

Contents

1 AZ-500 Azure Security (old)	8
1.1 Regards, <i>Azure Security Courseware Team</i>	8
1.2 title: Online Hosted Instructions permalink: index.html layout: home	8
2 Content Directory	8
2.1 Labs	8
2.2 Demos	9
3 AZ500 Lab Files	9
4 AZ500 Mod2 Lab1 setup	9
5 AZ500 Mod2 Lab2 setup	9
6 AZ500 Mod2 Lab 11 setup	9
7 SQL Template database deployment	9
8 SQL Template database deployment	9
9 GoDeploy SQL Template database deployment	10
10 Module 1: Lab 1 - Azure AD Privileged Identity Management	10
10.1 Azure AD Privileged Identity Management	10
10.2 Exercise 1 - Discover and Manage Azure Resources	10
10.2.1 Task 1: Lab Setup	10
10.2.2 Task 2: Enable Azure AD Premium P2 trial and create a test user.	10
10.2.3 Task 3: Discover resources	12
10.3 Exercise 2 - Assign Directory Roles	15
10.3.1 Task 1: Make a user eligible for a role	15
10.4 Exercise 3 - Activate and Deactivate PIM Roles	19
10.4.1 Task 1: Activate a role	19
10.4.2 Task 2: Use a role immediately after activation	22
10.4.3 Task 3: Deactivate a role	23
10.4.4 Task 4: Cancel a pending request	25
10.5 Exercise 4 - Directory Roles (General)	25
10.5.1 Task 1: Start an access review for Azure AD directory roles in PIM	25
10.5.2 Task 2: Approve or deny access	27
10.5.3 Task 3: Complete an access review for Azure AD directory roles in PIM	29
10.5.4 Task 4: Configure security alerts for Azure AD directory roles in PIM	29
10.6 Exercise 5 - PIM Resource Workflows	30
10.6.1 Task 1: Configure the Global Administrator role to require approval.	30
10.6.2 Task 2: Enable Isabella for Global Administrator privileges.	31
10.6.3 Task 3: Approve or deny requests for Azure resource roles in PIM	34
10.6.3.1 View pending requests	34
10.7 Exercise 6 - View audit history for Azure AD roles in PIM	35
10.7.1 Task 1: View audit history	36
10.7.2 Task 2: Filter audit history	37
11 Module 1 - Lab 2: Key Vault (Implementing Secure Data by setting up Always Encrypted)	37
11.1 Exercise 1: Introduction to Azure Key Vault	37
11.1.1 Task 1: Download SQL Server Management Studio	37
11.1.2 Task 2: Use PowerShell to create a Key Vault	37
11.1.3 Task 3: Add a key and secret to Key Vault	38
11.1.4 Task 4: Add a Secret to Key Vault	38
11.1.5 Task 5: Enable a Client Application	38
11.1.6 Task 6: Add a Key Vault Policy allowing the application access to the Key Vault.	39
11.1.7 Task 7: Use Key Vault to Encrypt Data with Azure SQL Database	39
11.1.8 Task 8: Create a Table in the SQL Database	40
11.1.9 Task 9: Create and Encrypt a Table	40

11.1.10 Task 10: Build a Console Application to work with Encrypted Columns	41
12 Module 1: Lab 3: Using Multi-Factor Authentication for Secure Access	42
12.1 Exercise 1: MFA Authentication Pilot (Require MFA for specific apps with Azure Active Directory conditional access)	42
12.1.1 Task 1: Create your conditional access policy	42
12.1.2 Task 2: Evaluate a simulated sign-in	43
12.1.3 Task 3: Test your conditional access policy	44
12.2 Exercise 2: MFA Conditional Access (Complete an Azure Multi-Factor Authentication pilot roll out)	44
12.2.1 Task 1: Enable Azure Multi-Factor Authentication	45
12.2.2 Task 2: Test Azure Multi-Factor Authentication	46
13 Module 1: Lab 4: App Registration	46
13.1 Exercise 1: Application Registration	46
13.1.1 Task 1: Register a new application using the Azure portal	46
14 Module 1: Lab 5 - Application Service Principal	48
14.1 Exercise 1: Use the portal to create a service principal that can access resources	48
14.1.1 Task 1: Assign the application to a role	48
14.1.2 Task 2: Get values for signing in	49
14.1.3 Task 3: Create a new application secret	50
14.1.4 Task 4: Check Azure AD permissions	51
14.1.5 Task 5: Check Azure subscription permissions	51
15 Module 1: Lab 6: Manage Identity and Access	52
16 Lab 5: Introduction to Identity Protection in Azure	53
16.1 Exercise 1: Role-Based Access Control	53
16.1.1 Task 1: Create a User	53
16.1.2 Task 2: Create Groups In Portal, PowerShell, and CLI	55
16.2 Exercise 2: Practice - RBAC	55
16.2.1 Task 1: Create a resource group	55
16.2.2 Task 2: Grant access	56
16.2.3 Task 3: Remove access	56
16.3 Exercise 3: Role-based Access Control (RBAC) using PowerShell	57
16.3.1 Task 1: Grant access	57
16.3.2 Task 2: List access	58
16.3.3 Task 3: Remove access	58
17 Module 1: Lab 7: Azure Policy	58
17.1 Exercise 1: Using Azure Policy	58
17.1.1 Task 1: Create an Azure Policy Assignment	58
17.1.2 Task 2: Verify the Azure Policy Assignment	63
18 Module 1: Lab 8: Protecting Azure Resources with Resource Manager Locks	65
19 Lab 7: Protecting Azure Resources with Resource Manager Locks	66
19.1 Exercise 1: Creating Locks	66
19.1.1 Task 1: Adding a Lock (Portal)	66
19.1.2 Task 2: Adding a Lock (PowerShell)	66
20 Module 1: Lab 9: Transferring Subscriptions	67
20.1 Exercise 1: Transfer Azure subscriptions between Azure AD tenants	67
20.1.1 Task 1: To transfer the ownership of an Azure subscription	67
21 Module 2: Lab 2 - Function Apps	70
21.1 Exercise 1: Create a Function and Trigger	70
21.1.1 Task 1: Lab Setup	70
21.1.2 Task 2: Add a HTTP trigger to your function app	70
21.1.3 Task 3: Test a REST call to the HTTP trigger	71

22 Module 2: Lab 3 - Create a Kubernetes Cluster	72
22.1 Exercise 1: Create an AKS environment	72
22.1.1 Task 1: Prepare the environment and Create a Resource Group.	72
22.1.2 Task 2: Create the AKS Cluster in CLI	72
22.1.3 Task 3: Connect to the cluster	72
22.1.4 Task 4: Run the application	73
22.1.5 Task 5: Test the application	73
22.1.6 Task 6: Monitor health and logs	74
22.1.7 Task 7: Delete the cluster	74
23 Module 2: Lab 4 - Create a VNet	75
23.1 Exercise 1: Create a virtual network using the Azure portal	75
23.1.1 Task 1: Create a virtual network	75
23.1.2 Task 2: Create virtual machines	75
23.1.3 Task 3: Create the second VM	76
23.1.4 Task 4: Connect to a VM from the internet	76
23.1.5 Task 5: Communicate between VMs	77
24 Module 2: Lab 5 - NSGs	78
24.1 Exercise 1: Filter network traffic with a network security group using the Azure portal	78
24.1.1 Task 1: Create a virtual network	78
24.1.2 Task 2: Create application security groups	78
24.1.3 Task 3: Create a network security group	79
24.1.4 Task 4: Associate network security group to subnet	79
24.1.5 Task 5: Create security rules	79
24.1.6 Task 6: Create virtual machines	79
24.1.7 Task 7: Create the second VM	80
24.1.8 Task 8: Associate network interfaces to an ASG	80
24.1.9 Task 9: Test traffic filters	80
25 Module 2: Lab 6 - NVA	81
25.1 Exercise 1: Route network traffic with a route table using the Azure portal	82
25.1.1 Task 1: Create a route table	82
25.1.2 Task 2: Create a route	82
25.1.3 Task 3: Associate a route table to a subnet	82
25.1.4 Task 4: Add subnets to the virtual network	83
25.1.5 Task 5: Associate myRouteTablePublic to your Public subnet	83
25.1.6 Task 6: Create an NVA	84
25.1.7 Task 7: Turn on IP forwarding	85
25.1.8 Task 8: Create public and private virtual machines	85
25.1.9 Task 9: Route traffic through an NVA	86
25.1.10 Task 10: Enable ICMP through the Windows firewall	86
25.1.11 Task 11: Turn on IP forwarding within myVmNva	87
25.1.12 Task 12: Test the routing of network traffic	87
26 Module 2: Lab 7: Service Endpoints	88
26.1 Exercise 1: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal	88
26.1.1 Task 1: Create a virtual network	88
26.1.2 Task 2: Enable a service endpoint	88
26.1.3 Task 3: Restrict network access for a subnet	89
26.1.4 Task 4: Restrict network access to a resource	91
26.1.5 Task 5: Create a file share in the storage account	91
26.1.6 Task 6: Restrict network access to a subnet	91
26.1.7 Task 7: Create virtual machines	92
26.1.8 Task 8: Confirm access to storage account	92
26.1.9 Task 9: Confirm access is denied to storage account	93
27 Module 2: Lab 8 - VNet Peering	94
27.0.1 Exercise 1: Create Virtual Networks and implement Peering.	94
27.0.2 Task 1: Create virtual networks	94

27.0.3 Task 2: Peer virtual networks	94
27.0.4 Task 3: Create virtual machines	95
27.0.5 Task 4: Communicate between VMs	97
28 Lab 9: Azure DNS	98
28.1 Exercise 1: DNS Zones	98
28.1.1 Task 1: Create a DNS zone	98
28.2 Exercise 2: Manage DNS records and record sets by using the Azure portal	99
28.2.1 Task 1: Add a new record to a record set	99
28.2.2 Task 2: Update a record	100
28.2.3 Task 3: Remove a record from a record set	101
29 Module 2: Lab 10 - Load Balancer	103
29.1 Exercise 1: Distributing Network Traffic using a Standard Load Balancer	103
29.1.1 Task 1: Create a public load balancer	103
29.1.2 Task 2: Create a virtual network	104
29.1.3 Task 3: Create virtual machines	105
29.1.4 Task 4: Install IIS	106
29.1.5 Task 5: Create load balancer resources	106
29.1.6 Task 6: Create a health probe	108
29.1.7 Task 7: Create a load balancer rule	109
29.1.8 Task 8: Test the load balancer	111
29.2 Exercise 2: Load Balancer ARM Deployments	112
29.2.1 Task 1: Deploy an ARM template	112
30 Exercise 3: Deploying Application Gateways	113
30.0.1 Task 1: Create an application gateway	113
30.0.2 Task 2: Test the application gateway	122
31 Module 2: Lab 11: On-Prem to Azure Connections - VPN Gateways and Tunnelling	123
31.1 Exercise 1: Deploy Virtual Appliances and Gateways for intersite connectivity.	123
31.1.1 Task 1: Deploy a Virtual Appliance.	123
31.1.2 Task 2: Create a Resource Group and VNet.	124
31.1.3 Task 3: Create a Gateway Subnet and a Virtual network Gateway.	124
31.1.4 Task 4: Configure the Sophos virtual appliance.	126
31.1.5 Task 5: Creating Azure connection.	131
32 Module 2: Lab 12 - Azure Firewall	132
32.1 Exercise 1: Deploy an Azure Firewall	132
32.1.1 Task 1: Lab Setup	132
32.1.2 Task 2: Deploy the firewall	133
32.1.3 Task 3: Create a default route	135
32.1.4 Task 4: Configure an application rule	136
32.1.5 Task 5: Configure a network rule	137
32.1.6 Task 6: Change the primary and secondary DNS address for the Srv-Work network interface	137
32.1.7 Task 7: Test the firewall	137
33 Module 2 - Implement Platform Protection	138
33.1 Lab 13 - Secure Admin Access	138
33.2 Exercise 1: Deploy and connect to an Azure VM securely.	138
33.2.1 Task 1: Create SSH keys with PuTTYgen	138
33.2.2 Task 2: Create a Linux virtual machine in the Azure portal	142
33.2.3 Task 3: Connect to your VM	145
34 Module 2: Lab 14 - Azure Bastion	149
34.1 Exercise 1: Implement Azure Bastion	149
34.1.1 Task 1: Enable Azure Bastion on your subscription	149
34.1.2 Task 2: Create a bastion host	151
34.1.3 Task 3: Connect to a VM using a bastion host	153
35 Module 2: Lab 15 - Manage Azure DDoS Protection Standard	155

35.1	Exercise 1: Implement DDoS protection in Azure.	155
35.1.1	Task 1: Create a DDoS protection plan	155
35.1.2	Task 2: Enable DDoS for a new virtual network	156
35.1.3	Task 3: Disable DDoS for a virtual network	156
35.1.4	Task 4: Work with DDoS protection plans	156
35.1.5	Task 5: Configure alerts for DDoS protection metrics	156
35.1.6	Task 6: Use DDoS protection telemetry	158
35.1.7	Task 7: View DDoS mitigation policies	159
35.1.8	Task 8: Configure DDoS attack mitigation reports	159
35.1.9	Task 9: Configure DDoS attack mitigation flow logs	160
35.1.10	Task 10: Validate DDoS detection (Optional and not part of the AZ-500 course)	160
36	Module 2: Lab 16 - Antimalware for VMs	161
36.1	Exercise 1: Deploy Antimalware for Azure VMs.	161
36.2	Task 1: Create an Azure Virtual Machine with the Antimalware extension	161
37	Module 2: Lab 17 - Manage Windows updates by using Azure Automation	163
37.1	Exercise 1: Use Azure Automation to manage Windows Updates.	163
37.1.1	Task 1: Create a Resource Group	163
37.1.2	Task 2: Create Automation account	163
37.1.3	Task 3: Create a VM for use	164
37.1.4	Task 4: Enable Update Management	164
37.1.5	Task 5: View Update assessment	164
37.1.6	Task 6: Configure Alerts	165
37.1.7	Task 7: Schedule an Update Deployment	165
37.1.8	Task 8: View results of an update deployment	165
38	Module 2: Lab 18 - Custom Domains	166
38.0.1	Exercise 1: Add your custom domain name using the Azure Active Directory portal	166
38.0.2	Task 1: Add your custom domain name to Azure AD	166
38.0.3	Task 2: Add your DNS information to the domain registrar	168
38.0.4	Task 2: Verify your custom domain name	168
39	Module 2: Lab 19 - Private DNS	170
39.1	Exercise 1: Create an Azure private DNS zone using the Azure portal	170
39.1.1	Task 1: Create a private DNS zone	170
39.1.2	Task 2: Create a virtual network	170
39.1.3	Task 3: Link the virtual network	170
39.1.4	Task 4: Create the test virtual machines	171
39.1.5	Task 5: Create an additional DNS record	172
39.1.6	Task 6: Test the private zone	172
39.1.7	Task 7: Ping the VMs by name	172
40	Module 2: Lab 20 - Azure Blueprints	173
40.1	Exercise 1: Create a blueprint in the portal	173
40.1.1	Task 1: Create a blueprint	173
40.1.2	Task 2: Edit a blueprint	176
40.1.3	Task 3: Publish a blueprint	177
40.1.4	Task 4: Assign a blueprint	178
40.1.5	Task 5: Track deployment of a blueprint	179
40.1.6	Task 6: Unassign a blueprint	180
40.1.7	Task 6: Delete a blueprint	180
41	Module 2: Lab 1 - Monitor & Autoscale	180
41.1	Exercise 1: Lab setup	181
41.2	Exercise 2: Create your first Autoscale setting	181
41.3	Exercise 3: Scale based on a schedule	181
41.4	Exercise 4: Scale differently on specific dates	181
41.5	Exercise 5: View the scale history of your resource	182
41.6	Exercise 6: View the scale definition of your resource	182
42	Module 3: Classify a SQL Database	182

42.1 Exercise 1: Classify your SQL Database	182
42.1.1 Task 1: Lab Setup	182
42.2 Exercise 2: Begin Classification	183
43 Module 3: Auditing a Database	183
43.1 Exercise 1: Enable auditing on your database	183
43.1.1 Task 1: Lab Setup	183
43.1.2 Task 2: Enable auditing on your database	183
43.2 Exercise 2: Review audit logs	184
43.2.1 Task 1: Review audit logs on the SQL DB.	184
44 Module 3: Analyze audit logs and reports	184
44.1 Exercise 1: Get started with SQL database auditing	184
44.1.1 Task 0: Lab Setup	184
44.1.2 Task 1 - Set up auditing for your database	184
44.1.3 Task 2 - Analyze audit logs and reports	185
45 Module 4: Lab 1 - Azure Monitor	186
45.1 Exercise 1: Collect data from an Azure virtual machine with Azure Monitor	186
45.1.1 Task 1: Deploy an Azure VM to monitor.	186
45.1.2 Task 2: Create a workspace	186
45.1.3 Task 2: Enable the Log Analytics VM Extension	189
45.1.4 Task 3: Collect event and performance of a Windows VM.	189
45.1.5 Task 4: View data collected	191
45.2 Exercise 2: Monitor Websites with Azure Monitor Application Insights	192
45.2.1 Task 1: Enable Application Insights	192
45.2.2 Task 2: Create an HTML file	193
45.2.3 Task 3: Configure App Insights SDK	193
45.2.4 Task 4: Start monitoring in the Azure portal	193
46 Module 4: Lab 2 -Security Center	196
46.1 Exercise 1: Onboard your Azure subscription to Security Center Standard	196
46.1.1 Task 1: Automate data collection	196
46.2 Exercise 2: Onboard Windows computers to Azure Security Center	197
46.2.1 Task 1: Add new Windows computer	197
46.3 Exercise 3: Manage and respond to alerts in Azure Security Center	199
46.3.1 Task 1: Manage your alerts	199
46.3.2 Task 2: Respond to recommendations	201
47 Module 4: Lab 3 - Event hub	202
47.1 Exercise 1: Implementing Event Hub	203
47.1.1 Task 1: Enabling Event Hubs Namespace	203
47.1.2 Task 2: Create a storage account for later user	203
47.1.3 Task 3: Create new event hub	203
47.1.4 Task 4: Collect data to be able to send events into event hubs	204
47.1.5 Task 5: Download the script files	204
47.1.6 Task 6: Send some events to Event Hub	204
47.1.7 Task 7: Review the Events in EventHub and Blob Storage	204
47.1.8 Task 8: Review the Events from a REST query to the Blob storage	205
48 Module 4: Lab 4 - Azure Sentinel	205
48.1 Exercise 1: On-board Azure Sentinel	205
48.1.1 Task 1: Enable Azure Sentinel	205
48.1.2 Task 3: Connect data sources	206
49 Module 4: Lab 5 - Manage endpoint protection issues with Azure Security Center	208
49.1 Exercise 1: Implement the recommendation	209
49.1.1 Task 1: Install antimalware on Azure VMs	209
50 Module 4: Lab 6 - Security Playbook in Azure Sentinel	210
50.1 Exercise 1: Create and manage a Security Playbook in Azure.	210
50.1.1 Task 1: How to create a security playbook.	210

50.1.2 Task 2: How to run a security playbook	212
50.2 Exercise 2: Automate threat responses	213
50.2.1 Task 1: Automate Responses	213
51 Module 4: Lab 7 - Secure score in Azure Security Center	213
51.1 Exercise 1: Improve your secure score in Azure Security Center.	214
51.1.1 Task 1: View the secure score in the Azure Portal.	214
51.1.2 Task 2: View the individual secure scores.	214
52 Module 4: Lab 8 - Create security baselines	215
52.1 Exercise 1: Create an Identity & Access Management (IAM) baseline	215
52.1.1 Task 1: Restrict access to the Azure AD administration portal	215
52.1.2 Task 2: Enable Azure Multi-Factor Authentication (MFA)	216
52.1.3 Task 3: Block remembering MFA on trusted devices	217
52.1.4 Task 4: About guests	217
52.1.5 Task 5: Password options	218
52.1.6 Task 6: Establish an interval for reconfirming user authentication methods	218
52.1.7 Task 7: Disable Members invitations	218
52.1.8 Task 8: Users to create and manage security groups	219
52.1.9 Task 9: Self-service group management enabled	219
52.1.10 Task 10: Application options - Allow users to register apps	220
52.2 Exercise 2: Create an Azure Security Center baseline	220
52.2.1 Task 1: Enable System Updates	220
52.2.2 Task 2: Enable Security Configurations	221
52.2.3 Task 3: Enable Send me emails about alerts	224
52.2.4 Task 4: Enable Send email also to subscription owners	224
52.3 Exercise 3: Create an Azure storage accounts baseline	224
52.3.1 Task 1: Require security-enhanced transfers	224
52.3.2 Task 2: Enable binary large object (blob) encryption	225
52.3.3 Task 3: Periodically regenerate access keys	226
52.3.4 Task 4: Require Shared Access Signature (SAS) tokens to expire within an hour	227
52.3.5 Task 5: Require only private access to blob containers	228
52.4 Exercise 4: Create an Azure SQL Database baseline	228
52.4.1 Task 1: Enable auditing	229
52.4.2 Task 2: Enable a threat detection service	230
52.4.3 Task 3: Enable all threat detection types	231
52.5 Exercise 5: Create a logging and monitoring baseline	231
52.5.1 Task 1: Ensure that a log profile exists	231
52.5.2 Task 2: Change activity log retention is set to 365 days or more	233
52.5.3 Task 3: Create an activity log alert for "Creating, updating, or deleting a Network Security Group"	233
52.6 Exercise 6: Create a Networking baseline	236
52.6.1 Task 1: Restrict RDP and SSH access from the Internet	236
52.6.2 Task 2: Restrict SQL Server access from the Internet	237
52.6.3 Task 3: Configure the NSG flow logs	237
52.6.4 Task 4: Enable Network Watcher	238
52.7 Exercise 7: Create an Azure VM baseline	238
52.7.1 Task 1: Ensure that OS disk are encrypted	238
52.7.2 Task 2: Ensure only approved extensions are installed	240
53 Module 4: Lab 9 - JIT	240
53.1 Exercise 1: Manage virtual machine access using just-in-time	241
53.1.1 Task 1: Configure JIT access on a VM in Azure Security Center	241
53.1.2 Task 2: Request JIT access via ASC	245
53.1.3 Task 3: Edit a JIT access policy via ASC	246
53.1.4 Task 4: Audit JIT access activity in ASC	246
53.1.5 Task 5: Configure JIT access on a VM via the Azure VM blade	246
53.1.6 Task 5: Request JIT access to a VM via the Azure VM blade	247

1 AZ-500 Azure Security (old)

A new version of AZ-500 was released 17 July. There is a new lab repository to go with the content update - AZ500X-AzureSecurityTechnologies. Please move to this new version of the course and labs.

- **Are you a MCT?** - Have a look at our [GitHub User Guide for MCTs](#)
- **Need to manually build the lab instructions?** - Instructions are available in the [MicrosoftLearning/Docker-Build](#) repository

Be sure to use the [MCT Courseware Forum](#) for suggestions or general comments on the course content. Also, bugs and course errors can be reported on the [Courseware Support Forum](#).

To support the new changes, we introduced a new AZ-500 GitHub repository, starting on November 1 2019. At that time, all the AZ-500 labs have been replaced with this repository.

What are we doing?

- We are publishing the lab instructions and lab files on GitHub to allow for interaction between the course authors and MCTs. We hope this will help keep the content current as the Azure platform changes.
- This is an old GitHub repository for the AZ-500, Microsoft Azure Security course.
- Within each repository there are lab guides in the Markdown format in the Instructions folder. If appropriate, there are also additional files that are needed to complete the lab within the Allfiles\Labfiles folder. Not every course has corresponding lab files.
- For each delivery, trainers should download the latest files from GitHub. Trainers should also check the Issues tab to see if other MCTs have reported any errors.
- Lab timing estimates are provided but trainers should check to ensure this is accurate based on the audience.
- To do the labs you will need an internet connection and an Azure subscription. Please read the Instructor Prep Guide for more information on using the Cloud Shell.

How are we doing?

- If as you are teaching these courses, you identify areas for improvement, please use the Issues tab to provide feedback. We will periodically create new files to incorporate the changes.
- When launching Azure Cloud Shell for the first time, you will likely be prompted to create an Azure file share to persist Cloud Shell files. If so, you can typically accept the defaults, which will result in creation of a storage account in an automatically generated resource group. Note that this might happen again if you delete that storage account.
- Before you perform a template based deployments, you might need to register providers that handle provisioning of resource types referenced in the template. This is a one-time operation (per subscription) required when using Azure Resource Manager templates to deploy resources managed by these resource providers (if these resource providers have not been yet registered). You can perform registration from the subscription's Resource Providers blade in the Azure portal or by using Cloud Shell to run Register-AzResourceProvider PowerShell cmdlet or az provider Azure CLI command.

We hope using this GitHub repository brings a sense of collaboration to the labs and improves the overall quality of the lab experience.

1.1 Regards, *Azure Security Courseware Team*

1.2 title: Online Hosted Instructions permalink: index.html layout: home

2 Content Directory

Hyperlinks to each of the lab exercises and demos are listed below.

2.1 Labs

```
{% assign labs = site.pages | where_exp:"page", "page.url contains '/Instructions/Labs'" %} | Module | Lab | --- | --- | {%- for activity in labs %}{{ activity.lab.module }} | {{ activity.lab.title }}{% if activity.lab.type %} - {{
```

```
activity.lab.type }}{{% endif %}}]({{/home/ll/Azure_clone/Azure_new/AZ-500-Azure-Security/{{ site.github.url }}}}{{{ activity.url }}}) | {{% endfor %}}
```

2.2 Demos

```
{% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module  
| Demo | | --- | --- | {{% for activity in demos %}}| {{ activity.demo.module }} | [{{ activity.demo.title }}]({{/home/ll/Azure_clone/Azure_new/AZ-500-Azure-Security/{{ site.github.url }}}}{{{ activity.url }}}) | {{% endfor %}}
```

3 AZ500 Lab Files

This repository is a collection of setup scripts and templates for AZ500 labs. They compliment the lab exercises.

4 AZ500 Mod2 Lab1 setup

Click **Deploy to Azure**

This will deploy a new app and app service plan that can then be used to demonstrate the scale up options in AZ500 Mod2 Lab 1.

Populate the *site name, service plan name and resource group* with **unique** names.

5 AZ500 Mod2 Lab2 setup

Click **Deploy to Azure**

This will deploy a new blank function app.

Populate the *site name, service plan name and resource group* with **unique** names.

This is the yaml file to support the kubernetes deployment lab

6 AZ500 Mod2 Lab 11 setup

Click **Deploy to Azure**

This will deploy a new resource group with 1 Vnet 2 VMs and 3 Subnets for the AZ500 Mod 2 Lab 11.

The resource group name must be Test-FW-RG

7 SQL Template database deployment

Click **Deploy to Azure**, this will load the template into azure for deployment. You will then need to populate the parameters specified in the lab guide.

