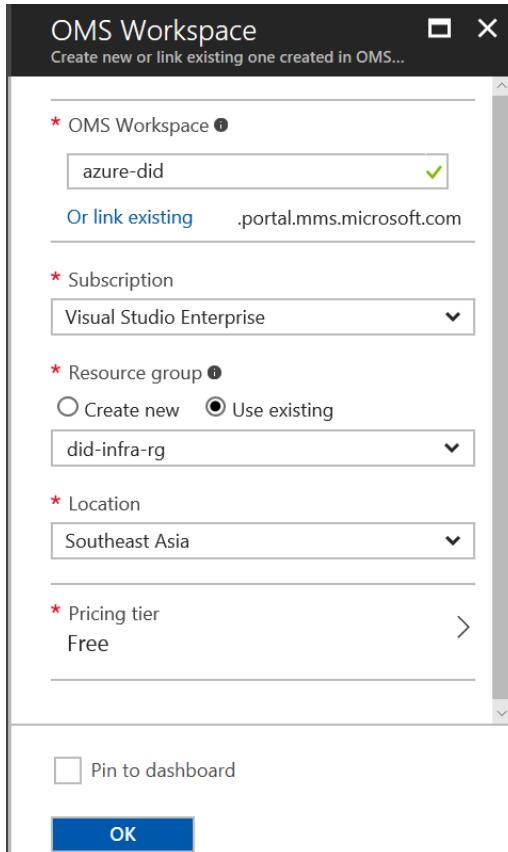
In Chapter 6, you were introduced Azure Log Analytics which is part of Operation Management Suite, allowing you to monitor resources with rich solution gallery. This lab is going to walk you through steps to set up Azure Log Analytics.

Perform the following steps to complete this lab:

5. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
6. From the left panel, click **New**.
7. On the **New** blade, click **Data + Analytics**.
8. Click **Log Analytics**.



9. On the **OMS Workspace** blade, enter name of the new workspace under **OMS Workspace** setting.
10. Select your subscription under **Subscription** setting.
11. Select **Use existing** under **Resource group** setting.
12. Select location under **Location** setting.
13. Keep **Free** tier by default under **Pricing tier** for evaluation purpose.
14. Click **OK**.



15. Wait a few minutes until the deployment is successful.

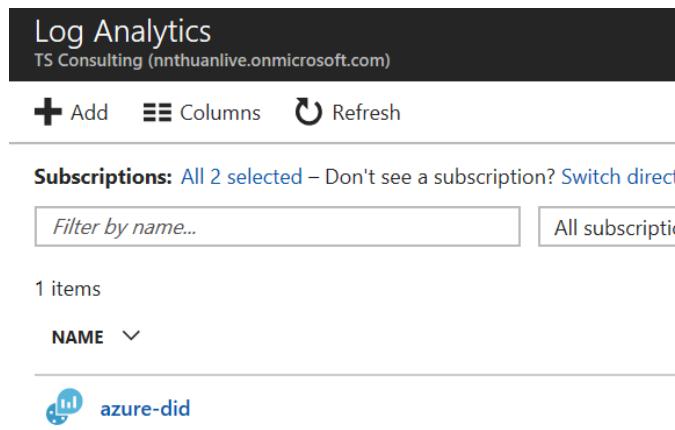
Now you have completed this lab.

## Lab 5.7 – Adding Azure Network Security Group Analytics

You previously created an OMS workspace to use Azure Log Analytics to monitor Azure resource. This lab is going to walk you through step to add Azure Network Security Group Analytics from the solution gallery to monitor your Azure network security group.

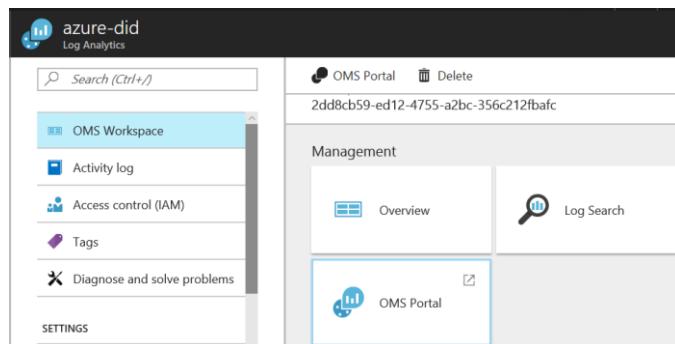
Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. Open **Log Analytics**. You can go to **More services** and add **Log Analytics** navigation to the left panel.