The test data that will be loaded into the Db is AdventureworksLT

The firewall rules for the SQL server are set to allow all azure clients to access

8 SQL Template database deployment

Click **Deploy to Azure**, this will load the template into azure for deployment. You will then need to populate the parameters specified in the lab guide.

The test data that will be loaded into the Db is AdventureworksLT

The firewall rules for the SQL server are set to allow all azure clients to access

9 GoDeploy SQL Template database deployment

Click **Deploy to Azure**, this will load the template into azure for deployment. You will then need to populate the parameters specified in the lab guide. Alternatively the parameters are also in this JSON file that you can copy into the template deployment wizard

The test data that will be loaded into the Db is AdventureworksLT

The firewall rules for the SQL server are set to allow all azure clients to access

This repository is a collection of lab manuals for the AZ500 labs. They compliment the AZ500 Azure Security course.

10 Module 1: Lab 1 - Azure AD Privileged Identity Management

Scenario

In this lab, you'll learn how to use Azure Privileged Identity Management (PIM) to enable just-in-time administration and control the number of users who can perform privileged operations. You'll also learn about the different directory roles available as well as newer functionality that includes PIM being expanded to role assignments at the resource level. Lessons include:

- Getting Started with PIM
- PIM Security Wizard
- PIM for Directory Roles
- PIM for Role Resources

The Managing Identities course also covers Azure RBAC and Azure Active Directory. This content has been included here also to provide more context and foundation for the remainder of the course.

10.1 Azure AD Privileged Identity Management

10.2 Exercise 1 - Discover and Manage Azure Resources

10.2.1 Task 1: Lab Setup

This lab requires creating a user that will be used for PIM.

1. In the **Azure Portal** open the **Cloud Shell** in **PowerShell** mode. If prompted click **Create Storage**.
2. Run the following command to authenticate

```
Connect-AzureAD
```

Note: If you close your Cloud Shell session you may be required to enter this command again throughout the labs.

3. Run the following PowerShell Commands to create an AD user and password in your default domain

```
$PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile  
$PasswordProfile.Password = "Pa55w.rd"  
$domainObj = get-azureaddomain  
$domain = $domainObj[0].name  
New-AzureADUser -DisplayName "Isabella Simonsen" -PasswordProfile $PasswordProfile -UserPrincipalName isabella.simonsen@contoso.com
```

10.2.2 Task 2: Enable Azure AD Premium P2 trial and create a test user.

1. In the Azure Portal, on the Hub menu click **Azure Active Directory**.
2. Select **Licences** then **All Products**.
3. Click **Try / Buy**.

Licenses - All products

Default Directory - Azure Active Directory

« + Try / Buy + Assign ☰

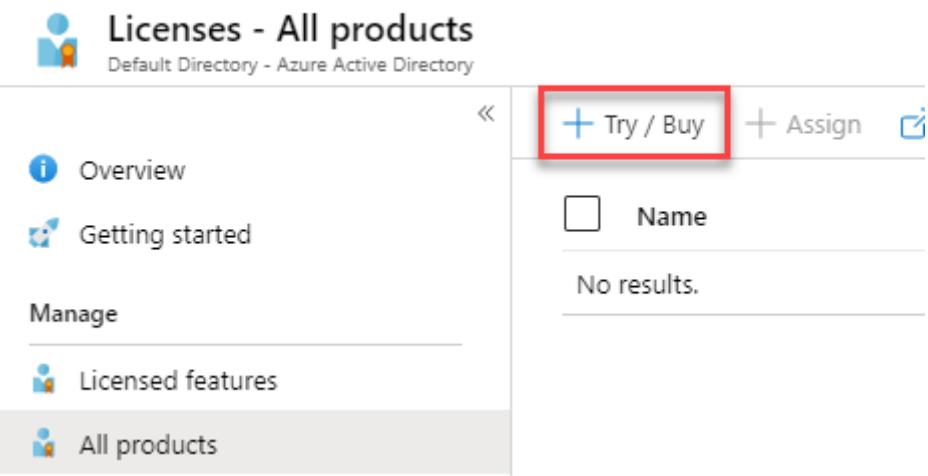
Overview Getting started

Manage

Licensed features

All products

No results.



4. Click the drop down arrow and select **Activate** on the **Azure AD Premium P2** product.

Activate

X

Browse available plans and features

i If you would like to purchase a subscription directly from Microsoft, please see the [Purchase services catalog](#).

ENTERPRISE MOBILITY + SECURITY E5

Enterprise Mobility + Security E5 is the comprehensive cloud solution to address your consumerization of IT, BYOD, and SaaS challenges. In addition to Azure Active Directory Premium P2 the suite includes Microsoft Intune and Azure Rights Management.

[More information](#)

▼ Free trial

AZURE AD PREMIUM P2

With Azure Active Directory Premium P2 you can gain access to advanced security features, richer reports and rule based assignments to applications. Your end users will benefit from self-service capabilities and customized branding.

[More information](#)

^ Free trial

Azure Active Directory Premium P2 enhances your directory with additional features that include multi-factor authentication, policy driven management and end-user self-service. [Learn more about features](#)

The trial includes 100 licenses and will be active for 30 days beginning on the activation date. If you wish to upgrade to a paid version, you will need to purchase Azure Active Directory Premium P2. [Learn more about pricing](#)

Azure Active Directory Premium P2 is licensed separately from Azure Services. By confirming this activation you agree to the [Microsoft Online Subscription Agreement](#) and the [Privacy Statement](#).

Activate

You may need to log out of the Azure portal and log in again for this to refresh

10.2.3 Task 3: Discover resources

1. In the Azure Portal, click All services and search for and select **Azure AD Privileged Identity Management**.

Microsoft Azure

All services

Azure AD Privileged Identity Management

Azure Database for MySQL servers

Azure AD Security

2. Click **Azure resources**.

Home > Privileged Identity Management - Quick start

Privileged Identity Management - Quick start

Quick start

Tasks

- My roles
- My requests
- Approve requests
- Review access

Manage

- Azure AD roles
- Azure AD custom roles (Preview)
- Azure resources

Activity

- My audit history

Introduction

Secure your organization

Azure AD Privileged Identity Management

Azure AD Privileged Identity Management

Azure AD Privileged Identity Management

What's new in Privileged Identity Management

- All services
- Azure Active Directory
- Azure resources

Feature update

Azure Active Directory

Improved activation of PIM

Friday, March 22, 2019

New feature

Azure Active Directory

3. Click **Discover resources** to launch the discovery experience.

The screenshot shows the 'Privileged Identity Management - Azure resources' interface. On the left, there's a sidebar with 'Quick start', 'Tasks' (including 'My roles', 'My requests', 'Approve requests', and 'Review access'), and a 'Manage' section. The main area has a 'Discover resources' button at the top, which is highlighted with a red box. Below it are sections for 'Subscription', 'Search by resource name', and 'Resource'. A note says 'Resources are only visible when you have an active role assigned'. There's also a placeholder text 'Discover resources or activate an eligible role assignment to c'.

4. On the Discovery pane, use **Resource state filter** and **Select resource type** to filter the management groups or subscriptions you have write permission to. It's probably easiest to start with **All** initially.

Azure resources - Discovery

The screenshot shows the 'Azure resources - Discovery' page. At the top are 'Refresh' and 'Manage resource' buttons. Below is a note: 'Discover Azure resources that you have write permission to.' A 'Resource state filter' dropdown is open, showing 'All' (which is highlighted with a red box), 'Managed', and 'Unmanaged'. To the right is a 'Subscription' dropdown with an unchecked checkbox for 'Azure Pass - Sponsorship'.

5. Add a checkmark next to your Azure subscription.

The screenshot shows a dropdown menu labeled 'Resource' with a single item: 'Azure Pass - Sponsorship', which has a checked checkbox next to it.

6. Click **Manage resource** to start managing the selected resources.

Azure resources - Discovery

The screenshot shows the 'Azure resources - Discovery' page. At the top, there is a 'Refresh' button and a 'Manage resource' button, which is highlighted with a red box. Below these are two sections: 'Discover Azure resources that you have write permissions for' and 'Resource state filter'. The 'Resource state filter' dropdown is set to 'All'. There is also a search bar labeled 'Search by resource name' and a section titled 'Resource' with a checked checkbox for 'Azure Pass - Sponsorship'.

7. Click **Yes** when prompted.

Note: You can only search for and select management group or subscription resources to manage using PIM. When you manage a management group or a subscription in PIM, you can also manage its child resources.

Note: Once a management group or subscription is set to managed, it can't be unmanaged. This prevents another resource administrator from removing PIM settings.

10.3 Exercise 2 - Assign Directory Roles

10.3.1 Task 1: Make a user eligible for a role

In the following task you will make a user eligible for an Azure AD directory role.

1. Sign in to Azure portal
2. In the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.

The screenshot shows the 'All services' page in the Microsoft Azure portal. On the left, there is a sidebar with options like 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The main area shows a list of services under 'All', including 'General', 'Compute', and 'Networking'. The 'Azure AD Privileged Identity Management' service is listed at the top, with its icon and name highlighted with a red box. Below it are 'Azure Database for MySQL servers' and 'Azure AD Security'.

3. Select **Azure AD Roles**.



Privileged Identity Management - Quick start

Privileged Identity Management

« Quick start

Tasks

- My roles
- My requests
- Approve requests
- Review access

Manage

- Azure AD roles
- Azure AD custom roles (Preview)
- Azure resources

Activity

- My audit history

Troubleshooting + Support

- Troubleshoot
- New support request

→ Introduction
Secure your c

Azure AD Priv
Azure AD Priv
Azure AD Priv

What's new in Pri

- All services
- Azure Active Direc
- Azure resources

Feature update

Azure Active Directo

Improved activatio

Friday, March 22, 201

New feature

Azure Active Directo

New alert on pote

Tuesday, January 1, 2

New feature

Azure Active Directo

4. Click **Roles**.

Home > Azure AD roles - Overview

Azure AD roles - Overview

Default Directory

Overview

Quick start

Tasks

- My roles
- My requests
- Approve requests
- Review access

Manage

- Roles**
- Members
- Alerts
- Access reviews
- Wizard
- Settings

5. Click **Add assignments** to open Add managed members.

Contoso | Roles

Privileged Identity Management | Azure AD roles

Quick start

Overview

Add assignments

Refresh

Search by role name

Role

6. Click the **Select role** dropdown and select **Billing Administrator**.

Add assignments

Privileged Identity Management | Azure AD roles

Membership Setting

Resource

Contoso

Resource type

Directory

Select role ⓘ

Billing Administrator

Select member(s) * ⓘ

No member selected

7. Click **No member selected**, select **Isabella** and then click **Select**.

Add assignments

Privileged Identity Management | Azure AD roles

Membership Setting

Resource

Contoso

Resource type

Directory

Select role ⓘ

Billing Administrator

Select member(s) * ⓘ

No member selected

Privileged Identity Management | Azure AD roles

Search



Isabella Simonsen
Isabella@m365x468213.onmicrosoft.com



MOD Administrator
admin@M365x468213.onmicrosoft.com

8. On the Add assignments blade, click **Next**.
9. Click **Assign** to add the user to the role.
10. Select the **Billing Administrator** role.
11. Review the added assignment.

Billing Administrator - Assignments

The screenshot shows the 'Billing Administrator - Assignments' page. On the left, there's a sidebar with 'Manage' and three options: 'Assignments' (selected), 'Description', and 'Role settings'. At the top right, there are buttons for '+ Add member', 'Settings', 'Refresh', and 'Export'. Below these are tabs for 'Eligible roles' (selected), 'Active roles', and 'Expired roles'. A search bar says 'Search by member name'. The main table has columns: Name, User principal name, Scope, Membership, Start time, and End time. One row is shown: 'Billing Administrator' assigned to 'Isabella Simonsen' (User principal name: Isabella@gdaztest19ou) with a scope of 'Directory', membership type 'Direct', start time '2/24/2020, 1:54:25 PM', and end time 'Permanent'.

- When the role is assigned, the user you selected will appear in the members list as **Eligible** for the role.

10.4 Exercise 3 - Activate and Deactivate PIM Roles

10.4.1 Task 1: Activate a role

When you need to take on an Azure AD directory role, you can request activation by using the **My roles** navigation option in PIM.

- Open an **In Private** browsing session and navigate to <https://portal.azure.com> and login as **Isabella** using her UPN. example Isabella@myaad.onmicrosoft.com with the password **Pa55w.rd**. When prompted change Isabella's password.
- In the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.

The screenshot shows the Microsoft Azure portal homepage. On the left, there's a sidebar with 'Create a resource', 'Home', 'Dashboard', 'All services' (selected), and 'FAVORITES'. The main area has a search bar at the top right with the placeholder 'Search resources, services...'. Below it, there's a 'All services' section with a search input field containing 'Azure AD Privileged Identity Man'. A red box highlights the first result: 'Azure AD Privileged Identity Management' with the keyword 'privileged'. Other results include 'Azure Database for MySQL servers' and 'Azure AD Security'.

- Click **Azure AD roles**.

Privileged Identity Management

The screenshot shows the 'Quick start' blade of the Azure AD Privileged Identity Management interface. It includes sections for 'Tasks', 'Manage', and 'Activity'. The 'Manage' section has a red box around the 'Azure AD roles' item, which is currently selected. Other items in the 'Manage' section include 'Azure AD custom roles (Preview)' and 'Azure resources'. The 'Activity' section contains 'My audit history'. The 'Troubleshooting + Support' section includes 'Troubleshoot' and 'New support request'.

- Tasks
 - My roles
 - My requests
 - Approve requests
 - Review access
- Manage
 - Azure AD roles
 - Azure AD custom roles (Preview)
 - Azure resources
- Activity
 - My audit history
- Troubleshooting + Support
 - Troubleshoot
 - New support request

- On the **Quick start** blade click **Activate your role**.

The screenshot shows the 'Activation' blade of the Azure AD Privileged Identity Management interface. It features four main buttons: 'Assign', 'Activate', 'Approve', and 'Audit'. The 'Activate' button is highlighted with a red box. Below each button is a brief description and a 'View more' link.

Assign	Activate	Approve	Audit
Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary	Activate your eligible admin roles so that you can get limit standing access to the privileged identity	View and approve all activation request for specific Azure AD roles that you are configured to approve	View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant
Assign eligibility	Activate your role	Approve requests	View your history

- On the Billing Administrator role, scroll to the right and click **Activate**.

Azure AD roles - My roles

Default Directory

Overview Quick start

Tasks

- My roles
- My requests
- Approve requests

My Azure AD roles

Eligible roles Active roles

Refresh

Role name	Status	Pending requests	Action
Billing Administrator	Not active	No pending requests.	Activate

6. Click **Additional verification required**. **Click to continue**. You only have to authenticate once per session. Run through the wizard to authenticate Isabella.

Activate - Billing Administrator

Privileged Identity Management - Azure AD roles

⚠️ Additional verification required. Click to continue ➔

Assignment details

Scope 

Default Directory

Start time  02/24/2020  2:15:40 PM

duration (hours) 

7. Once returned to the Azure Portal, enter an activation reason and click **Activate**.

Activate - Billing Administrator

Privileged Identity Management - Azure resources



Assignment details

Scope

Default Directory



Start time * ⓘ

02/24/2020



2:17:27 PM

duration (hours) ⓘ



8

Reason (max 500 characters) ⓘ

Activate

By default, roles do not require approval unless configured explicitly in settings.

If the role does not require approval, it is activated and added to the list of active roles. If you want to use the role right away, follow the steps in the next section.

If the role requires approval to activate, a notification will appear in the upper right corner of your browser informing you the request is pending approval.

10.4.2 Task 2: Use a role immediately after activation

When you activate a role in PIM, it can take up to 10 minutes before you can access the desired administrative portal or perform functions within a specific administrative workload. To force an update of your permissions, use the **Application access** page as described in the following steps.

1. Click **Sign Out**.

Activation status

Privileged Identity Management - Azure AD roles



Stage 1

Processing your request and activating your role.



Stage 2

Validating that your activation is successful.



Stage 3

Activation complete, use the link below to sign out and log back in to start using your newly activated role.

[Sign out](#)

2. Log back in as Isabella.

10.4.3 Task 3: Deactivate a role

Once a role has been activated, it automatically deactivates when its time limit (eligible duration) is reached.

If you complete your administrator tasks early, you can also deactivate a role manually in Azure AD Privileged Identity Management.

1. Still signed in as **Isabella**, open Azure AD Privileged Identity Management.
2. Click **Azure AD roles**.
3. Click **My roles**.

Azure AD roles - Quick start
Default Directory

Overview

Quick start

Tasks

My roles (highlighted with a red box)

My requests

Approve requests

Review access

Manage

Roles

Members

Alerts

- Click **Active roles** to see your list of active roles.

Azure AD roles - My roles
Default Directory

Overview

Quick start

Tasks

My roles (highlighted with a red box)

My requests

Approve requests

Review access

My Azure AD roles

Eligible roles Active roles (highlighted with a red box)

Refresh

Role name	Status	Action
Billing Administrator	Access valid until October 25 at 3:48 PM	Deactivate

- Find the role you're done using and then click **Deactivate**.

Azure AD roles - My roles
Default Directory

Overview

Quick start

Tasks

My roles (highlighted with a red box)

My requests

Approve requests

Review access

My Azure AD roles

Eligible roles Active roles (highlighted with a red box)

Refresh

Role name	Status	Action
Billing Administrator	Access valid until October 25 at 3:48 PM	Deactivate (highlighted with a red box)

- Click **Deactivate** again.

Deactivate - Billing Administrator

Privileged Identity Management | Azure AD roles

Group name	Contoso
Role	Billing Administrator
Member	Isabella Simonsen
Start time	04/05/2020, 06:31:51
End time	5/4/2020, 2:31:51 PM

Deactivate **Cancel**

10.4.4 Task 4: Cancel a pending request

If you do not require activation of a role that requires approval, you can cancel a pending request at any time.

1. Open Azure AD Privileged Identity Management.
2. Click Azure AD roles.
3. Click Pending requests.
4. For the role that you want to cancel, click the Cancel button.

Note: The cancel button in this task is greyed out as the request was approved.

When you click Cancel, the request will be cancelled. To activate the role again, you will have to submit a new request for activation.

10.5 Exercise 4 - Directory Roles (General)

10.5.1 Task 1: Start an access review for Azure AD directory roles in PIM

Role assignments become "stale" when users have privileged access that they don't need anymore. In order to reduce the risk associated with these stale role assignments, privileged role administrators or global administrators should regularly create access reviews to ask admins to review the roles that users have been given. This task covers the steps for starting an access review in Azure AD Privileged Identity Management (PIM).

1. Return back to the browser that is logged in as your Global Admin Account.
2. From the PIM application main page click **Azure AD Roles** under the **Manage** section click **Access reviews** and click > **New**.

Azure AD roles - Access reviews

Default Directory

The screenshot shows the 'Access reviews for Azure AD directory roles' page. At the top, there are navigation links: 'New' (highlighted with a red box), 'Filter', 'Group', and 'Settings'. Below that is a search bar. A table header row includes 'ROLE' and 'OWNER' with a sorting icon. The main area displays a table with one row: 'Azure AD Global Administrator' under ROLE and 'Global Administrator' under OWNER. On the left, a sidebar titled 'Azure AD roles - Access reviews' lists several options: Overview, Quick start, Tasks (My roles, My requests, Approve requests, Review access), Manage (Roles, Members, Alerts, Access reviews, Wizard, Settings). The 'Access reviews' option in the Manage section is also highlighted with a red box.

3. Enter the following details and click **Start**:

- Review name: **Global Admin Review**
- Start Date: **Today's Date**
- Frequency: **One time**
- End Date: **End of next month**
- Review role membership: **Global Administrator**
- Reviewers: **Select your account**

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * ✓

Description (i)

Start date * (i) 02/24/2020

Frequency ▼

Duration (in days) (i) 1

End (i) Never End by Occurrences

Number of times

End date * (i) 03/31/2020

Users

Scope Everyone

*Review role membership

Global Administrator

Start

4. Once the review has completed and has a status of Active, click on the **Global Admin Review**.

Note: You may have to refresh your browser.

5. Select **Results** and see the outcome of **Not reviewed**.

Global Admin Review - Results

« Download

i Overview

Manage

Results

Reviewers

Settings

Search

User	Outcome	Reason
go deploy gdaztest14@outl...	Not reviewed	

10.5.2 Task 2: Approve or deny access

When you approve or deny access, you're just telling the reviewer whether you still use this role or not. Choose Approve if you want to stay in the role, or Deny if you don't need the access anymore. Your status won't change right away, until the reviewer applies the results. Follow these steps to find and complete the access review:

1. In the PIM application, select **Review access**.
2. Select the **Global Admin Review**.

The screenshot shows the 'Review access - Azure AD roles' page within the 'Privileged Identity Management' section. On the left, there's a sidebar with 'Review access' highlighted. The main area lists 'Azure AD roles' and 'Azure resources' under 'Review access'. To the right, a panel titled 'Access reviews for Azure AD directory roles' shows a review named 'Global Admin Review', which is highlighted with a red box.

3. Since you created the review, you appear as the only user in the review. Select the check mark next to your name.

Global Admin Review

Filter Group

Essentials ^

Owner
go deploy[gdaztest14@outlook.com]

Require reason on approval

true

End date
12/31/2019

Remaining
1

Select the user(s) from the list, and approve or deny their role request.

Search

User

↑↓ Reason

Not reviewed



go deploy
gdaztest14@outlook.com

Reason *

Approve

Deny

Reset

- Close the **Review Azure AD roles** blade.

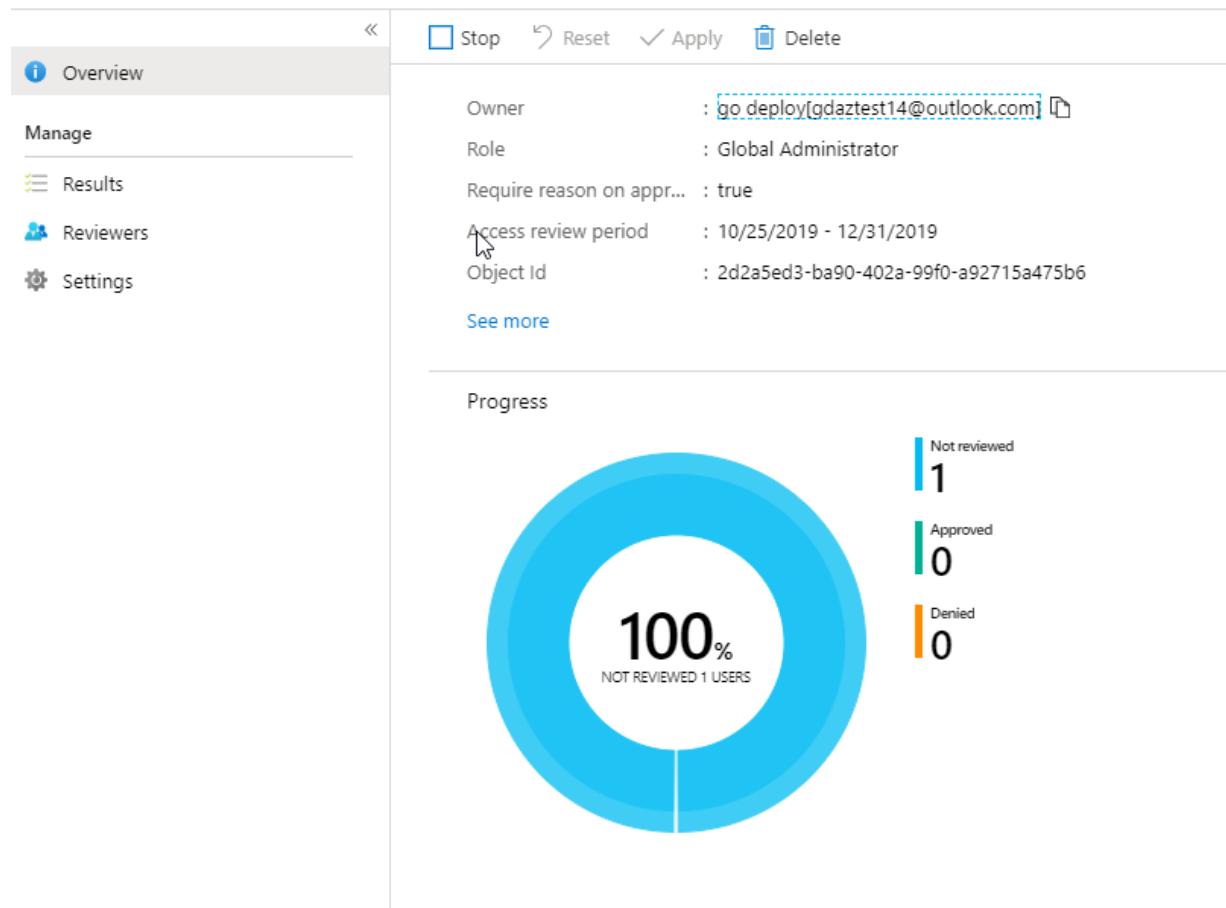
10.5.3 Task 3: Complete an access review for Azure AD directory roles in PIM

Privileged role administrators can review privileged access once an access review has been started. Azure AD Privileged Identity Management (PIM) will automatically send an email prompting users to review their access. If a user did not get an email, you can send them the instructions in how to perform an access review.

After the access review period is over, or all the users have finished their self-review, follow the steps in this task to manage the review and see the results.

- Go to the Azure portal and select the **Azure AD Privileged Identity Management**.
- Select **Azure AD Roles**.
- Select the **Access reviews**.
- Select the Global Admin Review.
- Review the blade.

Global Admin Review



10.5.4 Task 4: Configure security alerts for Azure AD directory roles in PIM

You can customize some of the security alerts in PIM to work with your environment and security goals. Follow these steps to open the security alert settings:

- Open **Azure AD Privileged Identity Management**.
- Click **Azure AD roles**.
- Click **Alerts** and then **Setting**.

The screenshot shows the 'Contoso | Alerts' page under 'Privileged Identity Management | Azure AD roles'. On the left, there's a sidebar with 'Quick start', 'Overview', 'Tasks' (including 'My roles', 'Pending requests', 'Approve requests', 'Review access'), 'Manage' (including 'Roles', 'Assignments', and 'Alerts'), and 'Access reviews'. The 'Alerts' item in the Manage section is highlighted with a red box. On the right, there are two tabs: 'Scan' and 'Setting', with 'Setting' also highlighted with a red box. Below the tabs, it says 'Alert' and 'No results'.

4. Click an alert name to see the settings for the preconfigured alerts.

10.6 Exercise 5 - PIM Resource Workflows

10.6.1 Task 1: Configure the Global Administrator role to require approval.

1. Open **Azure AD Privileged Identity Management**.
2. Click **Azure AD roles**.
3. Click **Roles** and select **Global Administrator**.
4. Click on **Role settings**.
5. On the **Role setting** blade, click on **Edit**.
6. Scroll down and select **Require Approval** and select your account as the approver then click **Select**.
7. On the **Edit role setting – Global Administrator** blade, click **Update**.

Edit role setting - Global Administrator

Privileged Identity Management - Azure AD roles

Activation Assignment Notification

Activation maximum duration (hours)

Azure MFA

On activation, require None

Require justification on activation

Require ticket information on activation

Require approval to activate

 Select approver(s)

1 Member(s), 0 Group(s) selected >

If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers.

Selected approvers:



10.6.2 Task 2: Enable Isabella for Global Administrator privileges.

1. Open Azure AD Privileged Identity Management.
2. Click Azure AD roles.
3. On the Quick Start blade, select Assign eligibility.



Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)



Assign

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary

[Assign eligibility](#)



Activate

Activate your eligible admin roles so that you can get limit standing access to the privileged identity

[Activate your role](#)



Approve

View and approve all activation request for specific Azure AD roles that you are configured to approve

[Approve requests](#)



Audit

View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant

[View your history](#)

4. Select **Global Administrator** and click **+ Add assignments**.
5. On the **Add assignments** blade, under **Select member(s)** click **No member selected**, select **Isabella** and click **Select > Next** and then **Assign**.
6. Open an in Private Browsing session and login to portal.azure.com as Isabella.
7. Open **Azure AD Privileged Identity Management**.
8. Select **My Roles**.

The screenshot shows the 'Privileged Identity Management - Quick start' page. On the left, there's a sidebar with 'Quick start' and 'Tasks'. Under 'Tasks', 'My roles' is highlighted with a red box. Other tasks include 'My requests', 'Approve requests', and 'Review access'. To the right, there's a large arrow pointing right with the text 'Introduc...', 'Secure...', and 'Azure A', 'Azure A', 'Azure A'. Below that is a 'What's new' section with checkboxes for 'All services' and 'Azure Active'.

9. **Activate** the Global Administrator Role.

The screenshot shows the 'My roles - Azure AD roles' page. On the left, there's a sidebar with 'Activate', 'Azure AD roles', 'Azure resources', 'Troubleshooting + Support', and 'New support request'. The 'Activate' button is highlighted with a red box. The main area shows a table with two rows: 'Global Administrator' (Status: Not active, Pending requests: 0 pending request(s)) and 'Billing Administrator' (Status: Not active, Pending requests: 0 pending request(s)). There's a 'Pending requests' column and an 'Action' column with a 'Activate' button, which is also highlighted with a red box.

10. Verify Isabella's identity using the wizard.

Activate - Global Administrator



Privileged Identity Management - Azure AD roles

⚠ Additional verification required. Click to continue →

Assignment details

Scope



Default Directory

Start time ⓘ

02/24/2020



3:31:33 PM

duration (hours) ⓘ



Reason (max 500 characters) ⓘ

- Once you are returned to the **Activate - Global Administrator** blade, enter the justification **I need to carry out some administrative tasks** and click **Activate**.

Activate - Global Administrator

Privileged Identity Management - Azure resources



Assignment details

Scope



Default Directory

Start time * ⓘ

02/24/2020



3:32:35 PM

duration (hours) ⓘ



8

*Reason (max 500 characters) ⓘ

I need to carry out some administrative tasks



Activate

10.6.3 Task 3: Approve or deny requests for Azure resource roles in PIM

With Azure AD Privileged Identity Management (PIM), you can configure roles to require approval for activation, and choose one or multiple users or groups as delegated approvers. Follow the steps in this article to approve or deny requests for Azure resource roles.

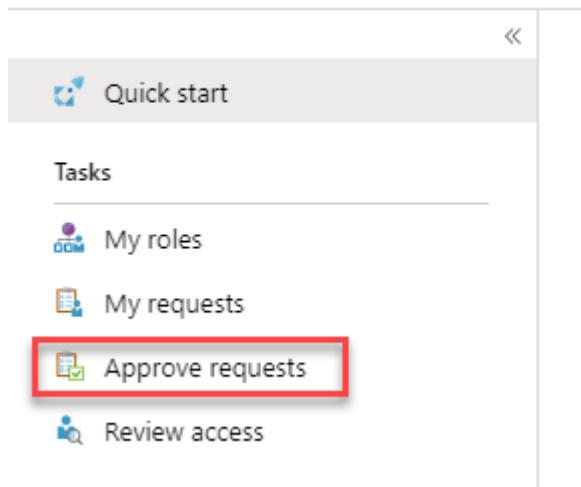
10.6.3.1 View pending requests

As a delegated approver, you'll receive an email notification when an Azure resource role request is pending your approval. You can view these pending requests in PIM.

1. Switch back to the browser you are signed in with your Global Administrative account.
2. Open **Azure AD Privileged Identity Management**.
3. Click **Approve requests**.

Privileged Identity Manager

Privileged Identity Management



Note: You may need to refresh your browser to see the request.

- Click the request from Isabella and enter the justification **Granted for this task** and click **Approve**.

The screenshot shows the 'Approve requests - Azure AD roles' page. On the left, there's a sidebar with options like 'Approve requests', 'Azure AD roles', 'Azure resources', 'Azure managed applications', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main area shows two tables of requests. The top table is titled 'Requests to renew or extend role assignments' and has a single row: 'No requests pending approval'. The bottom table is titled 'Requests for role activations' and has one row highlighted with a red box. This row shows a request from 'Global Administrator' to 'Isabella Simonsen' on '2/24/2020, 3:34 PM' for a 'Default Directory' resource with a 'Directory' assignment type. The justification 'I need to carry out s...' is visible.

- Switch back to the In Private Browsing session where Isabella is signed in and click My Roles and click the Active roles tab. Note the status.

The screenshot shows the 'My roles - Azure AD roles' page. The sidebar includes 'Activate' (selected), 'Azure AD roles', 'Azure AD custom roles (Preview)', 'Azure resources', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main area has tabs for 'Eligible roles' and 'Active roles' (selected). A table lists active roles with columns 'Role name' and 'Status'. The table shows two entries: 'Global Administrator' with status 'Access valid until October 25 at 4:15 PM' and 'Billing Administrator' with status 'Not active'.

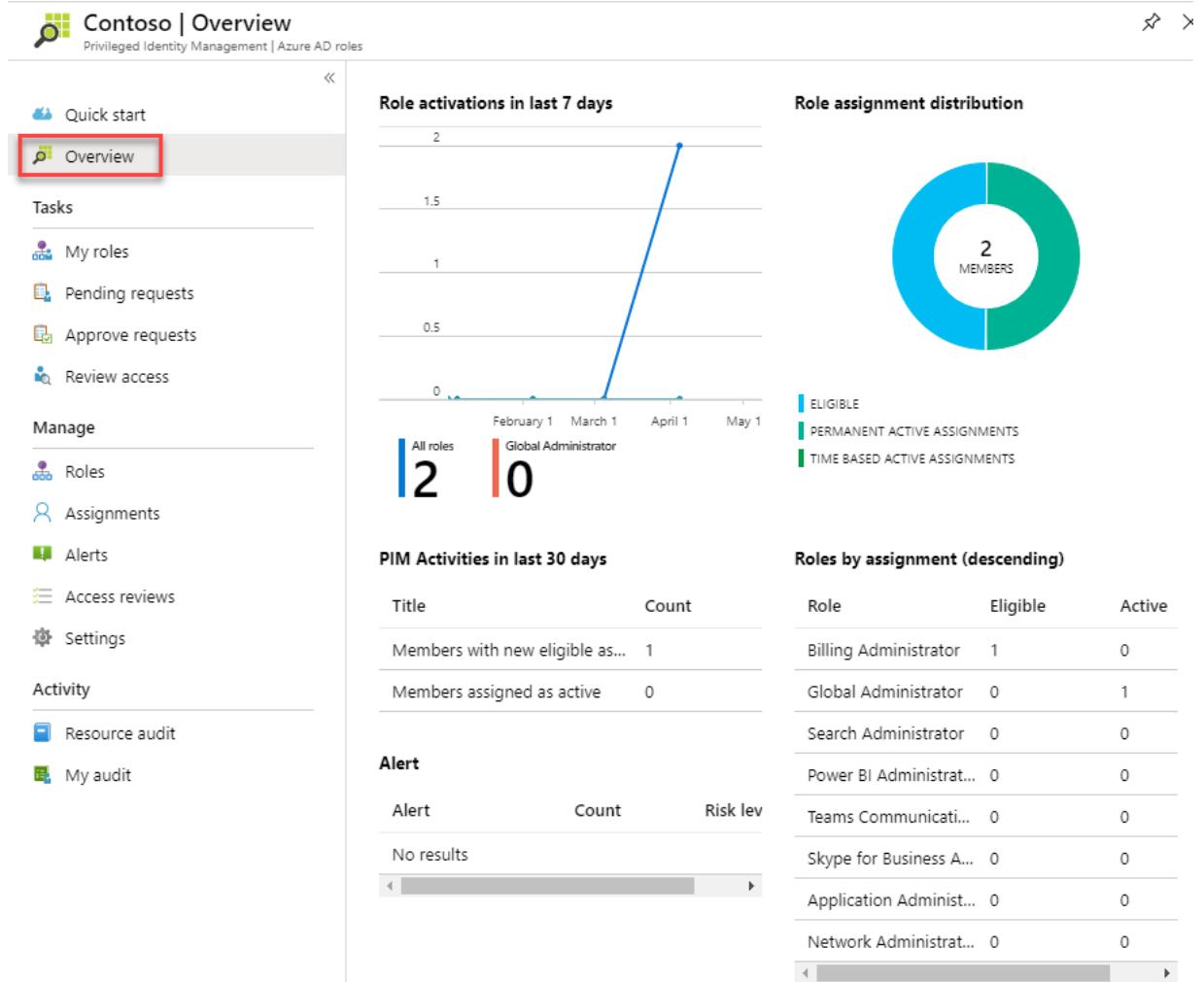
10.7 Exercise 6 - View audit history for Azure AD roles in PIM

You can use the Azure Active Directory (Azure AD) Privileged Identity Management (PIM) audit history to see all the role assignments and activations within the past 30 days for all privileged roles. If you want to see the full audit history of activity in your directory, including administrator, end user, and synchronization activity, you can use the [Azure Active Directory security and activity reports](#).

10.7.1 Task 1: View audit history

Follow these steps to view the audit history for Azure AD roles.

1. Open **Azure AD Privileged Identity Management**.
2. Click **Azure AD roles**.
3. Click to see the charts available.



4. Click **Resource audit**.

Depending on your audit history, a column chart is displayed along with the total activations, max activations per day, and average activations per day.

At the bottom of the page, a table is displayed with information about each action in the available audit history. The columns have the following meanings:

Column	Description
Time	When the action occurred.
Requestor	User who requested the role activation or change. If the value is Azure System , check the Azure audit history.
Action	Actions taken by the requestor. Actions can include Assign, Unassign, Activate, Deactivate, or AddedOutsideDomain.
Member	User who is activating or assigned to a role.
Role	Role assigned or activated by the user.
Reasoning	Text that was entered into the reason field during activation.
Expiration	When an activated role expires. Applies only to eligible role assignments.

5. To sort the audit history, click the **Time**, **Action**, and **Role** buttons.

10.7.2 Task 2: Filter audit history

- At the top of the audit history page, use the filter options to filter the results.

Results: You have now completed this lab.

11 Module 1 - Lab 2: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Scenario

This module includes the following tasks:

- Azure confidential computing
- Azure Key Vault

11.1 Exercise 1: Introduction to Azure Key Vault

Scenario

In this lab, you will get started with Azure Key Vault to create a hardened container (a vault) in Azure, to store and manage cryptographic keys and secrets in Azure. First you will use Azure PowerShell. Then you will store a password as a secret that could then be used with an Azure application.

11.1.1 Task 1: Download SQL Server Management Studio

- To download the latest version of SQL Management Studio required for this lab visit the following link and select download SQL Management Studio <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio>

Note: You do not need to wait for the SQL Management Studio to install before continuing.

11.1.2 Task 2: Use PowerShell to create a Key Vault

In this exercise, you will use PowerShell to create an Azure Key Vault.

- Start PowerShell by clicking **Start > PowerShell**

- Use the following command to authenticate to Azure using the account for your Azure subscription.

`Login-AzAccount`

- Create a new Resource Group

`New-AzResourceGroup -Name 'KeyVaultPSRG' -Location 'eastus'`

- Create a key vault in the resource group. **The VaultName must be unique therefore change to something unique.**

`New-AzKeyVault -VaultName '<keyvault name>' -ResourceGroupName 'KeyVaultPSRG' -Location 'eastus'`

Note: The output of this shows important pieces of information: Vault Name in this case that is KeyVaultPS and the Vault URI: <https://KeyVaultPS.vault.azure.net>

- In the Azure Portal open the **KeyVaultPSRG** Resource Group.

- Click on the Key Vault name to examine what you have created.

Note: For all future instructions replace KeyVaultPS with the name of your Key Vault.

- Click **Access Policies > + Add Access Policy**

- Select **Key, Secret and Certificate Management** from **Configure from template (optional)**

- Click **Select Principal** and search for and then click on your account, then click on **Select**

- Click **Add** and then **Save**

11.1.3 Task 3: Add a key and secret to Key Vault

1. Return to the PowerShell window.
2. Add a software-protected key to the Key Vault using this command. Be sure to change the placeholder text to your vault name.
`$key = Add-AZKeyVaultKey -VaultName '<YourVaultName>' -Name 'MyLabKey' -Destination 'Software'`
3. Move back to **KeyVaultPS** in the Azure portal. Click **Keys** under Settings in the left navigation pane.
4. Click **MyLabKey**
5. Click the Current Version.
6. Examine the information about the key you created.
Note: You can always reference this key by using its URI. To get the most current version, just reference <https://keyvaultps.vault.azure.net/keys/MyLabKey/> or if need be the exact version: <https://keyvaultps.vault.azure.net/keys/MyLabKey/da1a3a1efa5dxxxxxxxxxxxxd53c5959e>
7. Move back to the PowerShell window. To display the current version of the key, enter the following command.
`$Key.key.kid`
8. To view the Key you just created you can use the Get-AzureKeyVaultKey cmdlet. Be sure to change the placeholder text to your vault name.
`Get-AZKeyVaultKey -VaultName '<YourVaultName>'`

11.1.4 Task 4: Add a Secret to Key Vault

1. Next, you will add a secret to the **KeyVaultPS**. To do this, add a variable named **\$secretvalue** using the following code.
`$secretvalue = ConvertTo-SecureString 'Pa55w.rd1234' -AsPlainText -Force`
2. Next add the secret to the Vault with this command. Be sure to change the placeholder text to your vault name.
`$secret = Set-AZKeyVaultSecret -VaultName 'YourVaultName' -Name 'SQLPassword' -SecretValue $secretvalue`
3. Move back to the Azure Portal on **KeyVaultPS** and click **Secrets**
4. Click the Secret **SQLPassword**
5. Click the current version
6. Examine the Secret that you created
Note: You can always reference this key by using its URI. To get the most current version just reference <https://keyvaultps.vault.azure.net/secrets/SQLPassword> or if need be the exact version: <https://keyvaultps.vault.azure.net/secrets/SQLPassword/c5aada85d3acxxxxxxxxx8701efafcf3>
7. Click the **Show secret value** button -- notice that the password appears.
8. To view the Secret, use the Get-AzureKeyVaultSecret cmdlet. Be sure to change the placeholder text to your vault name.
`Get-AZKeyVaultSecret -VaultName 'YourVaultName'`

11.1.5 Task 5: Enable a Client Application

You will enable your client application to access the Azure SQL Database service. This will be done by setting up the required authentication and acquiring the Application ID and Secret that you will need to authenticate your application. These steps will be accomplished in the Azure portal.

1. Open the Azure portal and navigate to Azure Active Directory.
2. Click **App Registrations** under **Manage** in the left navigation pane.
3. Click **+ New registration**

4. Provide the name **sqlApp** for your application. Under **Redirect URI (optional)**, select **Web**, and for the SIGN-ON URL type **<https://sqlapp>**
5. Click **Register**.
6. Once the App Registration is complete click on **sqlApp** if it does not automatically appear.
7. Copy your Application (client) ID as you will need it later.
8. Click **Certificates & secrets**
9. Click **+ New client secret**
10. In the **Description** section, enter **Key1** for the description. Select **1 year** from the **Expires** list, then click **Add**
11. Copy the Key1 value as you will need it later. If you close and reopen the blade, the value will show as hidden.

11.1.6 Task 6: Add a Key Vault Policy allowing the application access to the Key Vault.

1. In the **Azure portal** open your **Resource Group** created at the beginning of the lab
2. Select the **Azure Key vault**
3. Click **Access Policies**
4. Select the account associated with your Azure subscription
5. In the **Key Permissions** drop down select **Select All** to highlight all permissions
6. Select **Save**

Important! You must click save otherwise the permissions will not be committed

7. Run the following Powershell in the **Powershell ISE** to set the sqlApp key permissions replacing the placeholder text with **your account details**

```
$subscriptionName = '[Azure_Subscription_Name]'  
$applicationId = '[Azure_AD_Application_ID]'  
$resourceGroupName = '[Resource_Group_with_KeyVault]'  
$location = '[Azure_Region_of_KeyVault]'  
$vaultName = '[KeyVault_Name]'  
  
Login-AzAccount  
  
Set-AZKeyVaultAccessPolicy -VaultName $vaultName -ResourceGroupName $resourceGroupName -ServicePrincipalName $applicationId -PermissionsToKeys get,delete,create,update,manageContacts,manageAliases,managePurge  
Set-AZKeyVaultAccessPolicy -VaultName $vaultName -ResourceGroupName $resourceGroupName -ServicePrincipalName $applicationId -PermissionsToSecrets get,delete,create,update,managePurge
```

11.1.7 Task 7: Use Key Vault to Encrypt Data with Azure SQL Database

Scenario

In this task, you will create a blank Azure SQL Database, connect to it with SQL Server Management Studio and create a table. You will then encrypt two data columns using an autogenerated key from the Azure Key Vault. Then you will create a Console application using Visual Studio to Load data into the Encrypted Columns and then access that data securely using a connection string that accesses the key via Key Vault.

1. From the Azure Portal click **+ Create a resource**> **Databases** > **SQL Database**
2. Provide the following details on the SQL Database blade and click **Create**.
 - Resource Group: (create new) **SQLEncryptRG**
 - Database Name: **medical**
 - Server: **Create new**
 - Server name: **[Unique Server Name]**
 - Server Admin Login: **demouser**
 - Password: **Pa55w.rd1234**
 - Location: **[same location as KeyVaultPS]**

- Then click **OK**
 - Pricing Tier: Standard S0
- Once everything above is configured, select **Review + create**, then **Create**
 - Once the SQL Database is deployed, open it in the Azure Portal to locate and then copy the **ADO.NET Connection String**.

Note: When you save the connection string for future use, be sure to replace {your_username} with **demouser** and {your_password} with **Pa55w.rd1234**.

11.1.8 Task 8: Create a Table in the SQL Database

- Use the Azure portal to locate the Server name where the Medical Database is located and copy the name.
- On this same blade click Set Server firewall.
- Next click + **Add client IP** and then click **Save**.
- Open SQL Server Management Studio. Connect to the Server using these properties for the **Connect to Server** dialog.
 - Server Type: **Database Engine**
 - Server Name: [found on the Database Overview Blade]
 - Authentication: **SQL Server Authentication**
 - Login: **demouser**
 - Password: **Pa55w.rd1234**

11.1.9 Task 9: Create and Encrypt a Table

- In SQL Server Management Studio expand **Databases > Right-click medical > New Query**.
- Paste the following code into the query window and click Execute

```
CREATE TABLE [dbo].[Patients] (
    [PatientId] [int] IDENTITY(1,1),
    [SSN] [char](11) NOT NULL,
    [FirstName] [nvarchar](50) NULL,
    [LastName] [nvarchar](50) NULL,
    [MiddleName] [nvarchar](50) NULL,
    [StreetAddress] [nvarchar](50) NULL,
    [City] [nvarchar](50) NULL,
    [ZipCode] [char](5) NULL,
    [State] [char](2) NULL,
    [BirthDate] [date] NOT NULL
)
```

- After the table is created successfully, expand **medical > tables > right-click dbo.Patients** and select **Encrypt Columns**.
- Click **Next**.
- On the Column Selection Screen check **SSN** and **Birthdate**. Then set the Encryption Type for SSN to **Deterministic** and for Birthdate **Randomized**. Click **Next**.

6. On the Master Key Configuration page on the Select the Key store provider, click **Azure Key Vault**. Click **Sign in** and authenticate. Select your Azure Key Vault. Click **Next**.
7. On the Run Settings screen click **Next** and then **Finish** to Proceed with the encrypting.
8. When the encryption process is complete, click **Close** and expand **medical > security > Always Encrypted Keys** and note that now there are keys found.

11.1.10 Task 10: Build a Console Application to work with Encrypted Columns

1. Open Visual Studio 2019 and Sign in using your Azure account.
2. Click **File > New > Project**
3. Next select **C# > Console App (.NET Framework)** and provide the name **OpsEncrypt** in the location **C:** and then click **Create**.
4. Right-Click the **OpsEncrypt** project > click **Properties**.
5. Change the **Target Framework** to **.NET Framework 4.7.2**. Click **Yes** when prompted to change the **Target Framework**.
6. Install the following **NuGet** packages by going to **Tools > NuGet Package Manager > Package Manager Console**.


```
Install-Package Microsoft.SqlServer.Management.AlwaysEncrypted.AzureKeyVaultProvider
Install-Package Microsoft.IdentityModel.Clients.ActiveDirectory
```
7. Open the **program.cs** file in notepad from **Allfiles\Labs\Mod1_Lab02** and copy the code.
8. Replace the code in **Program.cs** in Visual Studio with the code you just copied.
9. Locate the **Connection string, clientId, and clientSecret** settings in the Main method and replace them with the values that you copied from the previous steps.
10. Click the **Start Button** in Visual Studio.
11. The **Console Application** will **Build** and then start. First it will ask for your password, then the app will add data to the database.
 - Server Password: **Pa55w.rd1234**
12. Leave the **Console Application Running** and move to the **SQL Management Studio**. Right-Click the medical database and click **New Query**.
13. Run the following query to see the data that was loaded into the database is encrypted.


```
SELECT FirstName, LastName, SSN, BirthDate FROM Patients;
```

14. Now, move back to the console application where you will be asked to **Enter a Valid SSN**. This will query the encrypted column for the data. Notice that with the key called from the Key Vault, now the data is unencrypted and shown to the console window.

999-99-0003

15. To **Exit** you press enter.

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

Results : You have now completed this Lab.

12 Module 1: Lab 3: Using Multi-Factor Authentication for Secure Access

12.1 Exercise 1: MFA Authentication Pilot (Require MFA for specific apps with Azure Active Directory conditional access)

12.1.1 Task 1: Create your conditional access policy

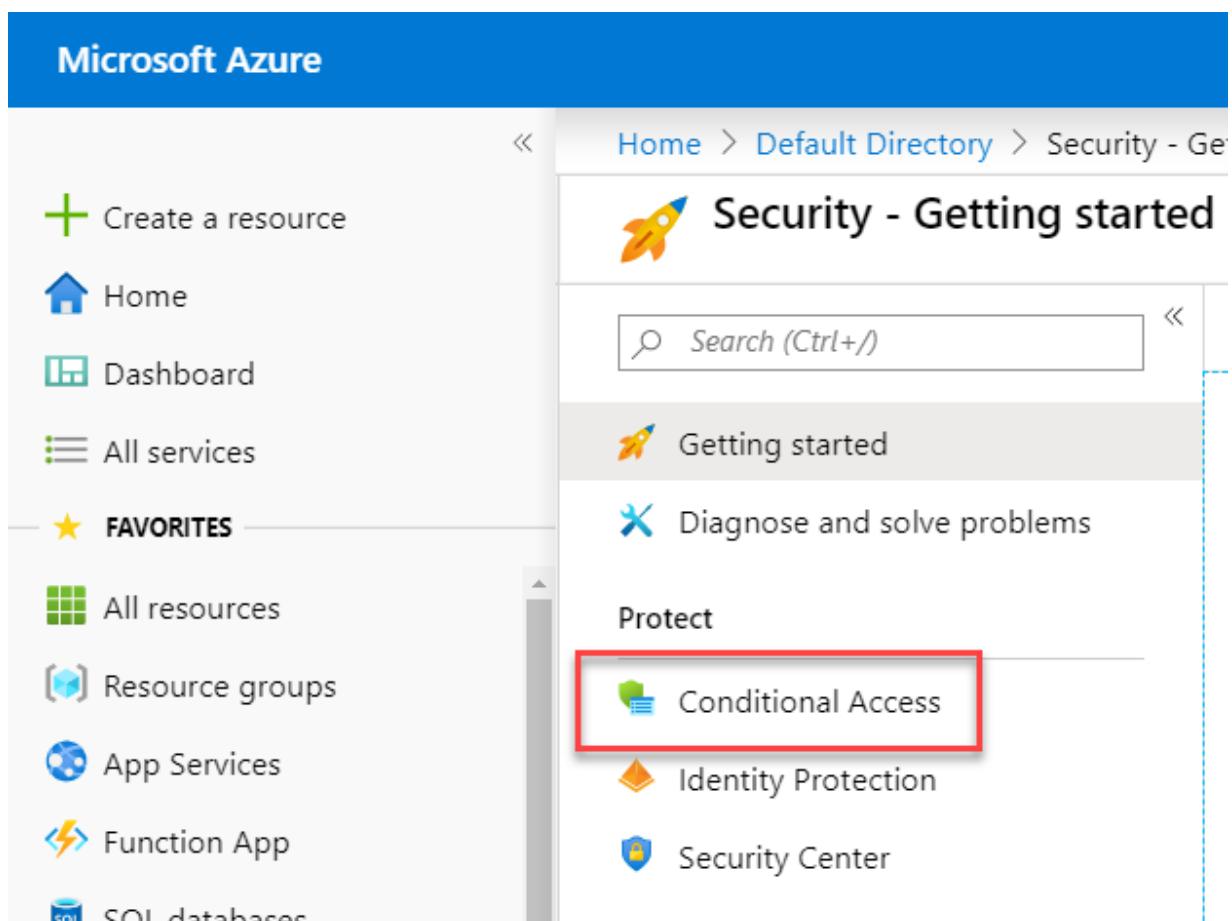
This section shows how to create the required conditional access policy. The scenario uses:

- The Azure portal as placeholder for a cloud app that requires MFA.
- Your sample user to test the conditional access policy.

In your policy, set:

Setting	Value
Users and groups	Isabella Simonsen
Cloud apps	Microsoft Azure Management
Grant access	Require multi-factor authentication

1. Sign in to the Azure Portal.
2. In the Azure portal, on the hub menu, click **Azure Active Directory**.
3. In the **Manage** section, click **Properties**, and click **Manage Security defaults**.
4. Change the **Enable Security defaults** option to **No**. Under reason, select **My organisation is using Conditional Access**, and click **Save**.
5. In the **Manage** section, click **Security**.
6. In the **Security** blade, click **Conditional access**.