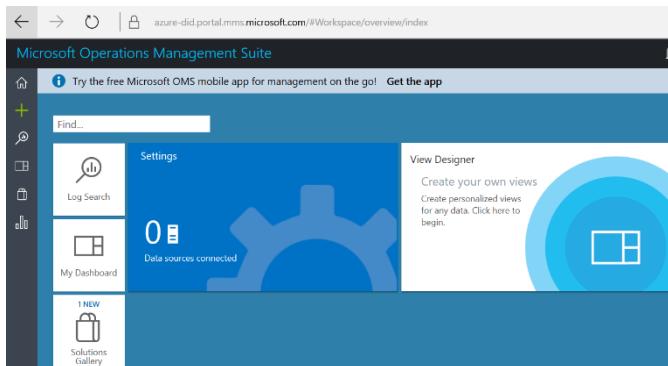
The screenshot shows the Azure Log Analytics workspace interface. At the top, it displays the workspace name 'Log Analytics' and the owner 'TS Consulting (nnthuanlive.onmicrosoft.com)'. Below the header are three buttons: 'Add', 'Columns', and 'Refresh'. The main area is titled 'Subscriptions' with the message 'All 2 selected – Don't see a subscription? [Switch directly](#)'. There is a 'Filter by name...' input field and a 'All subscriptions' button. Below this, it shows '1 items' and a dropdown menu set to 'NAME'. A single item 'azure-did' is listed, featuring a blue icon with a gear and a bar chart, and the text 'azure-did'.

3. Click the workspace you created.
4. From the **OMS Workspace**, click **OMS Portal**.

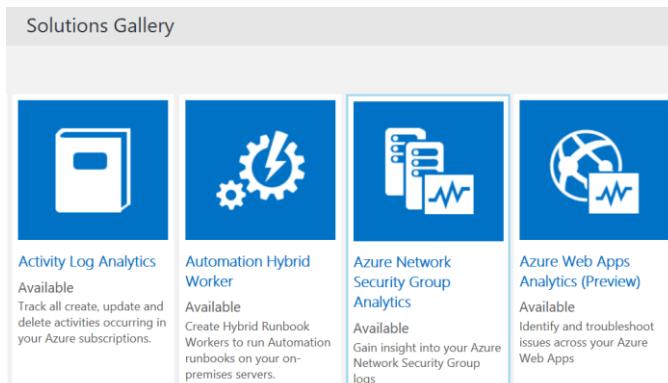


The screenshot shows the 'azure-did' OMS Workspace interface. The left sidebar has a 'Search (Ctrl+/' input field and links for 'OMS Workspace', 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems'. The 'SETTINGS' link is at the bottom. The main area has a 'Management' section with 'Overview' and 'Log Search' buttons, and a 'OMS Portal' button which is highlighted with a blue border.

5. You are redirected to the OMS workspace with the URL you configured step 5.



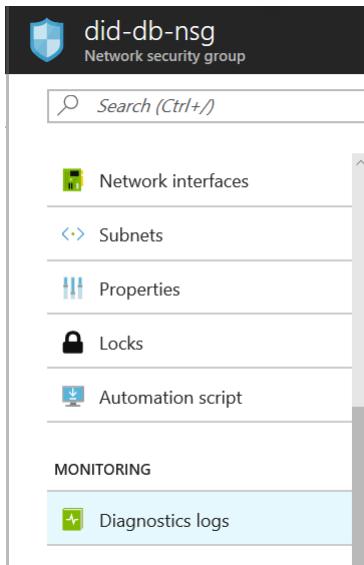
6. Click **Solutions Gallery**.
7. On the **Solutions Gallery** page, select **Azure Network Security Group Analytics**.



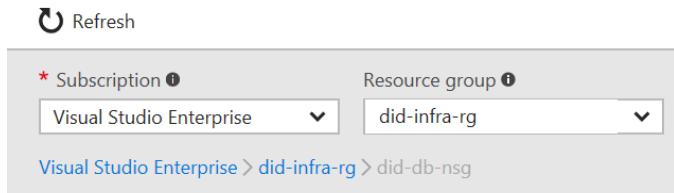
8. On the **Details** page, click **Add**.