7. On the **Conditional Access** page, in the toolbar on the top, click **New Policy**.

Note: if this is greyed out, refresh the browser session.

8. On the **New** page, in the **Name** textbox, type **Require MFA for Azure portal access**.
9. In the **Assignment** section, click **Users and groups**.
10. On the **Users and groups** page, perform the following steps:
 - a. Click **Select users and groups**, and then select **Users and groups**.
 - b. Click **Select**.
 - c. On the **Select** page, select **Isabella Simonsen**, and then click **Select**.
 - d. On the **Users and groups** page, click **Done**.
11. Click **Cloud apps or actions**.
12. On the **Cloud apps** page, perform the following steps:
 - a. Click **Select apps**.
 - b. Click **Select**.
 - c. On the **Select** page, select **Microsoft Azure Management**, and then click **Select**.
 - d. On the **Cloud apps** page, click **Done**.
13. In the **Access controls** section, click **Grant**.
14. On the **Grant** page, perform the following steps:
 1. Select **Grant access**.
 2. Select **Require multi-factor authentication**.
 3. Click **Select**.
15. In the **Enable policy** section, click **On**.
16. Click **Create**.

12.1.2 Task 2: Evaluate a simulated sign-in

Now that you have configured your conditional access policy, you probably want to know whether it works as expected. As a first step, use the conditional access what if policy tool to simulate a sign-in of your test user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report.

To initialize the what if policy evaluation tool, set:

- **Isabella Simonsen** as user
- **Microsoft Azure Management** as cloud app

Clicking **What If** creates a simulation report that shows:

- **Require MFA for Azure portal access** under **Policies that will apply**
 - **Require multi-factor authentication** as **Grant Controls**.
1. On the Conditional access - Policies page, in the menu on the top, click **What If**.

The screenshot shows the 'Conditional Access - Policies' page in the Azure Active Directory portal. On the left, there's a sidebar with 'Policies', 'Manage' (with options like 'Named locations', 'Custom controls (Preview)', 'Terms of use', 'VPN connectivity', and 'Classic policies'), and 'Troubleshooting + Support'. The main area has a top navigation bar with 'New policy', 'What If' (which is highlighted with a red box), and 'Got feedback?'. A blue banner below the navigation bar says, 'Interested in understanding the impact of the policies on a user sign-in?'. Below the banner, there's a section titled 'Policy Name' with a list of policy names: 'Baseline policy: Require MFA for admins (Preview)', 'Baseline policy: End user protection (Preview)', 'Baseline policy: Block legacy authentication (Preview)', 'Baseline policy: Require MFA for Service Management (Preview)', and 'Require MFA for Azure portal access'.

2. Click **Users**, select **Isabella Simonsen**, and then click **Select**.
3. To select a cloud app, perform the following steps:
 - a. Click **Cloud apps or actions**.
 - b. On the **Cloud apps** page, click **Select apps**.
 - c. Click **Select**.
 - d. On the **Select** page, select **Microsoft Azure Management**, and then click **Select**.
 - e. On the cloud apps page, click **Done**.
4. Click **What If**.
5. Note the result, **Require MFA for Azure portal access**.

The screenshot shows the 'Evaluation result' section. It has two tabs: 'Policies that will apply' (which is selected) and 'Policies that will not apply'. Below the tabs, there's a table with two columns: 'Policy Name' and 'Grant controls'. The 'Policy Name' column contains 'Require MFA for Azure portal access', and the 'Grant controls' column contains 'Require multi-factor authentication'.

Policy Name	Grant controls
Require MFA for Azure portal access	Require multi-factor authentication

12.1.3 Task 3: Test your conditional access policy

In the previous section, you have learned how to evaluate a simulated sign-in. In addition to a simulation, you should also test your conditional access policy to ensure that it works as expected.

To test your policy, try to sign-in to the Azure portal <https://portal.azure.com> using your **Isabella Simonsen** test account. You should see a dialog that requires you to set your account up for additional security verification.

12.2 Exercise 2: MFA Conditional Access (Complete an Azure Multi-Factor Authentication pilot roll out)

In this lab, you walk you through configuring a conditional access policy enabling Azure Multi-Factor Authentication (Azure MFA) when logging in to the Azure portal. The policy is deployed to and tested on a specific group of pilot users. Deployment of Azure MFA using conditional access provides significant flexibility for organizations and administrators compared to the traditional enforced method.

- Enable Azure Multi-Factor Authentication
- Test Azure Multi-Factor Authentication

12.2.1 Task 1: Enable Azure Multi-Factor Authentication

1. Return to the the Azure portal that is logged in as your Global Admin account.
2. On the Hub menu click **Azure Active Directory**,
3. Click **Groups** and click **+ New group**.

The screenshot shows the 'Groups - All groups' page in the Azure portal. At the top, it says 'Default Directory - Azure Active Directory'. Below that, there's a navigation bar with 'All groups' (selected), 'Deleted groups', 'Settings', and 'General'. To the right, there's a search bar labeled 'Search groups' and a 'Name' filter. In the center, there's a large button with a plus sign and the text '+ New group'.

4. Enter the following information then click **Create**:

- Group type; **Security**
- Group Name: **MFA Pilot**
- Group description: **MFA Pilot Group**
- Membership type: **Assigned**
- Members: Select **Isabella**

New Group

The screenshot shows the 'New Group' configuration page. It has several input fields with validation icons (green checkmarks) and dropdown menus. The fields are:

- Group type ***: Security
- Group name * ⓘ**: MFA Pilot
- Group description ⓘ**: MFA Pilot Group
- Membership type * ⓘ**: Assigned
- Owners**: (empty)
- Members**: 1 member selected

5. Browse to **Azure Active Directory**, click **Security** and select **Conditional access** on the **Security** Blade.
6. Select **+ New policy**
7. Name your policy **MFA Pilot**
8. Under **users and groups**, select the **Select users and groups** check box

- Select your pilot group **MFA Pilot**
 - Click **Select**
9. Under **Cloud apps or actions**, select the **Select apps** radio button
 - The cloud app for the Azure portal is **Microsoft Azure Management**
 - Click **Select**
 - Click **Done**
10. Skip the **Conditions** section
11. Under **Grant**, make sure the **Grant access** radio button is selected
 - Check the box for **Require multi-factor authentication**
 - Click **Select**
 - Click **Done**
12. Skip the **Session** section
13. Set the **Enable policy** toggle to **On**
14. Click **Create**

12.2.2 Task 2: Test Azure Multi-Factor Authentication

To prove that your conditional access policy works, you test logging in to a resource that should not require MFA and then to the Azure portal that requires MFA.

1. Open a new browser window in InPrivate or incognito mode and browse to <https://account.activedirectory.windows.net>
 - Log in with the Isabella account. You should not ask you to complete MFA.
 - Close the browser window.
2. Open a new browser window in InPrivate or incognito mode and browse to <https://portal.azure.com>
 - Log in with the Isabella account. You should now be required to register for and use Azure Multi-Factor Authentication.
 - Close the browser window.

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

Results : You have now completed this lab.

13 Module 1: Lab 4: App Registration

Scenario

Enterprise developers and software-as-a-service (SaaS) providers can develop commercial cloud services or line-of-business applications that can be integrated with Microsoft identity platform to provide secure sign-in and authorization for their services.

This lab shows you how to add and register an application using the App registrations experience in the Azure portal so that your app can be integrated with the Microsoft identity platform.

13.1 Exercise 1: Application Registration

13.1.1 Task 1: Register a new application using the Azure portal

1. Sign in to the Azure portal.
2. In the left-hand navigation pane, select the **Azure Active Directory** service, and then select **App registrations > New registration**.

The screenshot shows the 'Default Directory - App registrations' page in Azure Active Directory. At the top, there's a search bar and a 'New registration' button, which is highlighted with a red box. Below the search bar, there are links for 'Endpoints', 'Troubleshooting', and 'Got feedback?'. A welcome message says 'Welcome to the new and improved App registrations (now Generally Available). See what's new →'. A warning message says 'Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#). Still want to use App registrations (Legacy)? [Go back and tell us why](#)'. Below these, there are tabs for 'All applications', 'Owned applications', and 'Applications from personal account', with 'All applications' being the active tab. A search bar below the tabs says 'Start typing a name or Application ID to filter these results'. On the left, a sidebar titled 'Manage' lists various options: Overview, Getting started, Users, Groups, Organizational relationships, Roles and administrators, Enterprise applications, Devices, App registrations (which is also highlighted with a red box), Identity Governance, and Application proxy.

3. When the **Register an application** page appears, enter your application's registration information:

- **Name** - Enter: **Contoso App**
- **Supported account types** - Select **Accounts in this organizational directory only** (Read the options below).

Supported account types	Description
Accounts in this organizational directory only	Select this option if you're building
Accounts in any organizational directory	Select this option if you would like to
Accounts in any organizational directory and personal Microsoft accounts	Select this option to target the wide

- **Redirect URI (optional)** - Select **Web**, and then enter **https://app.contoso.com**
 - For web applications, provide the base URL of your app. For example, **http://localhost:31544** might be the URL for a web app running on your local machine. Users would use this URL to sign in to a web client application.
 - For public client applications, provide the URI used by Azure AD to return token responses. Enter a value specific to your application, such as **myapp://auth**.

1. When finished, select **Register**.

2. Azure AD assigns a unique application (client) ID to your app, and you're taken to your application's **Overview** page. To add additional capabilities to your application, you can select other configuration options including branding, certificates and secrets, API permissions, and more.

Contoso App

Display name : Contoso App
Application (client) ID : 46bb37d5-2c43-4de5-9dba-5150e92d3719
Directory (tenant) ID : 175a3ff3-9cd3-49a8-b60f-c27f49eeb562
Object ID : 16247541-cf97-4c61-81b9-8a0e4ccb2d13

Supported account types : My organization only
Redirect URIs : 1 web, 0 public client
Application ID URI : Add an Application ID URI
Managed application in ... : Contoso App

Call APIs

Documentation

Sign in users in 5 minutes

View all quickstart guides

Results: You have now completed this lab.

14 Module 1: Lab 5 - Application Service Principal

Scenario

This lab shows you how to create a new Azure Active Directory (Azure AD) application and service principal that can be used with role-based access control. When you have code that needs to access or modify resources, you can create an identity for the app. This identity is known as a service principal. You can then assign the required permissions to the service principal. This lab shows you how to use the portal to create the service principal. It focuses on a single-tenant application where the application is intended to run within only one organization. You typically use single-tenant applications for line-of-business applications that run within your organization.

14.1 Exercise 1: Use the portal to create a service principal that can access resources

You can set the scope at the level of the subscription, resource group, or resource. Permissions are inherited to lower levels of scope. For example, adding an application to the Reader role for a resource group means it can read the resource group and any resources it contains.

14.1.1 Task 1: Assign the application to a role

1. Navigate to the level of scope you wish to assign the application to. For example, to assign a role at the subscription scope, select **All services** and **Subscriptions**.

Microsoft Azure

All services

Subscriptions

2. Select your subscription.

The screenshot shows the Azure Subscriptions page. At the top, there's a breadcrumb navigation: Dashboard > Subscriptions. Below it, the title 'Subscriptions' is followed by 'Microsoft'. A blue 'Add' button is visible. A message says 'Showing subscriptions in Microsoft. Don't see a subscription? [Switch directories](#)'. Under 'My role', a dropdown shows '8 selected' with an 'Apply' button. A checked checkbox says 'Show only subscriptions selected in the [global subscriptions filter](#)'. A search bar contains 'Search to filter items...'. The main table has columns 'SUBSCRIPTION' and 'SUBSCRIPTION ID'. One row, 'Internal testing subscription', is highlighted with a red box.

3. Select **Access control (IAM)**.
4. Select **Add** and select **Add role assignment**.
5. Select the Contributor role you wish to assign to the application. To allow the application to execute actions like **reboot**, **start** and **stop** instances, select the **Contributor** role. By default, Azure AD applications aren't displayed in the available options. To find your application, search for the name **Contoso App** and select it.

The screenshot shows the 'Add role assignment' dialog. It has fields for 'Role' (set to 'Contributor'), 'Assign access to' (set to 'Azure AD user, group, or service principal'), and 'Select' (set to 'contoso'). Below these, a list shows 'Contoso App' with a checkmark next to it.

6. Select **Save** to finish assigning the role. You see your application in the list of users assigned to a role for that scope.

Your service principal is set up. You can start using it to run your scripts or apps. The next section shows how to get values that are needed when signing in programmatically.

14.1.2 Task 2: Get values for signing in

When programmatically signing in, you need to pass the tenant ID with your authentication request. You also need the ID for your application and an authentication key. To get those values, use the following steps:

1. Select **Azure Active Directory**.

2. From **App registrations** in Azure AD, select the **Contoso App** application.
3. Copy the **Directory (tenant) ID** and store it in your application code.

Display name : [Contoso App](#)
Application (client) ID : 46bb37d5-2c43-4de5-9dba-5150e92d3719
Directory (tenant) ID : 175a3ff3-9cd3-49a8-b60f-c27f49eeb562
Object ID : 16247541-cf97-4c61-81b9-8a8e4cbb2d13

4. Copy the **Application (client) ID** and store it in your application code.

Display name : [Contoso App](#)
Application (client) ID : 46bb37d5-2c43-4de5-9dba-5150e92d3719
Directory (tenant) ID : 175a3ff3-9cd3-49a8-b60f-c27f49eeb562
Object ID : 16247541-cf97-4c61-81b9-8a8e4cbb2d13

14.1.3 Task 3: Create a new application secret

You can choose a certificate or an application secret. In this task you will create an application secret.

1. Select **Certificates & secrets**.
2. Select **Client secrets -> New client secret**.



Contoso App - Certificates & secrets

<input type="text"/> Search (Ctrl+ /)	«
Overview	
Quickstart	
<hr/>	
Manage	
Branding	
Authentication	
Certificates & secrets	
API permissions	
Expose an API	
Owners	
Roles and administrators (Previous versions)	
Manifest	
<hr/>	
Support + Troubleshooting	
Troubleshooting	
New support request	

Credentials enable applications to identify themselves to the authentication service. For a higher level of assurance, we recommend using a certificate (instead of a client secret).

Certificates

Certificates can be used as secrets to prove the application's identity when requesting tokens.

Upload certificate

No certificates have been added for this application.

THUMBPRINT

START DATE

Client secrets

A secret string that the application uses to prove its identity when requesting a token.

New client secret

DESCRIPTION

EXPIRES

No client secrets have been created for this application.

- Provide a description of the secret, and a duration. When done, select **Add**.

After saving the client secret, the value of the client secret is displayed. Copy this value because you aren't able to retrieve the key later. You provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.

14.1.4 Task 4: Check Azure AD permissions

- Select **Azure Active Directory**.
- Select **User settings**.
- Check the **App registrations** setting. This value can only be set by an administrator. If set to **Yes**, any user in the Azure AD tenant can register an app.

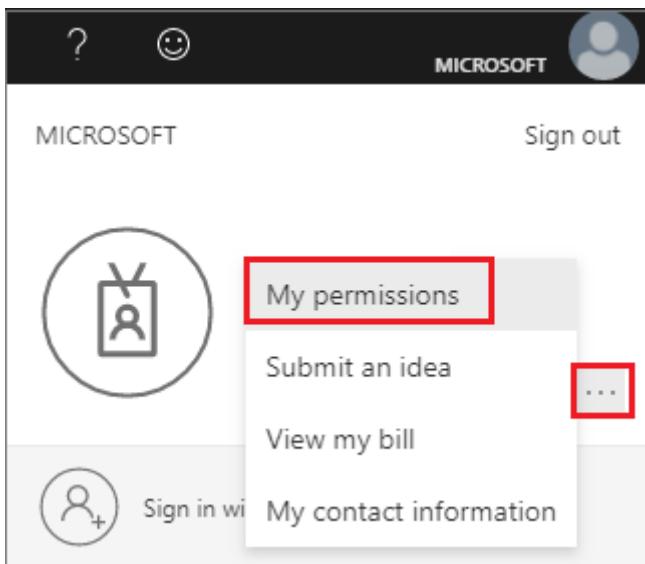
If the app registrations setting is set to **No**, only users with an administrator role may register these types of applications.

14.1.5 Task 5: Check Azure subscription permissions

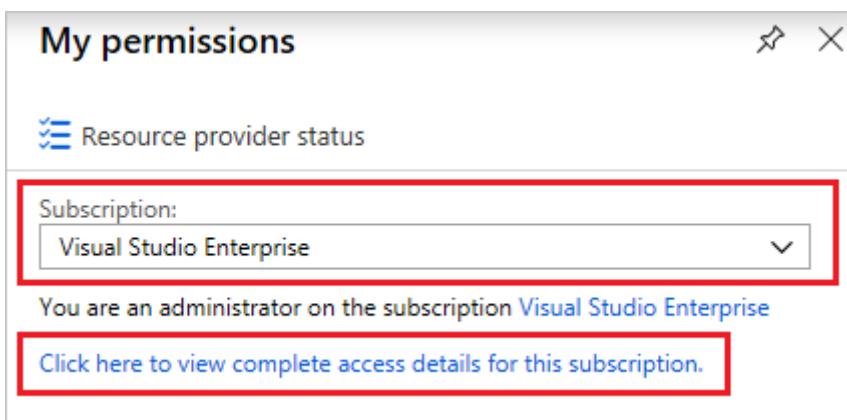
In your Azure subscription, your account must have `Microsoft.Authorization/*/Write` access to assign an AD app to a role. This action is granted through the Owner role or User Access Administrator.

To check your subscription permissions:

- Select your account in the upper right corner, and select ... -> **My permissions**.



- From the drop-down list, select the subscription you want to create the service principal in. Then, select [Click here to view complete access details for this subscription](#).



- Select **Role assignments** to view your assigned roles and determine if you have adequate permissions to assign an AD app to a role. If not, you would ask your subscription administrator to add you to User Access Administrator role. In the following image, the user is assigned to the Owner role, which means that user has adequate permissions.

Role assignments			
Name	Type	Role	Scope
<input type="text"/> Search by name or email	<input type="button"/> All	<input type="button"/> 2 selected	<input type="button"/> All scopes
2 items (1 Users, 1 Service Principals)			
NAME	TYPE	ROLE	
OWNER			
<input checked="" type="checkbox"/> Example User example@contoso.org	User	Owner, Service administrator	

Results: You have now completed this lab.

15 Module 1: Lab 6: Manage Identity and Access

Scenario

In this module, you'll learn about Role-Based Access Control as the foundation to organizing and managing an organization's administrative access based on the principle of least privilege. You will also review Azure Active Directory concepts, as well as gain insight into the threat landscape and security risks that are exposed to IT organizations through breach of privileged access. Lessons include:

- Role-Based Access Control
- Azure Active Directory (Refresher)
- Protecting Privileged Access in the Environment

16 Lab 5: Introduction to Identity Protection in Azure

16.1 Exercise 1: Role-Based Access Control

16.1.1 Task 1: Create a User

1. Sign in to the Azure portal <https://portal.azure.com/>
2. Select **Azure Active Directory** and on the overview blade note down your tenant domain.

The screenshot shows the Azure Active Directory - Overview page. At the top, there is a search bar labeled "Search (Ctrl+ /)" and buttons for "Switch directory" and "Delete directory". On the left, a sidebar has links for "Overview", "Getting started", "Manage", and "Users". The main area displays the tenant information: "Default Directory" (highlighted with a red box), "Azure AD Premium P2", and a "Sign-ins" section. The tenant domain "gdaztest14outlook.onmicrosoft.com" is also highlighted with a red box.

3. Select **Users**, and then select **New user**.
4. On the **User** page, fill out the blade with the following information:
 - **User name:** bill
 - **Name:** Bill Smith

New user

Default Directory

i Got a second? We would love your feedback on user creation →

Create user

Create a new user in your organization.
This user will have a user name like
alice@gdaztest14outlook.onmicrosoft.com.

Invite user

Invite a new guest user to collaborate with
your organization. The user will be emailed
an invitation they can accept in order to
begin collaborating.

[Help me decide](#)

Identity

User name ①

✓
@ gdaztest14outlook.onmicrosoft.com
Edit

The domain name I need isn't shown here

Name * ①

First name

Last name

5. Show the auto-generated password provided in the **Password** box. You'll need to give this password to the user for the initial sign-in process.

6. Select **Create**.

The user is created and added to your Azure AD tenant.

7. Launch **Azure Cloud Shell** by clicking on the PowerShell icon at the top of the Azure Portal and select PowerShell if prompted then run the following command to connect to AzureAD:

Connect-AzureAD

8. Enter the following commands to create a user in the PS cloud shell replacing `yourdomain` with your domain noted down earlier

```
$PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
```

```
$PasswordProfile.Password = "Pa55w.rd"
```

```
New-AzureADUser -DisplayName "Mark" -PasswordProfile $PasswordProfile -UserPrincipalName "Mark"
```

```
PS Azure:\> $PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile
```

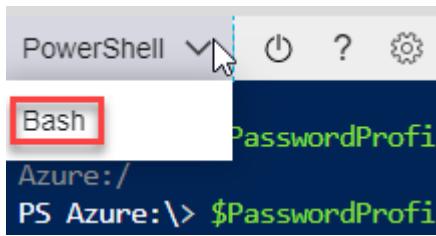
```
 Azure:/ PS Azure:\> New-AzureADUser -DisplayName "Mark" -PasswordProfile $PasswordProfile -UserPrincipalName "Mark@gaztest14outlook.onmicrosoft.com" -AccountEnabled $true -MailNickname "Mark"
```

ObjectID	DisplayName	UserPrincipalName	UserType
9637faa9-dc76-437b-b6de-59b749dd3c3c	Mark	Mark@gdaztest14outlook.onmicrosoft.com	Member

9. Run the following command to get a list of the users in Azure AD

Get-AzureADUser

10. Change the Azure cloud shell to azure CLI mode with Bash by using the drop down menu



- Enter the following command in **azure CLI** to create a user in Azure CLI replacing **yourdomain** with the domain you noted earlier.

```
az ad user create --display-name Tracy --password Pa55w.rd --user-principal-name Tracy@yourdomain.
```

You should now have 5 users in your Azure AD

16.1.2 Task 2: Create Groups In Portal, PowerShell, and CLI

- In the Azure Portal click **Azure Active Directory** on the **Azure AD blade** click **Groups** and select **New group**.

- Fill in the details with the following details:

- Group Type:** Security
- Group Name:** Senior Admins Group

- In the Members section, click No Members link and search for and select Bill then click **Select**.

- Click **Create**

- Launch the **Cloud Shell** in **Bash** mode by clicking the Cloud Shell icon at the top of the Azure Portal.

- In the **Cloud Shell** enter the following commands:

```
az login
az ad group create --display-name ServiceDesk --mail-nickname ServiceDesk
```

- Change the Cloud Shell to **PowerShell** and enter the following command:

```
New-AzureADGroup -DisplayName "Junior Admins" -MailEnabled $false -SecurityEnabled $true -MailNickname JAdm
```

- Exit the **Cloud Shell**.

- In the **Active Directory blade** click **Groups** and confirm you have **5** groups

Name	Object Id	Group Type
JA Junior Admins	3ce819ea-a8bc-47ad-9650-5b2be1...	Security
MP MFA Pilot	283c65eb-0705-42a9-a1ca-867191...	Security
SA Senior Admins Group	6bb50553-0f6d-490d-8b0e-80c554...	Security
SE ServiceDesk	131b57a3-f06a-47b5-8c11-fb28887...	Security

16.2 Exercise 2: Practice - RBAC

16.2.1 Task 1: Create a resource group

- In the navigation list, choose **Resource groups**.
- Choose **Add** to open the **Resource group** blade.
- For **Resource group name**, enter **myRBACrg**
- Select your subscription and the location of **East US**.
- Choose **Review + create** then **Create** to create the resource group.

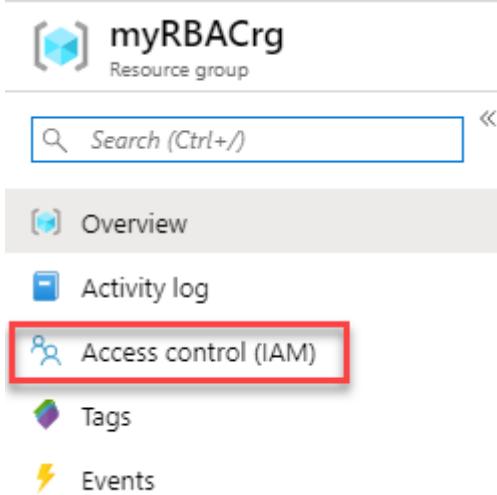
6. Choose **Refresh** to refresh the list of resource groups.

The new resource group appears in your resource groups list.

16.2.2 Task 2: Grant access

In RBAC, to grant access, you create a role assignment.

1. In the list of **Resource groups**, choose the new **myRBACrg** resource group.
2. Choose **Access control (IAM)** to see the current list of role assignments.



3. Choose **Add** to open the **Add role assignment** pane.

If you don't have permissions to assign roles, you won't see the **Add** option.

4. In the **Role** drop-down list, select **Virtual Machine Contributor**.
5. In the **Select** list, select **Bill Smith**.
6. Choose **Save** to create the role assignment.

After a few moments, the user is assigned the Virtual Machine Contributor role at the myRBACrg resource group scope.

16.2.3 Task 3: Remove access

In RBAC, to remove access, you remove a role assignment.

1. Click the Role Assignments tab.
2. In the list of role assignments, add a checkmark next to user with the Virtual Machine Contributor role.

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)

Name	Type	Role	Scope
<input type="checkbox"/> Contoso App	App	Contributor	Subscription (Inherited)
<input type="checkbox"/> MS-PIM	App	User Access Administrator	Subscription (Inherited)
<input type="checkbox"/> Bill Smith bill@gdaztest14outlook.onmicrosoft.com	User	Virtual Machine Contributor	This resource

3. Choose **Remove**.

4. In the remove role assignment message that appears, choose **Yes**.

16.3 Exercise 3: Role-based Access Control (RBAC) using PowerShell

In this exercise you use PowerShell to :

- Use the `Get-AzRoleAssignment` command to list the role assignments
- Use the `Remove-AzResourceGroup` command to remove access

16.3.1 Task 1: Grant access

To grant access for the user, you use the `New-AzRoleAssignment` command to assign a role. You must specify the security principal, role definition, and scope.

1. Launch the **Cloud Shell PowerShell**.

2. Get the ID of your subscription using the `Get-AzSubscription` command.

`Get-AzSubscription`

3. Save the subscription scope in a variable replacing the 000000's with your subscription ID.

`$subScope = "/subscriptions/00000000-0000-0000-0000-000000000000"`

4. Assign the Reader role to the user at the subscription scope by using the following command (replacing your domain with the tenant domain you noted earlier):

`New-AzRoleAssignment -SignInName bill@yourdomain.onmicrosoft.com -RoleDefinitionName "Reader" -Scope $subScope`

```
PS Azure:\> New-AzRoleAssignment -SignInName bill@gdaztest14outlook.onmicrosoft.com -RoleDefinitionName "Reader" -Scope $subScope
RoleAssignmentId : /subscriptions/0927670c-d3fc-435a-964a-b41d0e60ff04/providers/Microsoft.Authorization/roleAssignments/864f3642-9f8d-456c-893a-1e390ab88815
Scope           : /subscriptions/0927670c-d3fc-435a-964a-b41d0e60ff04
DisplayName     : Bill Smith
SignInName      : bill@gdaztest14outlook.onmicrosoft.com
RoleDefinitionName : Reader
RoleDefinitionId : acdd72a7-3385-48ef-bd42-f606fba81ae7
ObjectId        : 05e189ee-7850-45ea-b871-c50b83dbbabf
ObjectType      : User
CanDelegate     : False

Azure:/
```

5. Assign the Contributor role to the user at the resource group scope using the following command:

`New-AzRoleAssignment -SignInName bill@yourdomain.onmicrosoft.com -RoleDefinitionName "Contributor" -Scope $resourceScope`

16.3.2 Task 2: List access

1. To verify the access for the subscription, use the Get-AzRoleAssignment command to list the role assignments use the following command:

```
Get-AzRoleAssignment -SignInName bill@yourdomain.onmicrosoft.com -Scope $subScope
```

```
PS Azure:\> Get-AzRoleAssignment -SignInName bill@gdaztest14outlook.onmicrosoft.com -Scope $subScope
RoleAssignmentId : /subscriptions/0927670c-d3fc-435a-964a-b41d0e60ff04/providers/Microsoft.Authorization/roleAssignments/864f3642-9f8d-456c-893a-1e390ab88815
Scope            : /subscriptions/0927670c-d3fc-435a-964a-b41d0e60ff04
DisplayName      : Bill Smith
SignInName       : bill@gdaztest14outlook.onmicrosoft.com
RoleDefinitionName : Reader
RoleDefinitionId : acdd72a7-3385-48ef-bd42-f606fba81ae7
ObjectId         : 05e189ee-7850-45ea-b871-c50b83dbbabf
ObjectType       : User
CanDelegate     : False

Azure:/
```

In the output, you can see that the Reader role has been assigned to the RBAC Tutorial User at the subscription scope.

2. To verify the access for the resource group, use the Get-AzRoleAssignment command to list the role assignments using the following command:

```
Get-AzRoleAssignment -SignInName bill@yourdomain.onmicrosoft.com -ResourceGroupName "myRBACrg"
```

In the output, you can see that both the Contributor and Reader roles have been assigned to the RBAC Tutorial User. The Contributor role is at the myRBACrg resource group scope and the Reader role is inherited at the subscription scope.

16.3.3 Task 3: Remove access

To remove access for users, groups, and applications, use Remove-AzRoleAssignment to remove a role assignment.

1. Use the following command to remove the Contributor role assignment for the user at the resource group scope.

```
Remove-AzRoleAssignment -SignInName bill@yourdomain.onmicrosoft.com -RoleDefinitionName "Contributor"
```

2. Use the following command to remove the Reader role assignment for the user at the subscription scope.

```
Remove-AzRoleAssignment -SignInName bill@yourdomain.onmicrosoft.com -RoleDefinitionName "Reader" -
```

3. Remove the resource group by running the following command (When prompted to confirm press Y and press enter):

```
Remove-AzResourceGroup -Name "myRBACrg"
```

4. Close the Cloud Shell.

Results: You have now completed this lab.

17 Module 1: Lab 7: Azure Policy

In this lab, you will learn to use Azure Policy to do some of the more common tasks related to creating, assigning, and managing policies across your organization, such as:

- Assign a policy to enforce a condition for resources you create in the future

17.1 Exercise 1: Using Azure Policy

In this exercise, you will learn the basics of using Azure Policy. You will use a built-in policy to restrict which Azure regions can be used. You will then verify that the policy is working.

17.1.1 Task 1: Create an Azure Policy Assignment

In this task, you will first browse the built-in policy definitions using the Azure portal. You will then create a policy assignment using one of the built-in definitions to restrict which Azure Regions can be used. This policy will be scoped to the Test-RG resource group.

1. Log in to the Azure portal at <https://portal.azure.com> using your Azure subscription credentials.
2. Open the Cloud Shell in PowerShell Mode and run the following command to create a Resource Group in the UK South region.

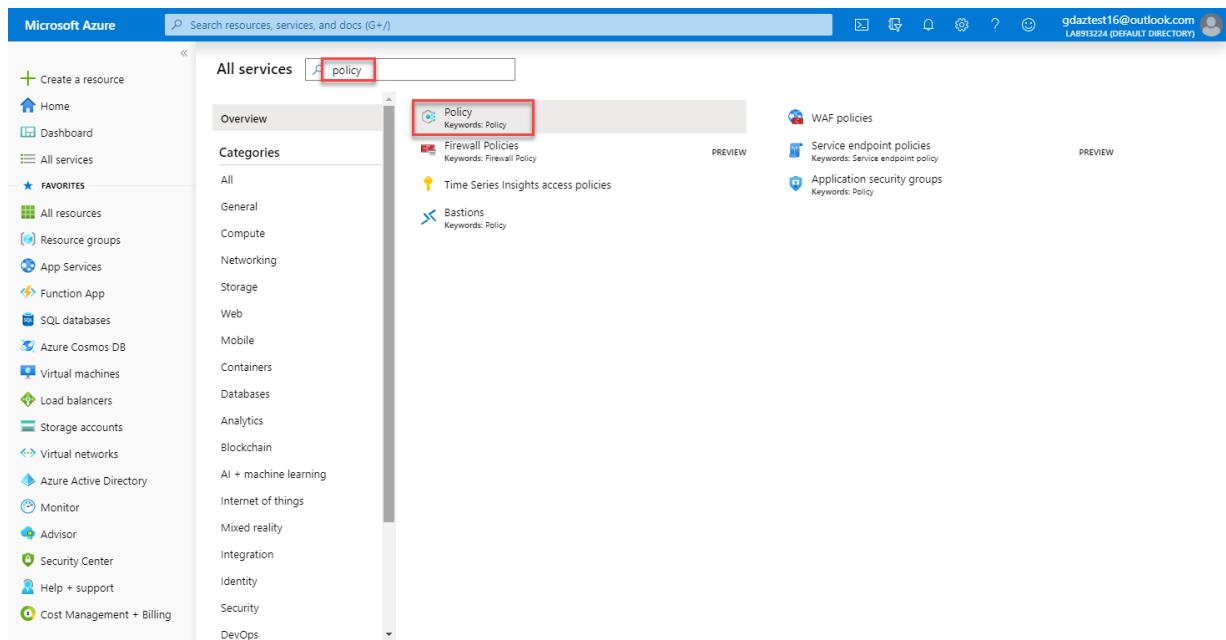
```
New-AzResourceGroup -Name myResourceGroup -Location UKSouth
```

```
PowerShell | ⚡ ? 🚦 { } 🔍
Azure:/ PS Azure:\> New-AzResourceGroup -Name myResourceGroup -Location UKSouth

ResourceGroupName : myResourceGroup
Location         : uksouth
ProvisioningState: Succeeded
Tags             :
ResourceId       : /subscriptions/6ed9778f-860f-4eac-9b7b-1046cac35221/resourceGroups/myResourceGroup

Azure:/ PS Azure:\>
```

3. In the Hub menu, click on **All services**. Enter **Policy** into the search box, and click on the **Policy** service.



4. The Azure Policy blade will open. Click on **Definitions** to show the list of available policy definitions.

The screenshot shows the Microsoft Azure Policy - Definitions page. On the left, there's a navigation sidebar with various service icons and a 'Definitions' item highlighted with a red box. The main area has a search bar at the top. Below it, there are filters for Scope (set to 'Azure Pass - Spon'), Definition type (set to 'All definition types'), Type (set to 'All types'), and Category (set to 'All categories'). A 'Search' input field contains 'Filter by name or id...'. The main table lists numerous policy definitions, such as 'Audit Windows VMs in which the Ad...', 'Audit CIS Microsoft Azure F...', and 'Audit Windows VMs that are not set t...'. Each row includes columns for Name, Definition location, Policies, Type, and Category.

5. Use the filters and search to find the policy definition called **Allowed locations**.

This screenshot is similar to the previous one but with a search term in the search bar. The search bar contains the text 'allowed locations', which is highlighted with a red box. The rest of the interface and data table are identical to the first screenshot.

Note: This policy only restricts resource locations, not resource group locations. There is a separate policy for 'Allowed locations for resource groups'.

6. Click on the **Allowed locations** policy definition to open the definition details view.

Note: Policy definitions take an array of locations as parameters. A policy rule is an 'if-then' statement. The 'if' clause checks to see if the resource location is included in the parameterized list, and if not the 'then' clause denies the resource creation.

The screenshot shows the Microsoft Azure Policy - Definitions page. The left sidebar includes links for creating a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and Cost Management + Billing. The 'Definitions' link under 'Authoring' is currently selected. The main content area displays a table of policy definitions. A red box highlights the first row, which contains the 'Allowed locations' policy definition. The table has columns for Name, Definition location, Policies, Type, Definition location, Category, and three dots. The 'Allowed locations' row shows 'Built-in' for Definition location, 'Policy' for Type, 'General' for Category, and three dots for more options.

Name	Definition location	Policies	Type	Definition location	Category	...
Allowed locations	Built-in		Policy	General	...	
Allowed locations for resource groups	Built-in		Policy	General	...	

7. Click Assign.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar with the placeholder "Search resources, services, and docs (G+)", and various account and service icons. On the left, a sidebar lists "Create a resource", "Home", "Dashboard", "All services", "FAVORITES" (with "Allowed locations" selected), "All resources", "Resource groups", "App Services", "Function App", "SQL databases", "Azure Cosmos DB", "Virtual machines", "Load balancers", "Storage accounts", "Virtual networks", "Azure Active Directory", "Monitor", "Advisor", "Security Center", "Help + support", and "Cost Management + Billing". The main content area is titled "Allowed locations" under "Policy definition". It shows the policy definition with fields: Name (Allowed locations), Description (This policy enables you to restrict the locations your organization can specify.), Available Effects (Deny), Category (General), Definition location (--), Definition ID (/providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd...), Type (Built-in), and Mode (Indexed). Below the definition details, there are tabs for "Definition", "Assignments (0)", and "Parameters". The "Definition" tab displays the JSON code for the policy:

```
1 {
2     "properties": {
3         "displayName": "Allowed locations",
4         "policyType": "Builtin",
5         "mode": "Indexed",
6         "description": "This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your location compliance requirements.",
7         "metadata": {
8             "category": "General"
9         },
10        "parameters": {
11            "listOfAllowedLocations": {
12                "type": "Array",
13                "metadata": {
14                    "description": "The list of locations that can be specified when deploying resources.",
15                    "strongType": "location",
16                    "displayName": "Allowed locations"
17                }
18            }
19        },
20        "policyRule": {
21            "if": {
22                "then": {
23                    "actions": [
24                        {
25                            "type": "Deny"
26                        }
27                    ]
28                }
29            }
30        }
31    }
32 }
```

- Click the Elipsis (...) button and assign the policy to your Subscription and the **myResourceGroup** resource group then click **Select**.

9. Complete the remainder of the policy assignment **Basics** tab with the following settings:
 - Exclusions: **Leave blank**
 - Assignment name: **Allow UK South for myResourceGroup**
 - Description: **Allow resources to be created in UK South Only for myResourceGroup**
 - Policy enforcement: **Enabled**
 - Assigned by: **Your name**
10. Click **Next** to proceed to the **Parameters** tab. In this tab you can provide values for parameters that are specified in the policy definition. Select **UK South** as the allowed location.

11. Click **Review + create**, followed by **Create** to create the policy assignment.
12. You will see a notification that the assignment was successful, and that the assignment will take around 30 minutes to complete.

Note: The reason the Azure policy assignment takes up to 30 minutes to be assigned is that it has to replicate globally although in the real world it generally only takes 2 - 3 minutes to be implemented. If the next task fails, simply wait a few minutes and attempt the steps again.

17.1.2 Task 2: Verify the Azure Policy Assignment

In this task, you will verify that the policy assignment created in the previous task is effective by attempting to create a virtual network in both a permitted region and a different region.

1. Click **Virtual Networks** on the Hub menu.
2. On the **Virtual Networks** blade, click **+ Add**
3. First, you will try to create a virtual network in East US. Since this is not an allowed location, the request should be blocked. Complete in the **Create virtual network** blade as follows:
 - Name: **myVnet**
 - Address space: **10.0.0.0/16**
 - Resource group: **myResourceGroup**
 - Location: **East US**
 - Address range: **10.0.0.0/24**

Leave the other settings at their default values and click **Review + create**.

Create virtual network

Name *****
 

Address space ***** 
 
10.0.0.0 - 10.0.255.255 (65536 addresses)

Add an IPv6 address space 

Subscription *****
 

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

Location *****
 

Subnet

Name *****

Address range ***** 
 
10.0.0.0 - 10.0.0.255 (256 addresses)

DDoS protection 
 Basic Standard

[Automation options](#)

4. Once you click create you will see a validation error. Click the error to open the error details.

Create virtual network

Name *

myVnet 

Address space * 

10.0.0.0/16 

10.0.0.0 - 10.0.255.255 (65536 addresses)

Add an IPv6 address space 

Subscription *

Azure Pass - Sponsorship 

Resource group *

myResourceGroup 

[Create new](#)

Location *

(US) East US 

Subnet

Name *

default 

Address range * 

10.0.0.0/24 



There were validation errors. Click here to view details.

[Create](#)

[Automation options](#)

5. You will see the error states you are disallowed by policy.

Errors

Summary [Raw Error](#)

ERROR DETAILS



Resource 'myVnet' was disallowed by policy. (Code: RequestDisallowedByPolicy)

Policy: [Allow UK South for myResourceGroup](#)

WAS THIS HELPFUL?

[Troubleshooting Options](#)

[New Support Request](#)

6. Return back to the Basics tab and change the resource location to **UK South** as this is the location permitted by the policy. Click **Review + create** again and verify that the operation is successful.

Summary

In this exercise, you learned to use Azure policy by browsing the built-in policy definitions and creating a policy assignment.

Results: You have now completed this lab.

18 Module 1: Lab 8: Protecting Azure Resources with Resource Manager Locks

Scenario

Resource Manager Locks provide a way for administrators to lock down Azure resources to prevent deletion or changing of a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and when applied will place the restriction on the resource for all users. These are very useful when you have an important resource in your subscription which users should not be able to delete or change and can help prevent accidental and malicious changes or deletion.

There are two types of resource locks that can be applied:

- **CanNotDelete** - This prevents anyone from deleting a resource whilst the lock is in place, however they may make changes to it.
- **ReadOnly** - As the name suggests, it makes the resource read only, so no changes can be made and it cannot be deleted. Resource locks can be applied to subscriptions, resource groups or individual resources as required. When you lock Subscription, all resources in that subscription (including ones added later) inherit the same lock. Once applied, these locks impact all users regardless of their roles. If it becomes necessary to delete or change a resource with a lock in place, then the lock will need to be removed before this can occur.

Permissions

Permission to set and remove locks requires access to one of the following RBAC permissions:

- `Microsoft.Authorization/*`
- `Microsoft.Authorization/locks/*`

By default, these actions are only available on the Owner and User Access Administrator built in RBAC Roles, however you can add them to custom roles as required. As mentioned, users with these roles are still subject

to the locks, but obviously they can remove them if required. Creation and deletion of a lock is tracked in the Azure Activity log.

19 Lab 7: Protecting Azure Resources with Resource Manager Locks

Locks can be created both at the time of creation of a resource inside an ARM template, or later using the portal or PowerShell.

19.1 Exercise 1: Creating Locks

The best way to ensure that locks are in place and protecting your resources is to create them at run time and configure them in your ARM templates. Locks are top level ARM resources; they do not sit underneath the resource being locked. They refer to the resource being locked, so this must exist first.

19.1.1 Task 1: Adding a Lock (Portal)

1. Open the Cloud Shell (PowerShell) and run the following commands to create a Resource Group and Storage Account. (*Change XXXXXX in the command to something unique*)

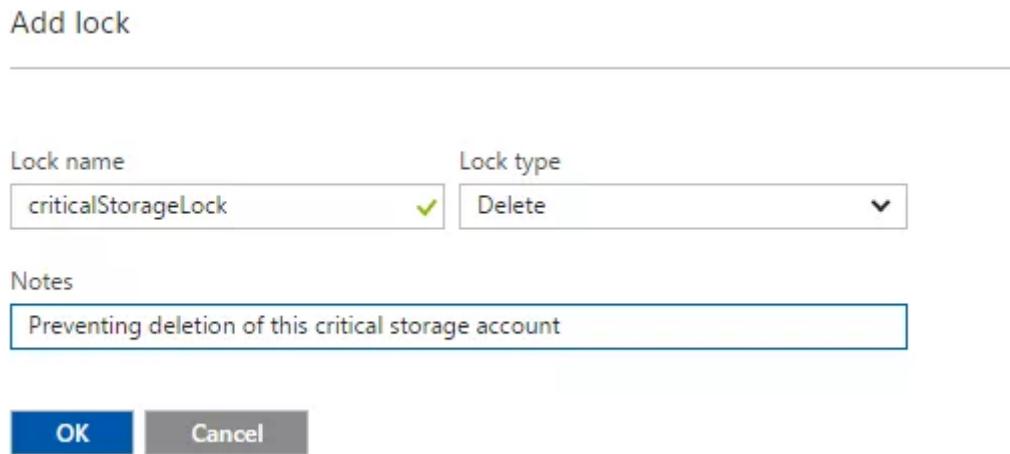
```
New-AzResourceGroup -Name LockRG -Location EastUS
```

```
New-AzStorageAccount -ResourceGroupName LockRG -Name XXXXXX -Location EastUS -SkuName Standard_LRS
```

2. Locate the Storage Account and select it. In the main blade, click the "Locks" icon



3. Click **Add**
4. Give the lock a name and description, then select the type, deletion or read only.



5. Click **OK** to save the lock. The resource is now protected.
6. Remove the lock by simply going back into **Locks**, select the lock and then go to delete.

19.1.2 Task 2: Adding a Lock (PowerShell)

1. Open the Cloud Shell (PowerShell) and run the following commands to create a Lock on the Storage Account. (*Change XXXXXX in the command to the name of your Storage Account*)

```
Connect-AzureAD
```

```
New-AzResourceLock -LockLevel CanNotDelete -LockName criticalStorageLock -ResourceName XXXXXX -Res  
2. To remove a lock use the following command. (Change XXXXXX in the command to the name of your  
Storage Account)  
Remove-AzResourceLock -LockName criticalStorageLock -ResourceName XXXXX -ResourceGroupName LockRG  
If prompted to confirm, enter Y and press Enter
```

By using Resource Logs you can put in place an extra line of defense against accidental or malicious changing and/or deletion of your most important resources. It's not perfect, as your administrators can still remove these locks, but doing so requires a conscious effort, as the only purpose for removing a lock is to circumvent it. As these locks sit outside of RBAC you can apply them and be sure that they are impacting all your users, regardless of what roles or custom permissions you may have granted them.

Results: You have now completed this lab.

20 Module 1: Lab 9: Transferring Subscriptions

Scenario

Occasionally, a need arises for transferring a subscription from an owner to an Azure AD tenant. In order to transfer a subscription from an Azure AD owner to another subscription, you need access to another subscription. If you do not have access to multiple subscriptions at this time, just review the process outlined below.

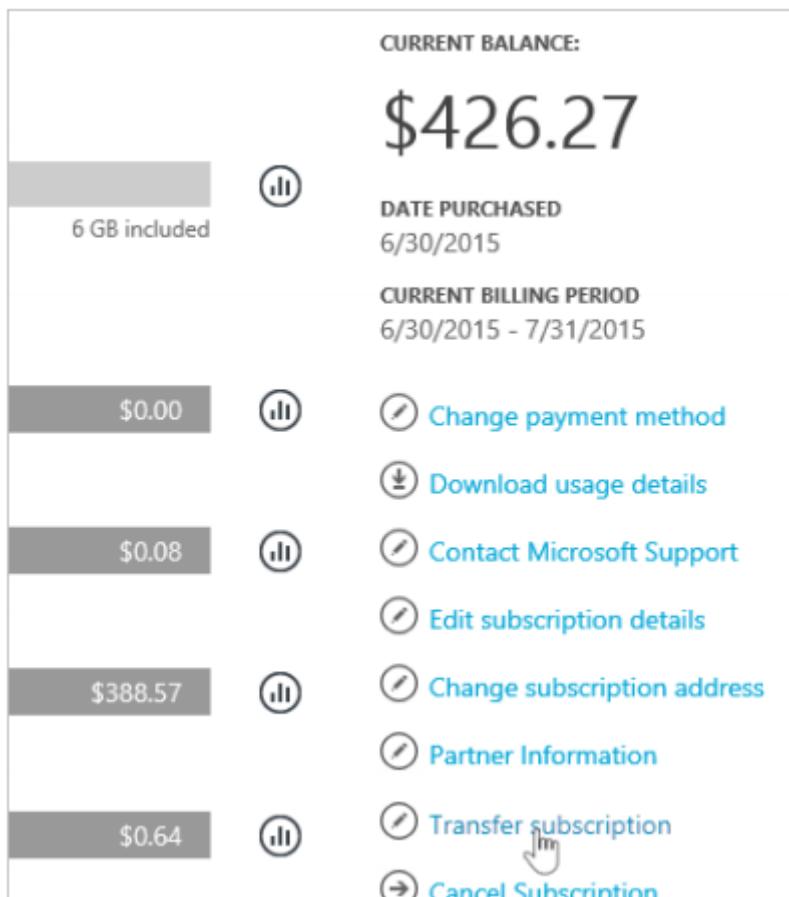
20.1 Exercise 1: Transfer Azure subscriptions between Azure AD tenants

20.1.1 Task 1: To transfer the ownership of an Azure subscription

1. Sign in at the Azure Portal as the account admin.
2. Navigate to **Cost Management + Billing > Subscriptions** and click **Manage**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various navigation options like 'Create a resource', 'Home', 'Dashboard', etc. A section titled 'FAVORITES' contains links to 'All services', 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', 'Security Center', and 'Cost Management + Billing'. The 'Cost Management + Billing' link is highlighted with a red box. At the bottom of the sidebar, there's a 'Help + support' link. The main content area is titled 'Cost Management + Billing - Subscriptions' and shows a 'Default Directory'. It includes a search bar, a 'New subscription' button, and a 'Manage' button (which is also highlighted with a red box). Below these are sections for 'Overview', 'Cost Management', 'Diagnose and solve problems', 'Billing' (with a 'Subscriptions' link highlighted with a red box), 'Invoices', 'Properties', and 'Payment methods'. Under 'Support + troubleshooting', there's a 'New support request' link.

3. Select your subscription.
 4. Verify that your subscription is eligible for self-serve transfer by checking the Offer and Offer ID against the supported offers list.
- Note:** At the time of writing, Azure Pass - Sponsorship subscriptions are not eligible for transfer. Follow this guide through for reference.
5. Select **Transfer subscription**.



6. Specify the recipient.

Note: If you transfer a subscription to a new Azure AD tenant, all role assignments in RBAC will be permanently deleted from the source tenant and not migrated to the target tenant.

TRANSFER SUBSCRIPTION

Specify New Owner

RBAC assignments are removed if the subscription moves to a new Azure AD tenant. Only the new owner will have access. Transfer will expose your email address, usage history, and billing history to the new owner. [Read this article](#) before proceeding

TRANSFER TO

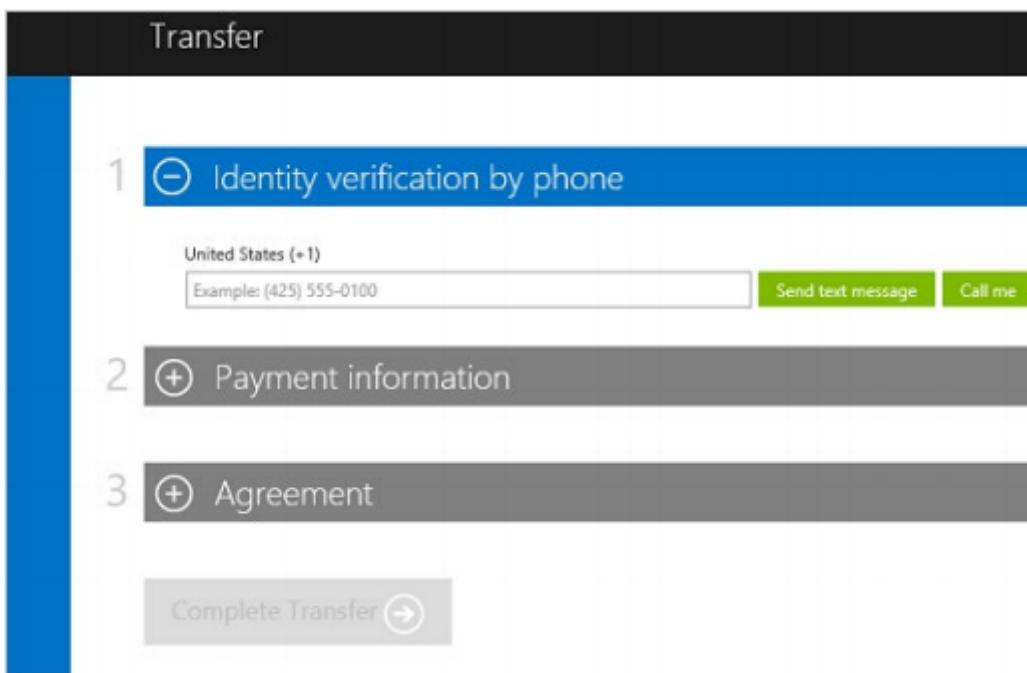
Retain this subscription within my Azure AD. [Learn More](#)

Enter an existing Microsoft account or work account

Re-enter the above Microsoft account or work account

Finish

7. The recipient automatically gets an email with an acceptance link.
8. The recipient selects the link and follows the instructions, including entering their payment information



9. Azure completes the subscription transfer.

At this point, billing ownership of the Azure subscription would be transferred to the new subscription.

Results: You have now completed this module.

21 Module 2: Lab 2 - Function Apps

Azure Function Apps uses the Azure App Service infrastructure. This topic shows you how to create a function app in the Azure portal. A function app is the container that hosts the execution of individual functions. When you create a function app in the App Service hosting plan, your function app can use all the features of App Service.