9. Wait a few minutes until the new solution is successfully added.
10. Go to your network security group. Under **MONITORING**, click **Diagnostics logs**.



11. Click **Turn on diagnostics**.



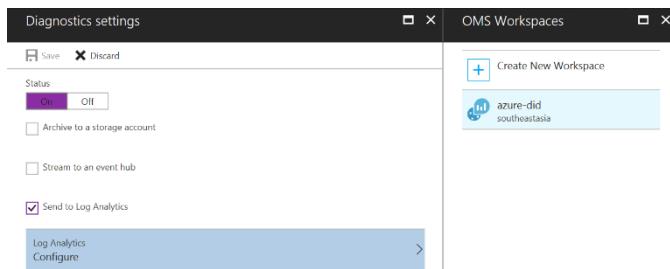
Turn on diagnostics to collect the following logs.

- NetworkSecurityGroupEvent
- NetworkSecurityGroupRuleCounter

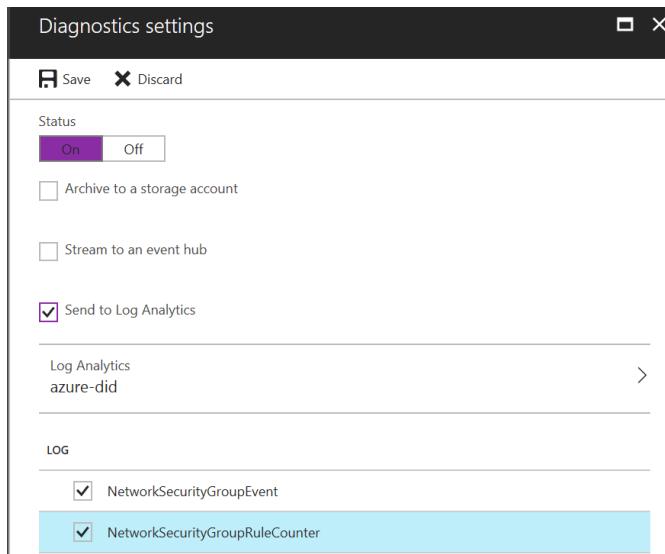
12. On the **Diagnostics settings** blade, click **On** under **Status** setting.
13. Select **Send to Log Analytics**.



14. Click to configure the workspace.
15. On the **OMS Workspaces** blade, select your newly created workspace.



16. Select **NetworkSecurityGroupEvent** and **NetworkSecurityGroupRuleCounter** under **LOG**.
17. Click **Save**.



#### 18. Verify again under **Log Analytics**.

Refresh

Subscription: **Visual Studio Enterprise**

Resource group: **did-infra-rg**

Visual Studio Enterprise > did-infra-rg > did-db-nsg

Diagnostics settings

Storage account: **Not configured**

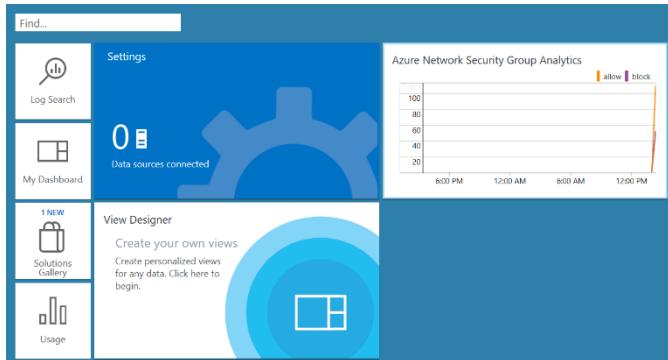
Event hub namespace: **Not configured**

Log Analytics: **azure-did**

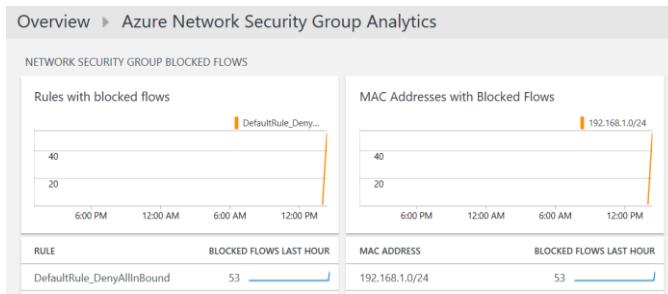
\* Log categories: 2 selected

Timespan: Last week

19. Enable diagnostics log and specify your log analytic workspace for other network security groups.
20. Go to **OMS Portal**. Click **Azure Network Security Group Analytics**.