21.1 Exercise 1: Create a Function and Trigger

21.1.1 Task 1: Lab Setup

1. In your browser, navigate to the following URL to open the ARM template:

<https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2Fraw.githubusercontent.com%2Faz76%2FCloud-Native-Azure-Development%2FModule-2%2FFunction-App%2Ffunction-app-template.json>

2. Click **Create new** under the Resource Group section.
3. Enter **myResourceGroup** as the name and click **OK**.
4. Select the check box at the bottom of the blade to agree to the terms.
5. Select **Purchase**

21.1.2 Task 2: Add a HTTP trigger to your function app

1. Select **Resource Groups**
2. Select the resource group you created in the lab setup
3. Select the function app service that has been created in the resource group

Note: There are no functions currently assigned to the function app

4. Select **Click to go back to the classic Function App management experience.**

5. Click **Functions**.
6. Click **+ New Function**.

7. In the top right click the slide button for **Experimental Language support**,

Note: New languages have now been added to the triggers

8. Select **HTTP trigger**.
9. Change the language to **PowerShell**.

10. Leave the name as the default,

11. Make sure **Authorization Level** is set to **Function**,

12. Click **Create**.

You have now created template PS1 HTTP trigger. If the template code does not appear, refresh the page

21.1.3 Task 3: Test a REST call to the HTTP trigger

1. Note the name of the function app (**next to the function app icon**).
2. Under the **HTTP trigger** function click **Manage**.
3. Under function keys select **copy** under actions on the default function key and paste this in a notepad file
4. Navigate to the following URL and copy the PowerShell code


```
https://raw.githubusercontent.com/godeploy/AZ500/master/AZ500%20Mod2%20Lab%202/RESTgetHTTPtrigger.ps1
```
5. Open a **PowerShell ISE** window and and paste the PowerShell code from the previous **URL**. (*If the Script pane is not open, select View>Show Script Pane.*)
6. Populate the variable `$functionappname = ""` with the name of your function app
7. Populate the variable `$functionkey = ""` with the long function key copied from the portal in the earlier step

8. Run the powershell script (F5)
9. In the results in the **ISE** you should see the following output

```
This is result of a normal GET operation calling your HTTP trigger  
Hello
```

```
This is result of a normal GET operation calling your HTTP trigger with an extra parameter passed  
Hello World!
```

```
This is result of a normal PUT operation calling your HTTP trigger that feeds a hash table convert  
Hello Max Power
```

Results: You have successfully built a HTTP trigger function app and communicated to it using REST based commands.

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**

Congratulations: You have now completed this lab.

22 Module 2: Lab 3 - Create a Kubernetes Cluster

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage clusters. In this quickstart, you deploy an AKS cluster using the Azure CLI. A multi-container application that includes a web front end and a Redis instance is run in the cluster. You then see how to monitor the health of the cluster and pods that run your application.

22.1 Exercise 1: Create an AKS environment

22.1.1 Task 1: Prepare the environment and Create a Resource Group.

1. Open a browser and navigate to the **Azure Portal** <https://portal.azure.com>
2. Click **Cloudshell** icon.



3. Select **Azure CLI BASH** if required and create a storage account.
4. Run the following command in the **Cloud Shell** to create a new **Resource Group**.

```
az group create --name myAKSResourceGroup --location eastus
```

Note: If you receive an error regarding the `Microsoft.Network` resource provider not being registered then run the following command and rerun the command in Step 4. Otherwise continue to Task 2.

```
az provider register --namespace 'Microsoft.Network'
```

22.1.2 Task 2: Create the AKS Cluster in CLI

1. Run the following command in the **CloudShell**.

```
az aks create --resource-group myAKSResourceGroup --name myAKSCluster --node-count 1 --enable-add
```

2. After a few minutes, the command completes and returns **JSON-formatted** information about the cluster.

22.1.3 Task 3: Connect to the cluster

To manage a Kubernetes cluster, you use `kubectl`, the Kubernetes command-line client. If you use Azure Cloud Shell, `kubectl` is already installed.

1. Open **Azure Cloud Shell** in Bash mode.
2. To configure `kubectl` to connect to your **Kubernetes cluster**, use the `az-aks-get-credentials` command. This command downloads credentials and configures the **Kubernetes CLI** to use them.

- ```
az aks get-credentials --resource-group myAKSResourceGroup --name myAKSCluster
```
3. To verify the connection to your cluster, use the kubectl-get command to return a list of the cluster nodes.

```
kubectl get nodes
```

  4. The following example output shows the single node created in the previous steps. Make sure that the status of the node is *Ready*:

| NAME                     | STATUS | ROLES | AGE   | VERSION |
|--------------------------|--------|-------|-------|---------|
| aks-nodepool1-31718369-0 | Ready  | agent | 6m44s | v1.9.11 |

#### 22.1.4 Task 4: Run the application

A Kubernetes manifest file defines a desired state for the cluster, such as what container images to run. In this lab, a manifest is used to create all objects needed to run the Azure Vote application. This manifest includes two kubernetes-deployment - one for the sample Azure Vote Python applications, and the other for a Redis instance. Two kubernetes-service are also created - an internal service for the Redis instance, and an external service to access the Azure Vote application from the internet. The manifest file has been created and saved to the Godeploy Github page for this lab. The file is azure-vote.yaml and can be found at [https://raw.githubusercontent.com/MicrosoftLearning/AZ-500-Azure-Security/master/Allfiles/Labs/Mod2\\_Lab1/azure-vote.yaml](https://raw.githubusercontent.com/MicrosoftLearning/AZ-500-Azure-Security/master/Allfiles/Labs/Mod2_Lab1/azure-vote.yaml)

1. Run the following command in the cloud shell, this will directly pull the yaml file needed from GitHub to deploy the AKS application

```
kubectl apply -f https://raw.githubusercontent.com/MicrosoftLearning/AZ-500-Azure-Security/master/Allfiles/Labs/Mod2_Lab1/azure-vote.yaml
```

2. The following example output shows the **Deployments and Services** created successfully:

```
deployment "azure-vote-back" created
service "azure-vote-back" created
deployment "azure-vote-front" created
service "azure-vote-front" created
```

**Note:** When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete.

#### 22.1.5 Task 5: Test the application

1. To monitor progress, use the kubectl-get command with the --watch argument.

```
kubectl get service azure-vote-front --watch
```

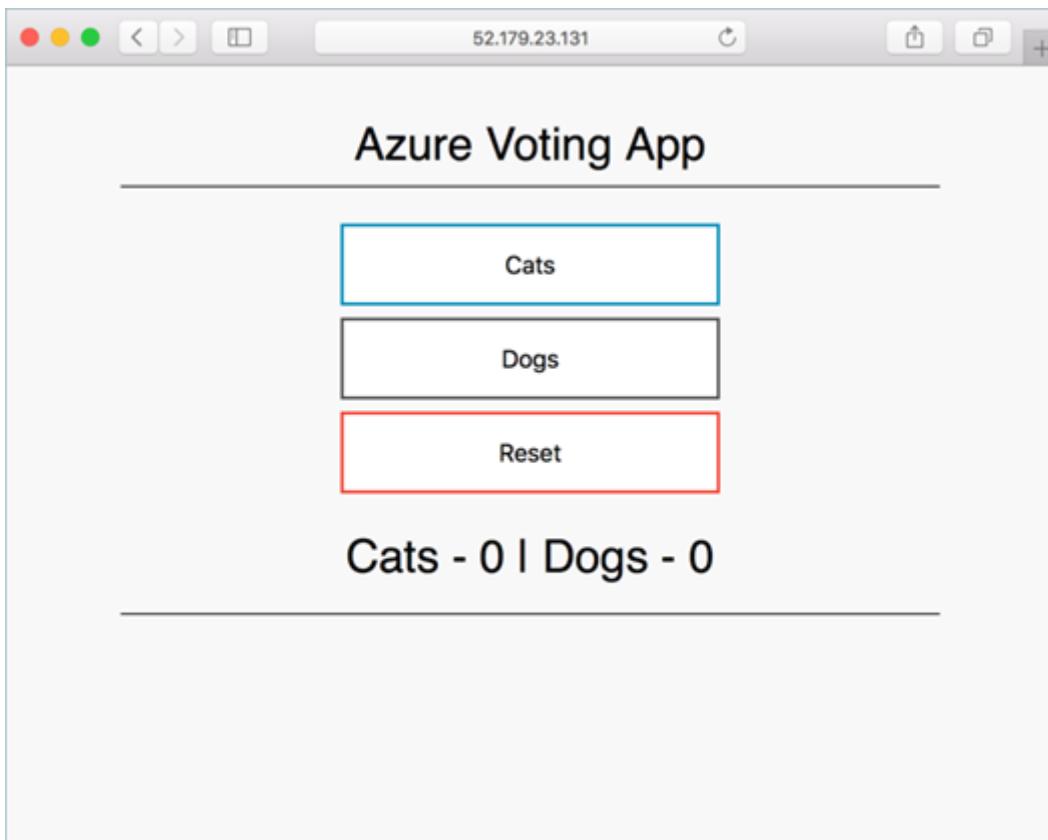
2. Initially the *EXTERNAL-IP* for the *azure-vote-front* service is shown as *pending*.

| NAME             | TYPE         | CLUSTER-IP | EXTERNAL-IP | PORT(S)      | AGE |
|------------------|--------------|------------|-------------|--------------|-----|
| azure-vote-front | LoadBalancer | 10.0.37.27 | <pending>   | 80:30572/TCP | 6s  |

3. When the *EXTERNAL-IP* address changes from *pending* to an actual public IP address, use **CTRL-C** to stop the kubectl watch process. The following example output shows a valid public IP address assigned to the service:

```
azure-vote-front LoadBalancer 10.0.37.27 52.179.23.131 80:30572/ TCP 2m
```

4. To see the Azure Vote app in action, open a web browser to the external IP address of your service as shown in the result of the previous command.



#### 22.1.6 Task 6: Monitor health and logs

When the AKS cluster was created, Azure Monitor for containers was enabled to capture health metrics for both the cluster nodes and pods. These health metrics are available in the Azure portal.

To see current status, uptime, and resource usage for the Azure Vote pods, complete the following steps:

1. Open a web browser to the Azure portal.
2. Select your resource group, such as *myAKSResourceGroup*, then select your AKS cluster, such as *myAKSCluster*.
3. Under **Monitoring** on the left-hand side, choose **Insights**
4. Across the top, choose to **+ Add Filter**
5. Select *Namespace* as the property, then choose **<All but kube-system>**
6. Choose to view the **Containers**.

The *azure-vote-back* and *azure-vote-front* containers are displayed

7. Click the view live data button then switch to the running application (Cats/Dogs) to click the vote buttons then switch back to view the live data under the Logs window.

#### 22.1.7 Task 7: Delete the cluster

When the cluster is no longer needed, use the **az group delete** command to remove the resource group, container service, and all related resources.

1. Run the following command in the **Cloud Shell** in Bash mode to delete the Resource Group.

```
az group delete --name myAKSResourceGroup --yes --no-wait
```

**Note:** It may take some time to delete the Resource Group. The **--no-wait** option runs the command in the background.

**Results:** You have now completed this lab.

## 23 Module 2: Lab 4 - Create a VNet

### Scenario

In this module, you'll will be introduced to Azure virtual networks. What are virtual networks and how are they organized? How do you create and configure virtual networks with templates, PowerShell, CLI, or the Azure portal? What is the difference between public, private, static, and dynamic IP addressing? How are system routes, routing tables, and routing algorithms used? Lessons include:

- Introducing Virtual Networks
- Creating Azure Virtual Networks
- Review of IP Addressing

### 23.1 Exercise 1: Create a virtual network using the Azure portal

#### Scenario

A virtual network is the fundamental building block for your private network in Azure. It enables Azure resources, like virtual machines (VMs), to securely communicate with each other and with the internet. In this lab, you will learn how to create a virtual network using the Azure portal. Then, you can deploy two VMs into the virtual network, securely communicate between the two VMs, and connect to the VMs from the internet.

#### 23.1.1 Task 1: Create a virtual network

1. On the upper-left side of the screen, select **Create a resource > Networking > Virtual network**.
2. In **Create virtual network**, enter or select this information:

| Setting        | Value                                                                             |
|----------------|-----------------------------------------------------------------------------------|
| Subscription   | Select your subscription.                                                         |
| Resource group | Select <b>Create new</b> , enter <i>myResourceGroup</i> , then select <b>OK</b> . |
| Name           | Enter <i>myVirtualNetwork</i> .                                                   |
| Location       | Select <b>East US</b> .                                                           |

Select the IP Addresses tab and enter the following values:

| Setting                | Value                          |
|------------------------|--------------------------------|
| Address space          | Enter <i>10.1.0.0/16</i> .     |
| Subnet - Name          | Enter <i>myVirtualSubnet</i> . |
| Subnet - Address range | Enter <i>10.1.0.0/24</i> .     |

3. Leave the rest as default and select **Review + create**, then click **Create**.

#### 23.1.2 Task 2: Create virtual machines

Create two VMs in the virtual network:

1. On the upper-left side of the screen, select **Create a resource > Compute > Virtual machine**.
2. In **Create a virtual machine - Basics**, enter or select this information:

| Setting                 | Value                                                                     |
|-------------------------|---------------------------------------------------------------------------|
| <b>PROJECT DETAILS</b>  |                                                                           |
| Subscription            | Select your subscription.                                                 |
| Resource group          | Select <b>myResourceGroup</b> . You created this in the previous section. |
| <b>INSTANCE DETAILS</b> |                                                                           |
| Virtual machine name    | Enter <i>myVm1</i> .                                                      |
| Region                  | Select <b>East US</b> .                                                   |
| Availability options    | Leave the default <b>No infrastructure redundancy required</b> .          |
| Image                   | Select <b>Windows Server 2019 Datacenter</b> .                            |
| Size                    | Select <b>Standard DS1 v2</b> .                                           |

| Setting                         | Value                                              |
|---------------------------------|----------------------------------------------------|
| <b>ADMINISTRATOR ACCOUNT</b>    |                                                    |
| Username                        | Enter a username of your choosing.<br>Pa55w.rd1234 |
| Password                        | Reenter password.                                  |
| Confirm Password                |                                                    |
| <b>INBOUND PORT RULES</b>       |                                                    |
| Public inbound ports            | Select <b>Allow selected ports</b> .               |
| Select inbound ports            | Select <b>HTTP</b> and <b>RDP</b> .                |
| <b>SAVE MONEY</b>               |                                                    |
| Already have a Windows license? | Leave the default <b>No</b> .                      |

3. Select **Next : Disks**.
4. In **Create a virtual machine - Disks**, leave the defaults and select **Next : Networking**.
5. In **Create a virtual machine - Networking**, select this information:

| Setting         | Value                                                    |
|-----------------|----------------------------------------------------------|
| Virtual network | Leave the default <b>myVirtualNetwork</b> .              |
| Subnet          | Leave the default <b>myVirtualSubnet (10.1.0.0/24)</b> . |
| Public IP       | Leave the default ( <b>new</b> ) <b>myVm1-ip</b> .       |

6. Select **Next : Management**.
7. In **Create a virtual machine - Management**, for **Diagnostics storage account**, select **Create New**.
8. In **Create storage account**, enter or select this information:

| Setting      | Value                                                                          |
|--------------|--------------------------------------------------------------------------------|
| Name         | Enter <i>myvmstorageaccount</i> . If this name is taken, create a unique name. |
| Account kind | Leave the default <b>Storage (general purpose v1)</b> .                        |
| Performance  | Leave the default <b>Standard</b> .                                            |
| Replication  | Leave the default <b>Locally-redundant storage (LRS)</b> .                     |

9. Select **OK**
10. Select **Review + create**. You're taken to the **Review + create** page where Azure validates your configuration.
11. When you see the **Validation passed** message, select **Create**.

### 23.1.3 Task 3: Create the second VM

1. Complete steps 1 and 9 from above.
- Note:** In step 2, for the **Virtual machine name**, enter *myVm2*. In step 7, for **Diagnosis storage account**, make sure you select **myvmstorageaccount**.
2. Select **Review + create**. You're taken to the **Review + create** page and Azure validates your configuration.
  3. When you see the **Validation passed** message, select **Create**.

### 23.1.4 Task 4: Connect to a VM from the internet

After you've created *myVm1*, connect to the internet.

1. In the portal's search bar, enter *myVm1*.
2. Select the **Connect** button.

3. Select **RDP**, then **Download RDP File**. Azure creates a Remote Desktop Protocol (.rdp) file and downloads it to your computer.
4. Open the downloaded .rdp file.
  1. If prompted, select **Connect**.
  2. Enter the username and password you specified when creating the VM.

**Note:** You may need to select **More choices > Use a different account**, to specify the credentials you entered when you created the VM.
5. Select **OK**.
6. You may receive a certificate warning during the sign in process. If you receive a certificate warning, select **Yes or Continue**.

### 23.1.5 Task 5: Communicate between VMs

1. In the Remote Desktop of *myVm1*, open PowerShell.
2. Enter `ping myVm2`

You'll receive a message similar to this:

```
Pinging myVm2.0v0zze1s0uiedpvtxz5z0r0cxg.bx.internal.clouda
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 10.1.0.5:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The `ping` fails because `ping` uses the Internet Control Message Protocol (ICMP). By default, ICMP isn't allowed through the Windows firewall.

3. To allow *myVm2* to ping *myVm1* in a later step, enter this command:

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

This command allows ICMP inbound through the Windows firewall:

4. Close the remote desktop connection to *myVm1*.
5. Complete the steps in **Connect to a VM from the internet** task again, but connect to *myVm2*.
6. From a command prompt, enter `ping myvm1`.

You'll get back something like this message:

```
Pinging myVm1.0v0zze1s0uiedpvtxz5z0r0cxg.bx.internal.cloudapp.net [10.1.0.4] with 32 bytes of data
Reply from 10.1.0.4: bytes=32 time=1ms TTL=128
Reply from 10.1.0.4: bytes=32 time<1ms TTL=128
Reply from 10.1.0.4: bytes=32 time<1ms TTL=128
Reply from 10.1.0.4: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.1.0.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

You receive replies from *myVm1* because you allowed ICMP through the Windows firewall on the *myVm1* VM in step 3.

7. Close the remote desktop connection to *myVm2*.

---

**WARNING:** Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

---

**Results:** You have now completed this lab.

## 24 Module 2: Lab 5 - NSGs

You can filter network traffic inbound to and outbound from a virtual network subnet with a network security group. Network security groups contain security rules that filter network traffic by IP address, port, and protocol. Security rules are applied to resources deployed in a subnet. In this tutorial, you learn how to:

- Create a network security group and security rules
- Create a virtual network and associate a network security group to a subnet
- Deploy virtual machines (VM) into a subnet
- Test traffic filters

### 24.1 Exercise 1: Filter network traffic with a network security group using the Azure portal

#### 24.1.1 Task 1: Create a virtual network

1. Select + **Create a resource** on the upper left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **Review + create**, then click **Create**:

| Setting        | Value                                                       |
|----------------|-------------------------------------------------------------|
| Name           | myVirtualNetwork                                            |
| Subscription   | Select your subscription.                                   |
| Resource group | Select <b>Create new</b> and enter <i>myResourceGroup</i> . |
| Location       | Select <b>East US</b> .                                     |

Select the IP Addresses tab and enter the following values:

| Setting                | Value                                                                   |
|------------------------|-------------------------------------------------------------------------|
| Address space          | 10.0.0.0/16                                                             |
| Subnet- Name           | Change the default subnet name to <b>mySubnet</b> and click <b>Save</b> |
| Subnet - Address range | 10.0.0.0/24                                                             |

#### 24.1.2 Task 2: Create application security groups

An application security group enables you to group together servers with similar functions, such as web servers.

1. Select + **Create a resource** on the upper left corner of the Azure portal.
2. In the **Search the Marketplace** box, enter *Application security group*. When **Application security group** appears in the search results, select it, select **Application security group** again under **Everything**, and then select **Create**.
3. Enter, or select, the following information, and then select **Create**:

| Setting        | Value                                                               |
|----------------|---------------------------------------------------------------------|
| Name           | myAsgWebServers                                                     |
| Subscription   | Select your subscription.                                           |
| Resource group | Select <b>Use existing</b> and then select <b>myResourceGroup</b> . |
| Location       | East US                                                             |

4. Complete step 3 again, specifying the following values:

| Setting        | Value                                                               |
|----------------|---------------------------------------------------------------------|
| Name           | myAsgMgmtServers                                                    |
| Subscription   | Select your subscription.                                           |
| Resource group | Select <b>Use existing</b> and then select <b>myResourceGroup</b> . |

| Setting  | Value   |
|----------|---------|
| Location | East US |

#### 24.1.3 Task 3: Create a network security group

1. Select + **Create a resource** on the upper left corner of the Azure portal.
2. Select **Networking**, and then select **Network security group**.
3. Enter, or select, the following information, and then select **Create**:

| Setting        | Value                                                               |
|----------------|---------------------------------------------------------------------|
| Name           | myNsg                                                               |
| Subscription   | Select your subscription.                                           |
| Resource group | Select <b>Use existing</b> and then select <i>myResourceGroup</i> . |
| Location       | East US                                                             |

#### 24.1.4 Task 4: Associate network security group to subnet

1. In the *Search resources, services, and docs* box at the top of the portal, begin typing *myNsg*. When **myNsg** appears in the search results, select it.
2. Under **SETTINGS**, select **Subnets** and then select + **Associate**.
3. Under **Associate subnet**, select **Virtual network** and then select **myVirtualNetwork**. Select **Subnet**, select **mySubnet**, and then select **OK**.

#### 24.1.5 Task 5: Create security rules

1. Under **SETTINGS**, select **Inbound security rules** and then select + **Add**.
2. Create a security rule that allows ports 80 and 443 to the **myAsgWebServers** application security group. Under **Add inbound security rule**, enter, or select the following values, accept the remaining defaults, and then select **Add**:

| Setting                 | Value                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Destination             | Select <b>Application security group</b> , and then select <b>myAsgWebServers</b> for <b>Application security group</b> . |
| Destination port ranges | Enter 80,443                                                                                                              |
| Protocol                | Select TCP                                                                                                                |
| Name                    | Allow-Web-All                                                                                                             |

3. Complete step 2 again, using the following values:

| Setting                 | Value                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Destination             | Select <b>Application security group</b> , and then select <b>myAsgMgmtServers</b> for <b>Application security group</b> . |
| Destination port ranges | Enter 3389                                                                                                                 |
| Protocol                | Select TCP                                                                                                                 |
| Priority                | Enter 110                                                                                                                  |
| Name                    | Allow-RDP-All                                                                                                              |

In this tutorial, RDP (port 3389) is exposed to the internet for the VM that is assigned to the *myAsgMgmtServers* application security group. For production environments, instead of exposing port 3389 to the internet, it's recommended that you connect to Azure resources that you want to manage using a VPN or private network connection.

#### 24.1.6 Task 6: Create virtual machines

1. Select + **Create a resource** found on the upper left corner of the Azure portal.

2. Select **Compute**, and then select **Windows Server 2016 Datacenter**.
3. Enter, or select, the following information, and accept the defaults for the remaining settings:

| Setting        | Value                                                          |
|----------------|----------------------------------------------------------------|
| Subscription   | Select your subscription.                                      |
| Resource group | Select <b>Use existing</b> and select <b>myResourceGroup</b> . |
| Name           | myVmWeb                                                        |
| Location       | Select <b>East US</b> .                                        |
| User name      | Enter a user name of your choosing.                            |
| Password       | Pa55w.rd1234                                                   |

4. Select a size for the VM and then select **Select**.
5. Under **Networking**, select the following values, and accept the remaining defaults:

| Setting                    | Value                            |
|----------------------------|----------------------------------|
| Virtual network            | Select <b>myVirtualNetwork</b> . |
| NIC network security group | Select <b>None</b> .             |

6. Under **Management**, select **Off** for **Boot diagnostics**.
7. Select **Review + Create** at the bottom left corner, select **Create** to start VM deployment.

#### 24.1.7 Task 7: Create the second VM

Complete above steps 1-7 again, but in step 3, name the VM *myVmMgmt*. The VM takes a few minutes to deploy. Do not continue to the next step until the VM is deployed.

#### 24.1.8 Task 8: Associate network interfaces to an ASG

When the portal created the VMs, it created a network interface for each VM and attached the network interface to the VM. Add the network interface for each VM to one of the application security groups you created previously:

1. In the *Search resources, services, and docs* box at the top of the portal, begin typing *myVmWeb*. When the **myVmWeb** VM appears in the search results, select it.
2. Under **SETTINGS**, select **Networking**. Select **Application security groups**, then **Configure the application security groups**, then select **myAsgWebServers** for **Application security groups**, and then select **Save**.
3. Complete steps 1 and 2 again, searching for the **myVmMgmt** VM and selecting the **myAsgMgmt-Servers** ASG.

#### 24.1.9 Task 9: Test traffic filters

1. Connect to the *myVmMgmt* VM. Enter *myVmMgmt* in the search box at the top of the portal. When **myVmMgmt** appears in the search results, select it. Select the **Connect** button.
2. Select **RDP**, then **Download RDP file**.
3. Open the downloaded rdp file and select **Connect**. Enter the user name and password you specified when creating the VM. You may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM.
4. Select **OK**.
5. You may receive a certificate warning during the sign-in process. If you receive the warning, select **Yes** or **Continue** to proceed with the connection.

The connection succeeds because port 3389 is allowed inbound from the internet to the *myAsgMgmtServers* application security group that the network interface attached to the *myVmMgmt* VM is in.

6. Connect to the *myVmWeb* VM from the *myVmMgmt* VM by entering the following command in a PowerShell session:

```
mstsc /v:myVmWeb
```

You are able to connect to the *myVmWeb* VM from the *myVmMgmt* VM because VMs in the same virtual network can communicate with each other over any port, by default. You can't, however, create a remote desktop connection to the *myVmWeb* VM from the internet because the security rule for the *myAsgWebServers* doesn't allow port 3389 inbound from the internet, and inbound traffic from the Internet is denied to all resources, by default.

7. To install Microsoft IIS on the *myVmWeb* VM, enter the following command from a PowerShell session on the *myVmWeb* VM:

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

8. After the IIS installation is complete, disconnect from the *myVmWeb* VM, which leaves you in the *myVmMgmt* VM remote desktop connection.

9. Disconnect from the *myVmMgmt* VM.

10. In the *Search resources, services, and docs* box at the top of the Azure portal, begin typing *myVmWeb* from your computer. When **myVmWeb** appears in the search results, select it. Note the **Public IP address** for your VM. The address shown in the following picture is 137.135.84.74, but your address is different:

| Setting                  | Value                                    |
|--------------------------|------------------------------------------|
| Computer name            | myVmWeb                                  |
| Operating system         | Windows                                  |
| Size                     | Standard DS1 v2 (1 vcpus, 3.5 GB memory) |
| <b>Public IP address</b> | <b>137.135.84.74</b>                     |
| Virtual network/subnet   | myVirtualNetwork/mySubnet                |
| DNS name                 | Configure                                |

11. To confirm that you can access the *myVmWeb* web server from the internet, open an internet browser on your computer and browse to <http://<public-ip-address-from-previous-step>>. You see the IIS welcome screen because port 80 is allowed inbound from the internet to the *myAsgWebServers* application security group that the network interface attached to the *myVmWeb* VM is in.

---

**WARNING:** Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

---

**Results:** You have now completed this lab.

## 25 Module 2: Lab 6 - NVA

### Scenario

Azure routes traffic between all subnets within a virtual network, by default. You can create your own routes to override Azure's default routing. The ability to create custom routes is helpful if, for example, you want to route traffic between subnets through a network virtual appliance (NVA). In this lab, you learn how to:

- Create a route table
- Create a route
- Create a virtual network with multiple subnets
- Associate a route table to a subnet
- Create an NVA that routes traffic
- Deploy virtual machines (VM) into different subnets
- Route traffic from one subnet to another through an NVA

## 25.1 Exercise 1: Route network traffic with a route table using the Azure portal

### 25.1.1 Task 1: Create a route table

1. On the upper-left side of the screen, select **Create a resource > Networking > Route table**, alternatively search for Route table in the Azure portal.
2. In **Create route table**, enter or select this information:

| Setting                                   | Value                                                                            |
|-------------------------------------------|----------------------------------------------------------------------------------|
| Name                                      | Enter <i>myRouteTablePublic</i> .                                                |
| Subscription                              | Select your subscription.                                                        |
| Resource group                            | Select <b>Create new</b> , enter <i>myResourceGroup</i> , and select <b>OK</b> . |
| Location                                  | Leave the default <b>East US</b> .                                               |
| Virtual network gateway route propagation | Leave the default <b>Enabled</b> .                                               |

3. Select **Create**.

### 25.1.2 Task 2: Create a route

1. In the portal's search bar, enter *myRouteTablePublic*.
2. When **myRouteTablePublic** appears in the search results, select it.
3. In **myRouteTablePublic** under **Settings**, select **Routes > + Add**.
4. In **Add route**, enter or select this information:

| Setting          | Value                             |
|------------------|-----------------------------------|
| Route name       | Enter <i>ToPrivateSubnet</i> .    |
| Address prefix   | Enter <i>10.0.1.0/24</i> .        |
| Next hop type    | Select <b>Virtual appliance</b> . |
| Next hop address | Enter <i>10.0.2.4</i> .           |

5. Select **OK**.

### 25.1.3 Task 3: Associate a route table to a subnet

Before you can associate a route table to a subnet, you have to create a virtual network and subnet.

1. On the upper-left side of the screen, select **Create a resource > Networking > Virtual network**.
2. In **Create virtual network**, enter or select this information:

| Setting        | Value                                                |
|----------------|------------------------------------------------------|
| Subscription   | Select your subscription.                            |
| Resource group | Select <b>Select existing &gt; myResourceGroup</b> . |
| Name           | Enter <i>myVirtualNetwork</i> .                      |
| Location       | Leave the default <b>East US</b> .                   |

Select the IP Addresses tab and enter the following values:

| Setting                | Value                                                                             |
|------------------------|-----------------------------------------------------------------------------------|
| Address space          | Enter <i>10.0.0.0/16</i> .                                                        |
| Subnet - Name          | Select the existing default subnet to change the name to Public then select Save. |
| Subnet - Address range | Enter <i>10.0.0.0/24</i> .                                                        |

3. Leave the rest of the defaults and select **Review + create**, then click **Create**.

#### 25.1.4 Task 4: Add subnets to the virtual network

1. In the portal's search bar, enter *myVirtualNetwork*.
2. When **myVirtualNetwork** appears in the search results, select it.
3. In **myVirtualNetwork**, under **Settings**, select **Subnets > + Subnet**.

The screenshot shows the Azure portal interface for managing subnets. At the top, the navigation bar includes 'Dashboard > myVirtualNetwork - Subnets'. Below this, the main title is 'myVirtualNetwork - Subnets' with a subtitle 'Virtual network'. On the left, there's a sidebar with links: 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Address space', 'Connected devices', and 'Subnets'. The 'Subnets' link is highlighted with a red box. The main content area has a search bar 'Search (Ctrl+ /)' and two buttons: '+ Subnet' (highlighted with a red box) and '+ Gateway subnet'. A table lists existing subnets: 'Public' with 'ADDRESS RANGE' '10.0.0.0/24'. The table has columns 'NAME' and 'ADDRESS RANGE'.

4. In **Add subnet**, enter this information:

| Setting       | Value                      |
|---------------|----------------------------|
| Name          | Enter <i>Private</i> .     |
| Address space | Enter <i>10.0.1.0/24</i> . |

5. Leave the rest of the defaults and select **OK**.

6. Select **+ Subnet** again. This time, enter this information:

| Setting       | Value                      |
|---------------|----------------------------|
| Name          | Enter <i>DMZ</i> .         |
| Address space | Enter <i>10.0.2.0/24</i> . |

7. Like the last time, leave the rest of the defaults and select **OK**.

Azure shows the three subnets: **Public**, **Private**, and **DMZ**.

#### 25.1.5 Task 5: Associate myRouteTablePublic to your Public subnet

1. Select **Public**.

2. In Public, select **Route table** > **MyRouteTablePublic** > Save.

The screenshot shows the Azure portal interface for creating a route table. On the left, under 'Public' settings, the 'Address range (CIDR block)' is set to '10.0.0.0/24'. Under 'Route table', it says 'None'. On the right, the 'Resource' pane lists existing route tables: 'None' and 'myRouteTablePublic eastus', which is highlighted with a red box. A message at the top right states: 'These are the route tables in the selected subscription and location 'East US''. Buttons for 'Save', 'Discard', 'Delete', and 'Refresh' are visible at the top left of the left pane.

#### 25.1.6 Task 6: Create an NVA

NVAs are VMs that help with network functions like routing and firewall optimization. You can select a different operating system if you want. This tutorial assumes you're using **Windows Server 2016 Datacenter**.

1. On the upper-left side of the screen, select **Create a resource** > **Compute** > **Virtual Machine**.
2. In **Create a virtual machine - Basics**, enter or select this information:

| Setting                         | Value                                                            |
|---------------------------------|------------------------------------------------------------------|
| <b>PROJECT DETAILS</b>          |                                                                  |
| Subscription                    | Select your subscription.                                        |
| Resource group                  | Select <b>myResourceGroup</b>                                    |
| <b>INSTANCE DETAILS</b>         |                                                                  |
| Virtual machine name            | Enter <i>myVmNva</i>                                             |
| Region                          | Select <b>East US</b> .                                          |
| Availability options            | Leave the default <b>No infrastructure redundancy required</b> . |
| Image                           | Select <b>Windows Server 2016 Datacenter</b> .                   |
| Size                            | Select <b>Standard DS1 v2</b> .                                  |
| <b>ADMINISTRATOR ACCOUNT</b>    |                                                                  |
| Username                        | Enter a user name of your choosing.                              |
| Password                        | Pa55w.rd1234                                                     |
| Confirm Password                | Reenter password.                                                |
| <b>INBOUND PORT RULES</b>       |                                                                  |
| Public inbound ports            | Select <b>None</b> .                                             |
| <b>SAVE MONEY</b>               |                                                                  |
| Already have a Windows license? | Leave the default <b>No</b> .                                    |

3. Select **Next : Disks**.
4. In **Create a virtual machine - Disks**, select the settings that are right for your needs.
5. Select **Next : Networking**.
6. In **Create a virtual machine - Networking**, select this information:

| Setting         | Value                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------|
| Virtual network | Leave the default <b>myVirtualNetwork</b> .                                                      |
| Subnet          | Select <b>DMZ (10.0.2.0/24)</b> .                                                                |
| Public IP       | Select <b>None</b> . You don't need a public IP address. The VM won't connect over the internet. |

7. Leave the rest of the defaults and select **Next : Management**.
8. In **Create a virtual machine - Management**, for **Diagnostics storage account**, select **Create New**.

9. In **Create storage account**, enter or select this information:

| Setting      | Value                                                      |
|--------------|------------------------------------------------------------|
| Name         | Enter a unique storage account name.                       |
| Account kind | Leave the default <b>Storage (general purpose v1)</b> .    |
| Performance  | Leave the default <b>Standard</b> .                        |
| Replication  | Leave the default <b>Locally-redundant storage (LRS)</b> . |

10. Select **OK**

11. Select **Review + create**. You're taken to the **Review + create** page and Azure validates your configuration.

12. When you see that **Validation passed**, select **Create**.

The VM takes a few minutes to create. Don't keep going until Azure finishes creating the VM. The **Your deployment is underway** page will show you deployment details.

13. When your VM is ready, select **Go to resource**.

#### 25.1.7 Task 7: Turn on IP forwarding

Turn on IP forwarding for *myVmNva*. When Azure sends network traffic to *myVmNva*, if the traffic is destined for a different IP address, IP forwarding will send the traffic to the correct location.

1. On **myVmNva**, under **Settings**, select **Networking**.
2. Select **myvmnva123**. That's the network interface Azure created for your VM. It will have a string of numbers to make it unique for you.
3. Under **Settings**, select **IP configurations**.
4. On **myvmnva123 - IP configurations**, for **IP forwarding**, select **Enabled** and then select **Save**.

The screenshot shows the Azure portal interface for managing IP configurations. At the top, the navigation path is: Home > myVmNva - Networking > myvmnva397 - IP configurations. The main title is "myvmnva397 - IP configurations" with a subtitle "Network interface". On the left, there's a sidebar with links: Overview, Activity log, Access control (IAM), Tags, Settings, and IP configurations (which is highlighted with a red box). The main content area has two sections: "IP forwarding settings" where "IP forwarding" is set to "Enabled" (also highlighted with a red box), and "IP configurations" where a single subnet "DMZ (10.0.2.0/24)" is listed. A search bar at the bottom is labeled "Search IP configurations".

#### 25.1.8 Task 8: Create public and private virtual machines

Create a public VM and a private VM in the virtual network. Later, you'll use them to see that Azure routes the *Public* subnet traffic to the *Private* subnet through the NVA.

1. Complete steps 1-12 of the Create an NVA task. Use most of the same settings. These values are the ones that have to be different:

| Setting                     | Value                                                                                                                                                             |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PUBLIC VM</b>            |                                                                                                                                                                   |
| <b>BASICS</b>               |                                                                                                                                                                   |
| Virtual machine name        | Enter <i>myVmPublic</i> .                                                                                                                                         |
| <b>NETWORKING</b>           |                                                                                                                                                                   |
| Subnet                      | Select <b>Public (10.0.0.0/24)</b> .                                                                                                                              |
| Public IP address           | Accept the default.                                                                                                                                               |
| Public inbound ports        | Select <b>Allow selected ports</b> .                                                                                                                              |
| Select inbound ports        | Select <b>HTTP and RDP</b> . <i>If the Networking tab does not allow the selected ports to be changed, click the Advanced button to change the port settings.</i> |
| <b>MANAGEMENT</b>           |                                                                                                                                                                   |
| Diagnostics storage account | Leave the default.                                                                                                                                                |
| <b>PRIVATE VM</b>           |                                                                                                                                                                   |
| <b>BASICS</b>               |                                                                                                                                                                   |
| Virtual machine name        | Enter <i>myVmPrivate</i> .                                                                                                                                        |
| <b>NETWORKING</b>           |                                                                                                                                                                   |
| Subnet                      | Select <b>Private (10.0.1.0/24)</b> .                                                                                                                             |
| Public IP address           | Accept the default.                                                                                                                                               |
| Public inbound ports        | Select <b>Allow selected ports</b> .                                                                                                                              |
| Select inbound ports        | Select <b>HTTP and RDP</b> .                                                                                                                                      |
| <b>MANAGEMENT</b>           |                                                                                                                                                                   |
| Diagnostics storage account | Leave the default.                                                                                                                                                |

You can create the *myVmPrivate* VM while Azure creates the *myVmPublic* VM. Don't continue with the rest of the steps until Azure finishes creating both VMs.

### 25.1.9 Task 9: Route traffic through an NVA

1. Sign in to *myVmPrivate* over remote desktop
2. In the portal's search bar, enter *myVmPrivate*.
3. When the **myVmPrivate** VM appears in the search results, select it.
4. Select **Connect** then select **RDP** to create a remote desktop connection to the *myVmPrivate* VM.
5. In **Connect to virtual machine**, select **Download RDP File**. Azure creates a Remote Desktop Protocol (.rdp) file and downloads it to your computer.
6. Open the downloaded .rdp file.
  1. If prompted, select **Connect**.
  2. Enter the user name and password you specified when creating the Private VM.
  3. You may need to select **More choices > Use a different account**, to use the Private VM credentials.
7. Select **OK**.

You may receive a certificate warning during the sign in process.

8. Select **Yes** to connect to the VM.

### 25.1.10 Task 10: Enable ICMP through the Windows firewall

In a later step, you'll use the trace route tool to test routing. Trace route uses the Internet Control Message Protocol (ICMP), which the Windows Firewall denies by default. Enable ICMP through the Windows firewall.

1. In the Remote Desktop of *myVmPrivate*, open PowerShell.
2. Enter this command:

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

You're using trace route to test routing in this tutorial. For production environments, we don't recommend allowing ICMP through the Windows Firewall.

### 25.1.11 Task 11: Turn on IP forwarding within myVmNva

You turned on IP forwarding for the VM's network interface using Azure. The VM's operating system also has to forward network traffic. Turn on IP forwarding for *myVmNva* VM's operating system with these commands.

1. From a command prompt on the *myVmPrivate* VM, open a remote desktop to the *myVmNva* VM:

```
mstsc /v:myvmnva
```

2. From PowerShell on the *myVmNva*, enter this command to turn on IP forwarding:

```
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -Name IpEnableRouter -Value 1
```

3. Restart the *myVmNva* VM. From the taskbar, select **Start button > Power button, Other (Planned) > Continue**.

That also disconnects the remote desktop session.

4. After the *myVmNva* VM restarts, create a remote desktop session to the *myVmPublic* VM. While still connected to the *myVmPrivate* VM, open a command prompt and run this command:

```
mstsc /v:myVmPublic
```

5. In the Remote Desktop of *myVmPublic*, open PowerShell.

6. Enable ICMP through the Windows firewall by entering this command:

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

### 25.1.12 Task 12: Test the routing of network traffic

First, let's test routing of network traffic from the *myVmPublic* VM to the *myVmPrivate* VM.

1. From PowerShell on the *myVmPublic* VM, enter this command:

```
tracert myVmPrivate
```

The response is similar to this example:

```
Tracing route to myVmPrivate.vpgub4nqnocezhjgurw44dnxrc.bx.internal.cloudapp.net [10.0.1.4]
over a maximum of 30 hops:
```

```
1 <1 ms * 1 ms 10.0.2.4
2 1 ms 1 ms 1 ms 10.0.1.4
```

Trace complete.

You can see the first hop is to 10.0.2.4. It's NVA's private IP address. The second hop is to the private IP address of the *myVmPrivate* VM: 10.0.1.4. Earlier, you added the route to the *myRouteTablePublic* route table and associated it to the *Public* subnet. As a result, Azure sent the traffic through the NVA and not directly to the *Private* subnet.

2. Close the remote desktop session to the *myVmPublic* VM, which leaves you still connected to the *myVmPrivate* VM.

3. From a command prompt on the *myVmPrivate* VM, enter this command:

```
tracert myVmPublic
```

It tests the routing of network traffic from the *myVmPrivate* VM to the *myVmPublic* VM. The response is similar to this example:

```
Tracing route to myVmPublic.vpgub4nqnocezhjgurw44dnxrc.bx.internal.cloudapp.net [10.0.0.4]
over a maximum of 30 hops:
```

```
1 1 ms 1 ms 1 ms 10.0.0.4
```

Trace complete.

You can see Azure routes traffic directly from the *myVmPrivate* VM to the *myVmPublic* VM. By default, Azure routes traffic directly between subnets.

4. Close the remote desktop session to the *myVmPrivate* VM.

---

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

---

**Results :** You have now completed this lab.

## 26 Module 2: Lab 7: Service Endpoints

Virtual network service endpoints enable you to limit network access to some Azure service resources to a virtual network subnet. You can also remove internet access to the resources. Service endpoints provide direct connection from your virtual network to supported Azure services, allowing you to use your virtual network's private address space to access the Azure services. Traffic destined to Azure resources through service endpoints always stays on the Microsoft Azure backbone network. In this tutorial, you learn how to:

- Create a virtual network with one subnet
- Add a subnet and enable a service endpoint
- Create an Azure resource and allow network access to it from only a subnet
- Deploy a virtual machine (VM) to each subnet
- Confirm access to a resource from a subnet
- Confirm access is denied to a resource from a subnet and the internet

### 26.1 Exercise 1: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal

#### 26.1.1 Task 1: Create a virtual network

1. Select **+** **Create a resource** on the upper left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter, or select, the following information, and then select **Review + create**, then click **Create**:

| Setting        | Value                                                       |
|----------------|-------------------------------------------------------------|
| Subscription   | Select your subscription                                    |
| Resource group | Select <b>Create new</b> and enter <i>myResourceGroup</i> . |
| Name           | myVirtualNetwork                                            |
| Location       | Select <b>East US</b>                                       |

Select the IP Addresses tab and enter the following values:

| Setting              | Value       |
|----------------------|-------------|
| Address space        | 10.0.0.0/16 |
| Subnet Name          | Public      |
| Subnet Address range | 10.0.0.0/24 |

Select the Security tab and enter the following values:

| Setting         | Value    |
|-----------------|----------|
| DDoS protection | Basic    |
| Firewall        | Disabled |

#### 26.1.2 Task 2: Enable a service endpoint

Service endpoints are enabled per service, per subnet. Create a subnet and enable a service endpoint for the subnet.

1. In the **Search resources, services, and docs** box at the top of the portal, enter *myVirtualNetwork*. When **myVirtualNetwork** appears in the search results, select it.

2. Add a subnet to the virtual network. Under **SETTINGS**, select **Subnets**, and then select **+ Subnet**, as shown in the following picture:

The screenshot shows the Azure portal interface for managing subnets. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Address space, Connected devices, and Subnets. The 'Subnets' option is highlighted with a red box. The main content area is titled 'myVirtualNetwork - Subnets' and shows a table of subnets. The table has columns for NAME, ADDRESS RANGE, and AVAILABLE ADDRS. One row is visible for 'Public' with the address range '10.0.0.0/24' and available addresses '251'. A red box highlights the '+ Subnet' button at the top right of the table.

3. Under **Add subnet**, select or enter the following information, and then select **OK**:

| Setting           | Value                                                 |
|-------------------|-------------------------------------------------------|
| Name              | Private                                               |
| Address range     | 10.0.1.0/24                                           |
| Service endpoints | Select <b>Microsoft.Storage</b> under <b>Services</b> |

#### 26.1.3 Task 3: Restrict network access for a subnet

By default, all VMs in a subnet can communicate with all resources. You can limit communication to and from all resources in a subnet by creating a network security group and associating it to the subnet.

1. Select **+ Create a resource** on the upper left corner of the Azure portal.
2. Select **Networking**, and then select **Network security group**.
3. Under **Create a network security group**, enter, or select, the following information, and then select **Review + create**, then click **Create**:

| Setting        | Value                                                          |
|----------------|----------------------------------------------------------------|
| Name           | myNsgPrivate                                                   |
| Subscription   | Select your subscription                                       |
| Resource group | Select <b>Use existing</b> and select <i>myResourceGroup</i> . |
| Location       | Select <b>East US</b>                                          |

4. After the network security group is created, enter *myNsgPrivate* in the **Search resources, services, and docs** box at the top of the portal. When **myNsgPrivate** appears in the search results, select it.
5. Under **SETTINGS**, select **Outbound security rules**.
6. Select **+ Add**.

7. Create a rule that allows outbound communication to the Azure Storage service. Enter, or select, the following information, and then select **Add**:

| Setting                 | Value                        |
|-------------------------|------------------------------|
| Source                  | Select <b>VirtualNetwork</b> |
| Source port ranges      | *                            |
| Destination             | Select <b>Service Tag</b>    |
| Destination service tag | Select <b>Storage</b>        |
| Destination port ranges | *                            |
| Protocol                | Any                          |
| Action                  | Allow                        |
| Priority                | 100                          |
| Name                    | Allow-Storage-All            |

8. Create another outbound security rule that denies communication to the internet. This rule overrides a default rule in all network security groups that allows outbound internet communication. Complete steps 5-7 again, using the following values:

| Setting                 | Value                        |
|-------------------------|------------------------------|
| Source                  | Select <b>VirtualNetwork</b> |
| Source port ranges      | *                            |
| Destination             | Select <b>Service Tag</b>    |
| Destination service tag | Select <b>Internet</b>       |
| Destination port ranges | *                            |
| Protocol                | Any                          |
| Action                  | Deny                         |
| Priority                | 110                          |
| Name                    | Deny-Internet-All            |

9. Under **SETTINGS**, select **Inbound security rules**.

10. Select **+ Add**.

11. Create an inbound security rule that allows Remote Desktop Protocol (RDP) traffic to the subnet from anywhere. The rule overrides a default security rule that denies all inbound traffic from the internet. Remote desktop connections are allowed to the subnet so that connectivity can be tested in a later step. Under **SETTINGS**, select **Inbound security rules**, select **+Add**, enter the following values, and then select **Add**:

| Setting                 | Value                        |
|-------------------------|------------------------------|
| Source                  | Any                          |
| Source port ranges      | *                            |
| Destination             | Select <b>VirtualNetwork</b> |
| Destination port ranges | 3389                         |
| Protocol                | Any                          |
| Action                  | Allow                        |
| Priority                | 120                          |
| Name                    | Allow-RDP-All                |

12. Under **SETTINGS**, select **Subnets**.

13. Select **+ Associate**

14. Under **Associate subnet**, select **Virtual network** and then select **myVirtualNetwork** under **Choose a virtual network**.

15. Under **Choose subnet**, select **Private**, and then select **OK**.

#### 26.1.4 Task 4: Restrict network access to a resource

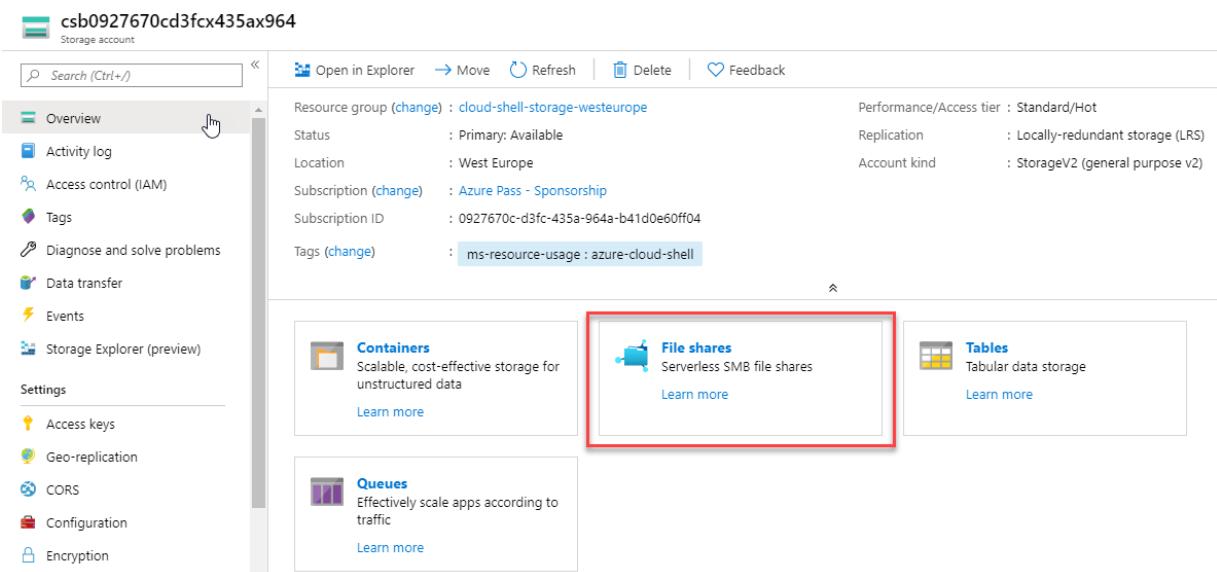
The steps necessary to restrict network access to resources created through Azure services enabled for service endpoints varies across services. See the documentation for individual services for specific steps for each service. The remainder of this tutorial includes steps to restrict network access for an Azure Storage account, as an example.

1. Select + **Create a resource** on the upper left corner of the Azure portal.
2. Select **Storage**, and then select **Storage account - blob, file, table, queue**.
3. Enter, or select, the following information, accept the remaining defaults, and then select **Review + create**, then click **Create**:

| Setting        | Value                                                                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name           | Enter a name that is unique across all Azure locations, between 3-24 characters in length, using only numbers, lowercase letters, and hyphens. For example, csb0927670cd3fcx435ax964. |
| Account kind   | StorageV2 (general purpose v2)                                                                                                                                                        |
| Location       | Select <b>East US</b>                                                                                                                                                                 |
| Replication    | Locally-redundant storage (LRS)                                                                                                                                                       |
| Subscription   | Select your subscription                                                                                                                                                              |
| Resource group | Select <b>Use existing</b> and select <i>myResourceGroup</i> .                                                                                                                        |

#### 26.1.5 Task 5: Create a file share in the storage account

1. After the storage account is created, enter the name of the storage account in the **Search resources, services, and docs** box, at the top of the portal. When the name of your storage account appears in the search results, select it.
2. Select **File shares**, as shown in the following picture:



3. Select + **File share**.
4. Enter *my-file-share* under **Name**, and then select **Create**.
5. Close the **File service** box.

#### 26.1.6 Task 6: Restrict network access to a subnet

By default, storage accounts accept network connections from clients in any network, including the internet. Deny network access from the internet, and all other subnets in all virtual networks, except for the *Private* subnet in the *myVirtualNetwork* virtual network.

1. Under **SETTINGS** for the storage account, select **Firewalls and virtual networks**.
2. Select **Selected networks**.
3. Select +**Add existing virtual network**.

- Under **Add networks**, select the following values, and then select **Add**:

| Setting          | Value                                                          |
|------------------|----------------------------------------------------------------|
| Subscription     | Select your subscription.                                      |
| Virtual networks | Select <b>myVirtualNetwork</b> , under <b>Virtual networks</b> |
| Subnets          | Select <b>Private</b> , under <b>Subnets</b>                   |

- Select **Save**.
- Close the **Firewalls and virtual networks** box.
- Under **SETTINGS** for the storage account, select **Access keys**.
- Note the **Key** value, as you'll have to manually enter it in a later step when mapping the file share to a drive letter in a VM.

#### 26.1.7 Task 7: Create virtual machines

To test network access to a storage account, deploy a VM to each subnet.