21. On the **Azure Network Security Group Analytics** page, there is a dashboard providing you statistics



Now you have completed this lab.

## Lab 5.8 – Adding Security Compliance suites to protect your Azure resource

In Microsoft Operations Management Suite, there is a package of two security solutions in the gallery named Security & Compliance. This package gives you the overall status of antimalware and security audit on your Azure resources. This lab is going to walk you through steps to add Security & Compliance.

Perform the following steps to complete this lab:

1. Open your OMS Workspace at the URL <https://azure-did.portal.mms.microsoft.com>
2. Click **Solutions Gallery**. Click **Security & Compliance**.



3. On the **Details** page, click **Add**.

Microsoft Operations Management Suite

Solutions Gallery ▶ Details

+

Security & Compliance

Add

Included solutions:

Antimalware Assessment

Security and Audit

4. Wait a few minutes until the package is successfully added.
5. It takes several hours for the first time when running the assessment.

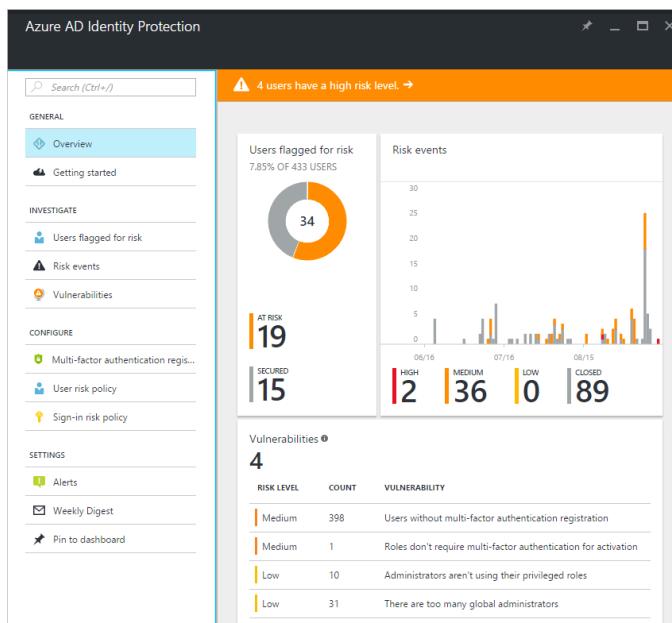
Now you have completed this lab. You can try with any other solutions in the gallery and pull the log to Microsoft OMS.

## Lab 5.9 – Exploring Azure AD Identity Protection

In Chapter 6, you were introduced Azure AD Identity Protection which offers the powerful capabilities to monitor and report Azure identity based on pre-defined risk levels. This lab is going to walk you through steps to explore Azure AD Identity Protection.

Perform the following steps to complete this lab:

1. Log into the Azure Management Portal (<https://portal.azure.com>) using your administrator account.
2. From the left panel, click **Azure AD Identity Protection**. You can go to **More services** and add **Azure AD Identity Protection** navigation to the left panel.
3. On the **Azure AD Identity Protection** blade, click **Overview**.
4. On the **Overview** blade, Azure AD Identity Protection provides you the visual dashboard showing user flagged for risk, risk event and vulnerabilities it foresees.

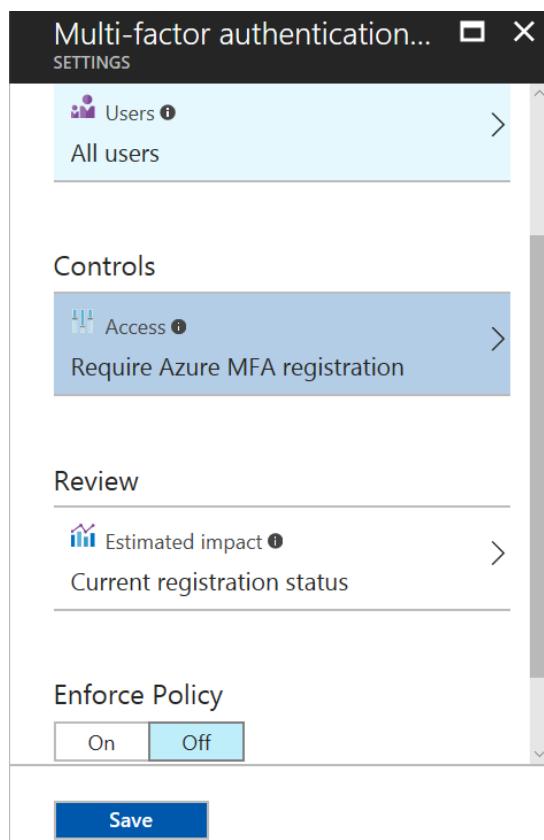


5. For each of information, Azure AD Identity Protection gives you a guidance to resolve. For example, click **Vulnerabilities**.
6. On the **Vulnerabilities** blade, Azure AD Identity Protection shows the list of vulnerabilities including risk level.

7. To know how to resolve this vulnerability, click a vulnerability.

Vulnerabilities		
AZURE AD IDENTITY PROTECTION		
RISK LEVEL	COUNT	VULNERABILITY
Medium	8	Users without multi-factor authentication registration

8. From the vulnerability blade, Azure AD Identity Protection automatically creates a policy to apply multi-factor authentication.
9. After configuring your multi-factor authentication, click **ON** under **Enforce Policy**. Click **Save**.



10. After saving the configuration, all of the accounts you selected will apply multi-factor authentication.
11. Under **INVESTIGATE** you can find different options to monitor users which are flagged for risk, risk events and vulnerabilities. All

of these things are displayed in the dashboard you were introduced earlier in this lab.

- Under **CONFIGURE**, Azure AD Identity Protection allows you to create multi-factor authentication policy because this policy is very important to protecting identity including brute-force attack mitigation. You can also apply user risk and sign-in risk policy for a given or a group of accounts.
- Under **SETTINGS**, you can configure **Alerts** on three user risk levels (Low, Medium and High).

 Save  Discard

---

Alert on user risk level at or above

Low  Medium  High

#### Recipients

Emails are sent to the users included below. New global admins, security admins and security readers will be added to this list by default.

---

INCLUDED

2 selected

>

- 
- With **Weekly Digest** setting, Azure will send you weekly email with summary of users at risk, risk events and vulnerabilities. Select **On** under **Weekly email** digest.



Save



Discard

---

Weekly email digest 

On

Off

## Recipients

Emails are sent to the users included below. New global admins, security admins and security readers will be added to this list by default.

---

INCLUDED

2 selected



Now you have completed this lab. To fully take advantages of Azure AD Identity Protection, you must firstly understand how Microsoft defines user risk event here <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-risk-events> and risk level <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-risk-events#risk-level>

*This page intentionally left blank*

## About the Author

Thuan Nguyen is a Solution Architect with nearly 10 years of experience spanning across industry of Information Technology and Services, focused on Microsoft Stack mostly Office 365, SharePoint, Azure and Enterprise Security. Thuan has been involved in number of successful Microsoft products and technologies deployment for mid-tier and large organizations, including government agencies.

He excels at designing a solution with high agility, driving the transformation of “Know-How” to technology and speaking in a different language of business to technical people. Besides that, he is knowledgeable about developing a technical community by his accumulated leadership skills during his time running two small start-up companies offering digital workplace product and solution on top of Microsoft Cloud services.

Thuan has been a Microsoft Most Valuable Professional (MVP) since 2011. Thuan is an active contributor to the world's community. He has been a guest speaker at several international conferences including European SharePoint Conference, Global Azure Bootcamp, ExpertsLive Asia Pacific, Business 365 Saturday, Microsoft Malaysia SharePoint Conference.

Thuan is regularly on Twitter (@nnthuan) and blogs at <http://thuansoldier.net>. You can reach Thuan at email thuan[at]outlook.com