- Select **+ Create a resource** found on the upper left corner of the Azure portal.
- Select **Compute**, and then select **Virtual Machine**.
- Enter, or select, the following information and then select **OK**:

| Setting        | Value                                                          |
|----------------|----------------------------------------------------------------|
| Name           | myVmPublic                                                     |
| User name      | Enter a user name of your choosing.                            |
| Password       | Pa55w.rd1234                                                   |
| Subscription   | Select your subscription.                                      |
| Resource group | Select <b>Use existing</b> and select <b>myResourceGroup</b> . |
| Location       | Select <b>East US</b> .                                        |
| Image          | Select <b>Windows Server 2019 Datacenter</b> .                 |

- Select a size for the virtual machine and then select **Select**.
- On the **Networking** tab select **myVirtualNetwork**. Then select **Subnet**, and select the **Public** subnet.
- Under **Network Security Group**, select **Basic** and allow port 3389.
- Click **Review + create**.
- On the **Summary** page, select **Create** to start the virtual machine deployment. The VM takes a few minutes to deploy, but you can continue to the next step while the VM is creating.
- Complete steps 1-8 again, but in step 3, name the virtual machine *myVmPrivate* and in step 5, select the **Private** subnet.

The VM takes a few minutes to deploy. Do not continue to the next step until it finishes creating and its settings open in the portal.

#### 26.1.8 Task 8: Confirm access to storage account

- Once the *myVmPrivate* VM finishes creating, open the blade for the VM by selecting **Go to resource**. Select the **Connect** button, then select RDP.
- After selecting the **Connect** button and RDP, select the Download RDP File button. A Remote Desktop Protocol (.rdp) file is created and downloaded to your computer.
- Open the downloaded rdp file. If prompted, select **Connect**. Enter the user name and password you specified when creating the VM. You may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM.
- Select **OK**.

5. You may receive a certificate warning during the sign-in process. If you receive the warning, select **Yes** or **Continue** to proceed with the connection.
6. On the *myVmPrivate* VM, map the Azure file share to drive Z using PowerShell. Before running the commands that follow, replace <storage-account-key> and <storage-account-name> with values you supplied and retrieved in the **Create a storage account** task.

```
$acctKey = ConvertTo-SecureString -String "<storage-account-key>" -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\<storage-a
New-PSDrive -Name Z -PSProvider FileSystem -Root "\\\<storage-account-name>.file.core.windows.net\m
```

The Azure file share successfully mapped to the Z drive.

7. Confirm that the VM has no outbound connectivity to the internet from a command prompt:

```
ping bing.com
```

You receive no replies because the network security group associated to the *Private* subnet does not allow outbound access to the internet.

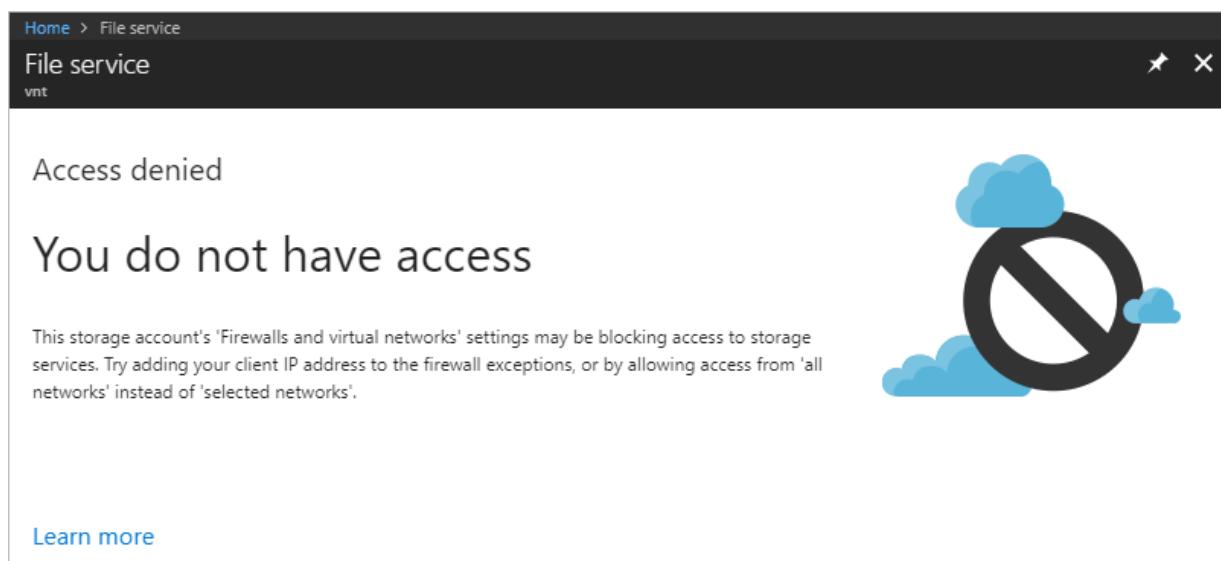
8. Close the remote desktop session to the *myVmPrivate* VM.

#### 26.1.9 Task 9: Confirm access is denied to storage account

1. Enter *myVmPublic* In the **Search resources, services, and docs** box at the top of the portal.
2. When **myVmPublic** appears in the search results, select it.
3. Complete steps 1-6 in the Confirm access to storage account task for the *myVmPublic* VM.

After a short wait, you receive a **New-PSDrive : Access is denied** error. Access is denied because the *myVmPublic* VM is deployed in the *Public* subnet. The *Public* subnet does not have a service endpoint enabled for Azure Storage. The storage account only allows network access from the *Private* subnet, not the *Public* subnet.

4. Close the remote desktop session to the *myVmPublic* VM.
5. From your computer, browse to the Azure portal.
6. Enter the name of the storage account you created in the **Search resources, services, and docs** box. When the name of your storage account appears in the search results, select it.
7. Select **File shares** then select *my-file-share*.
8. You receive the error shown in the following screenshot:



Access is denied, because your computer is not in the *Private* subnet of the *MyVirtualNetwork* virtual network.

---

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

---

**Results :** You have now completed this lab.

## 27 Module 2: Lab 8 - VNet Peering

### Scenario

You can connect virtual networks to each other with virtual network peering. These virtual networks can be in the same region or different regions (also known as Global VNet peering). Once virtual networks are peered, resources in both virtual networks are able to communicate with each other, with the same latency and bandwidth as if the resources were in the same virtual network. In this tutorial, you learn how to:

- Create two virtual networks
- Connect two virtual networks with a virtual network peering
- Deploy a virtual machine (VM) into each virtual network
- Communicate between VMs

### 27.0.1 Exercise 1: Create Virtual Networks and implement Peering.

#### 27.0.2 Task 1: Create virtual networks

1. Select + **Create a resource** on the upper, left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **Click Review + create**, then click **Create**:

| Setting        | Value                                                       |
|----------------|-------------------------------------------------------------|
| Name           | myVirtualNetwork1                                           |
| Subscription   | Select your subscription.                                   |
| Resource group | Select <b>Create new</b> and enter <i>myResourceGroup</i> . |
| Location       | Select <b>East US</b> .                                     |

Select the IP Addresses tab and enter the following values:

| Setting              | Value       |
|----------------------|-------------|
| Address space        | 10.0.0.0/16 |
| Subnet Name          | Subnet1     |
| Subnet Address range | 10.0.0.0/24 |

4. Complete steps 1-3 again, with the following changes:

| Setting              | Value                                                               |
|----------------------|---------------------------------------------------------------------|
| Name                 | myVirtualNetwork2                                                   |
| Address space        | 10.1.0.0/16                                                         |
| Resource group       | Select <b>Use existing</b> and then select <b>myResourceGroup</b> . |
| Subnet Address range | 10.1.0.0/24                                                         |

#### 27.0.3 Task 2: Peer virtual networks

1. In the Search box at the top of the Azure portal, begin typing *MyVirtualNetwork1*. When **myVirtualNetwork1** appears in the search results, select it.
2. Select **Peering**, under **SETTINGS**, and then select + **Add**.
3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **Review + create**, then click **Create**:

**OK.**

| Setting         | Value                                                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Name            | myVirtualNetwork1-myVirtualNetwork2                                                                                                                |
| Subscription    | Select your subscription.                                                                                                                          |
| Virtual network | myVirtualNetwork2 - To select the <i>myVirtualNetwork2</i> virtual network, select <b>Virtual network</b> , then select <i>myVirtualNetwork2</i> . |
| Name            | myVirtualNetwork2-myVirtualNetwork1                                                                                                                |

The **PEERING STATUS** is *Initiated*.

If you don't see the status, refresh your browser.

The **PEERING STATUS** is *Connected*. Azure also changed the peering status for the *myVirtualNetwork2-myVirtualNetwork1* peering from *Initiated* to *Connected*. Virtual network peering is not fully established until the peering status for both virtual networks is *Connected*.

#### 27.0.4 Task 3: Create virtual machines

1. Select + **Create a resource** on the upper, left corner of the Azure portal.
2. Select **Compute > Virtual Machine**. When creating the VM, select **Windows Server 2016 Datacenter** as the operating system.
3. Enter, or select, the following information for **Basics**, accept the defaults for the remaining settings, and then select **Create**:

| Setting        | Value                           |
|----------------|---------------------------------|
| Resource group | Select <b>myResourceGroup</b> . |
| Name           | myVM1                           |
| Region         | East US                         |
| User name      | localadmin                      |
| Password       | Pa55w.rd1234                    |

## Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

### Project details

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

\* Subscription 

Azure Pass - Sponsorship 

  \* Resource group 

myResourceGroup 

[Create new](#)

### Instance details

\* Virtual machine name 

myVM1 

\* Region 

(US) East US 

Availability options 

No infrastructure redundancy required 

\* Image 

Windows Server 2016 Datacenter 

[Browse all public and private images](#)

\* Size 

**Standard DS1 v2**

1 vcpu, 3.5 GiB memory

[Change size](#)

### Administrator account

\* Username 

localadmin 

\* Password 

\*\*\*\*\* 

[Review + create](#)

< Previous

Next : Disks >

4. Select the Networking Tab:

| Setting              | Value                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------|
| Virtual network      | myVirtualNetwork1 - If it's not already selected, select <b>Virtual network</b> and then select <b>myVirtualNetwork1</b> |
| Subnet               | Subnet1 - If it's not already selected, select <b>Subnet</b> and then select <b>Subnet1</b> under <b>Choose subnet</b>   |
| Public inbound ports | Select <b>Allow selected ports</b>                                                                                       |
| Select inbound ports | <b>RDP</b>                                                                                                               |

5. Select the Management Tab and turn all the radio buttons to **Off**.

## Create a virtual machine

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

**Azure Security Center**

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

Your subscription is protected by Azure Security Center standard plan.

**Monitoring**

Boot diagnostics  On  Off

OS guest diagnostics  On  Off

**Identity**

System assigned managed identity  On  Off

**Auto-shutdown**

Enable auto-shutdown  On  Off

**Backup**

Enable backup  On  Off



6. Select **Review + create** and click **Create**.
7. Complete the above steps again, with the following changes (The VMs take a few minutes to create. Do not continue with the remaining steps until both VMs are created.):

| Setting         | Value             |
|-----------------|-------------------|
| Name            | myVM2             |
| Virtual network | myVirtualNetwork2 |

### 27.0.5 Task 4: Communicate between VMs

1. In the *Search* box at the top of the portal, begin typing *myVM1*. When **myVM1** appears in the search results, select it.
2. Create a remote desktop connection to the *myVm1* VM by selecting **Connect**, then selecting **RDP**, then selecting the **Download RDP File** button.
3. To connect to the VM, open the downloaded RDP file. If prompted, select **Connect**.
4. Enter the user name and password you specified when creating the VM (you may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM), then select **OK**.
5. You may receive a certificate warning during the sign-in process. Select **Yes** to proceed with the connection.
6. In a later step, ping is used to communicate with the *myVm2* VM from the *myVm1* VM. Ping uses the Internet Control Message Protocol (ICMP), which is denied through the Windows Firewall, by default.

On the *myVm1* VM, enable ICMP through the Windows firewall, so that you can ping this VM from *myVm2* in a later step, using PowerShell:

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

Though ping is used to communicate between VMs in this tutorial, allowing ICMP through the Windows Firewall for production deployments is not recommended.

7. To connect to the *myVm2* VM, enter the following command from a command prompt on the *myVm1* VM:  
*If prompted, enter the credentials. Being able to connect this verifies you can use the peering connection to myVM2 using RDP on the internal network.*

```
mstsc /v:10.1.0.4
```

8. Since you enabled ping on *myVm1*, you can now ping it by IP address: *This verifies that the established peer is functioning as expected.*

```
ping 10.0.0.4
```

9. Disconnect your RDP sessions to both *myVM1* and *myVM2*.

---

**WARNING:** Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**

---

**Results :** You have now completed this lab.

## 28 Lab 9: Azure DNS

### Scenario

In this module, you will learn about DNS basics and specifically implementing Azure DNS. In the DNS Basics lesson you will review DNS domains, zones, record types, and resolution methods. In the Azure DNS lesson, we will cover delegation, metrics, alerts, and DNS hosting schemes.

### Objectives

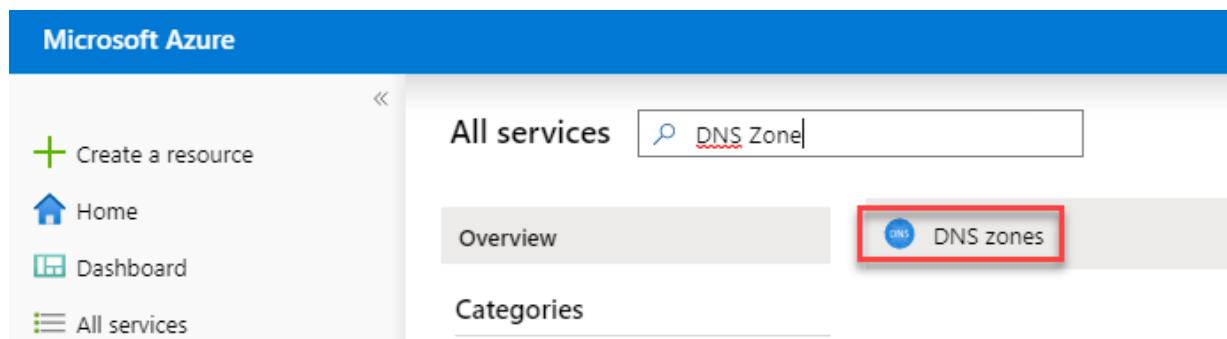
Lessons include:

- Azure DNS Basics
- Implementing Azure DNS

### 28.1 Exercise 1: DNS Zones

#### 28.1.1 Task 1: Create a DNS zone

1. Sign in to the Azure Portal.
2. On the Hub menu, click **All services** and search for and select **DNS zones**.



3. Click **+ Add**.

The screenshot shows the 'DNS zones' blade in the Azure portal. At the top, there's a 'Default Directory' dropdown, followed by a row of buttons: '+ Add' (highlighted with a red box), 'Edit columns', 'Refresh', and 'Export'. Below this is a search bar with 'Filter by name...' and a dropdown for 'Subscription == all'. A message says 'Showing 0 to 0 of 0 records.' and there's a sorting option 'Name ↑↓'. The main area is currently empty.

4. On the **Create DNS zone** blade enter the following values, then click **Review + create** and then click **Create**:

| Setting        | Value                              | Details                                                         |
|----------------|------------------------------------|-----------------------------------------------------------------|
| Subscription   | <i>Your subscription</i>           | Select a subscription to create the DNS zone in.                |
| Resource group | Create new: <i>myResourceGroup</i> | Create a resource group. The resource group name must be unique |
| Name           | <u>see details</u>                 | The name of the DNS zone (yours must be unique)                 |
| Location       | East US                            |                                                                 |

### Create DNS zone

Basics Tags Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more](#).

#### Project details

|                  |                            |
|------------------|----------------------------|
| Subscription *   | Azure Pass - Sponsorship   |
| Resource group * | (New) myResourceGroup      |
|                  | <a href="#">Create new</a> |

#### Instance details

|                           |              |
|---------------------------|--------------|
| Name *                    | azuredns.com |
| Resource group location ⓘ | (US) East US |

## 28.2 Exercise 2: Manage DNS records and record sets by using the Azure portal

This exercise shows you how to manage record sets and records for your DNS zone by using the Azure portal.

### 28.2.1 Task 1: Add a new record to a record set

1. In the Azure Portal, navigate to **All resources** and select your DNS zone you created in the previous task.

**Note:** Each DNS zone is its own resource, and information such as number of record-sets and name servers are viewable from this view.

2. Click **+ Record Set**.

azuredns.com  
DNS zone

Search (Ctrl+ /) <> + Record set → Move Delete zone Refresh

Overview Activity log Access control (IAM) Tags

Resource group (change) : myresourcegroup  
Subscription (change) : Azure Pass - Sponsorship  
Subscription ID : 0927670c-d3fc-435a-964a-b41d0e60ff04  
Tags (change) Click here to add tags

3. Enter **testrecord** for the name and **1.2.3.4** as the IP address and click **OK**.

Add record set azuredns.com

Name testrecord .azuredns.com

Type A

Alias record set ①  
 Yes  No

TTL \* 1 TTL unit Hours

IP address  
1.2.3.4 ...  
0.0.0.0 ...

#### 28.2.2 Task 2: Update a record

1. In the Overview blade for your DNS zone, select the testrecord you created.

| Name       | Type | TTL    | Value                                                                                                                                               | Alias resource type | Alias target |
|------------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------|
| @          | NS   | 172800 | ns1-05.azure-dns.com.<br>ns2-05.azure-dns.net.<br>ns3-05.azure-dns.org.<br>ns4-05.azure-dns.info.                                                   |                     |              |
| @          | SOA  | 3600   | Email: azuredns-hostmas...<br>Host: ns1-05.azure-dns.c...<br>Refresh: 3600<br>Retry: 300<br>Expire: 2419200<br>Minimum TTL: 300<br>Serial number: 1 |                     |              |
| testrecord | A    | 3600   | 1.2.3.4                                                                                                                                             |                     |              |

2. Under IP Address add the test address of **4.3.2.1** and click **Save**.

**testrecord**  
azuredns.com

Save Discard Delete Users Metadata

testrecord.azuredns.com

Type: A

Alias record set:  No

TTL \*: 1 Hours

IP address: 4.3.2.1 (highlighted)

### 28.2.3 Task 3: Remove a record from a record set

You can use the Azure portal to remove records from a record set. Note that removing the last record from a record set does not delete the record set.

1. In the Overview pane for your DNS zone, select the testrecord you created.

| Name       | Type | TTL    | Value                                                                                                                                               | Alias resource type | Alias target |
|------------|------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------|
| @          | NS   | 172800 | ns1-05.azure-dns.com.<br>ns2-05.azure-dns.net.<br>ns3-05.azure-dns.org.<br>ns4-05.azure-dns.info.                                                   |                     |              |
| @          | SOA  | 3600   | Email: azuredns-hostmas...<br>Host: ns1-05.azure-dns.c...<br>Refresh: 3600<br>Retry: 300<br>Expire: 2419200<br>Minimum TTL: 300<br>Serial number: 1 |                     |              |
| testrecord | A    | 3600   | 1.2.3.4                                                                                                                                             |                     |              |

2. Select **Delete** and click **Yes** when prompted.

**testrecord**  
azuredns.com

Save   Discard   **Delete**   Users   Metadata

testrecord.azuredns.com

Type: A

Alias record set:  Yes  No

TTL: 1 Hours

IP address: 4.3.2.1

## Work with NS and SOA records

NS and SOA records that are automatically created are managed differently from other record types.

### Modify SOA records

You cannot add or remove records from the automatically created SOA record set at the zone apex (name = "@"). However, you can modify any of the parameters within the SOA record (except "Host") and the record set TTL.

### Modify NS records at the zone apex

The NS record set at the zone apex is automatically created with each DNS zone. It contains the names of the Azure DNS name servers assigned to the zone.

You can add additional name servers to this NS record set, to support co-hosting domains with more than one

DNS provider. You can also modify the TTL and metadata for this record set. However, you cannot remove or modify the pre-populated Azure DNS name servers.

Note that this applies only to the NS record set at the zone apex. Other NS record sets in your zone (as used to delegate child zones) can be modified without constraint.

#### Delete SOA or NS record sets

You cannot delete the SOA and NS record sets at the zone apex (name = "@") that are created automatically when the zone is created. They are deleted automatically when you delete the zone.

You are then prompted to confirm you are wanting to delete the DNS zone. Deleting a DNS zone also deletes all records that are contained in the zone.

---

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

---

## 29 Module 2: Lab 10 - Load Balancer

### Scenario

In this module, you will learn about three ways to distribute network traffic: Azure Load Balancer, Azure Traffic Manager, and Azure Application Gateway. The Azure Load Balancer delivers high availability and network performance to your applications. The Azure Traffic Manager allows you to control the distribution of user traffic to your service endpoints. The Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

### Lessons include:

- Azure Load Balancer
- Azure Traffic Manager
- Azure Application Gateway

### 29.1 Exercise 1: Distributing Network Traffic using a Standard Load Balancer

In this section, you create a public load balancer that helps load balance virtual machines. Standard Load Balancer only supports a Standard Public IP address. When you create a Standard Load Balancer, and you must also create a new Standard Public IP address that is configured as the frontend (named as *LoadBalancerFrontend* by default) for the Standard Load Balancer.

#### 29.1.1 Task 1: Create a public load balancer

1. On the top left-hand side of the screen, click **Create a resource** > **Networking** > **Load Balancer**.
2. In the **Create load balancer** page, enter or select the following information, accept the defaults for the remaining settings, and then select **Review + create**:

| Setting           | Value                                                                |
|-------------------|----------------------------------------------------------------------|
| Subscription      | Select your subscription.                                            |
| Resource group    | Select <b>Create new</b> , and then type <i>myResourceGroupLB</i>    |
| Name              | <i>myLoadBalancer</i>                                                |
| Region            | Select <b>East US</b> .                                              |
| Type              | Public                                                               |
| SKU               | Standard                                                             |
| Public IP address | Select <b>Create new</b> and type <i>myPublicIP</i> in the name box. |
| Availability zone | <b>Zone-redundant</b>                                                |

## Create load balancer

Basics Tags Review + create

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

### Project details

Subscription \*

Azure Pass - Sponsorship

Resource group \*

(New) myResourceGroupLB

[Create new](#)

### Instance details

Name \*

myLoadBalancer

Region \*

(US) East US

Type \* ⓘ

Internal  Public

SKU \* ⓘ

Basic  Standard

### Public IP address

Public IP address \* ⓘ

Create new  Use existing

Public IP address name \*

myPublicIP

Public IP address SKU

Standard

Assignment \*

Dynamic  Static

Availability zone \*

Zone-redundant

[Review + create](#)

< Previous

Next : Tags >

[Download a template for automation](#)

3. On the Validation screen click **Create**.

### 29.1.2 Task 2: Create a virtual network

1. On the top left-hand side of the screen click **+ Create a resource** > **Networking** > **Virtual network** and enter these values for the virtual network:

- **myVnet** - for the name of the virtual network.
- **myResourceGroupLB** - for the name of the existing resource group

Select the IP Addresses tab and enter the following values:

- **10.0.0.0/16** - for the Address space
- **myBackendSubnet** - for the subnet name.
- **10.0.0.0/24** - for the Subnet Address range

2. Click **Review + create**, then click **Create** to create the virtual network.

### 29.1.3 Task 3: Create virtual machines

1. On the top left-hand side of the screen, click **Create a resource > Compute > Virtual Machine** and enter these values for the virtual machine:

- **myResourceGroupLB** - for **Resource group**, select *myResourceGroupLB* from the drop down menu.
- **myVM1** - for the name of the virtual machine.
- **Image** - Windows Server 2019 Datacenter.
- **localadmin** - for the **Username**
- **Pa55w.rd1234** - for the **Password**
- **HTTP (80) & RDP (3389)** - for the inbound port rules.

#### Create a virtual machine

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

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

**Project details**

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

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

**Instance details**

Virtual machine name \* ⓘ

Region \* ⓘ

Availability options ⓘ

Image \* ⓘ  [Browse all public and private images](#)

Size \* ⓘ **Standard D2s v3**  
2 vcpus, 8 GiB memory  
[Change size](#)

**Administrator account**

Username \* ⓘ

Password \* ⓘ

2. Click the Networking Tab and under Public IP click **Create new**. Name the IP Address **myPIP1** and click the **Standard SKU** then click **OK**.

**Note:** If you do not select the Standard SKU here you will have problems later in the lab.

## Create public IP address

X

Name \*

myPIP1

SKU ⓘ

Basic  Standard

Assignment ⓘ

Static

Availability zone

Zone-redundant

3. Select the **Management** Tab and ensure all radio buttons are **No** or **Off**.
4. Click **Review + create** then click **Create**.
5. Repeat the steps above to create a second VM, called *myVM2* using *myPIP2* for the new Public IP address.

### 29.1.4 Task 4: Install IIS

1. Click **All resources** in the left-hand menu, and then from the resources list click **myVM1** that is located in the *myResourceGroupLB* resource group.
2. On the **Overview** page, click **Connect** to RDP into the VM.
3. Log into the VM with username *localadmin*.
4. Open PowerShell and run the following command to install IIS.  
`Install-WindowsFeature Web-Server`
5. Repeat steps 1 to 4 for the virtual machine *myVM2*.

### 29.1.5 Task 5: Create load balancer resources

In this section, you configure load balancer settings for a backend address pool and a health probe, and specify a load balancer rule.

To distribute traffic to the VMs, a backend address pool contains the IP addresses of the virtual (NICs) connected to the load balancer. Create the backend address pool *myBackendPool* to include *VM1* and *VM2*.

1. Click **All resources** in the left-hand menu, and then click **myLoadBalancer** from the resources list.
2. Under **Settings**, click **Backend pools**, then click **Add**.

The screenshot shows the 'Backend pools' page for a 'myLoadBalancer' load balancer. On the left, there's a sidebar with links like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Below that is a 'Settings' section with Frontend IP configuration, Backend pools (which is selected and highlighted with a red box), and Health probes. At the top right, there are 'Add' and 'Refresh' buttons, and a search bar for 'backend address pools'. The main area is titled 'Virtual machine' and displays 'No results.'

3. On the **Add a backend pool** page, do the following:

- For name, type *myBackendPool*, as the name for your backend pool.
- For **Virtual network**, select *myVNet*.
- Add *myVM1* and *my VM2* under **Virtual Machine** along with their corresponding IP addresses, and then select **Add**.

**Add backend pool**

myLoadBalancer

Name \*

IP version

IPv4     IPv6

Virtual network ⓘ

myvnet (2 VM)

| Virtual machine                | IP address           |                                                                                                                                                                          |
|--------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> myvm1 | ipconfig1            | <input style="border: none; font-size: small;" type="button" value="..."/>                                                                                               |
| <input type="checkbox"/> myvm2 | ipconfig1 (10.0.0.5) | <input style="border: none; font-size: small;" type="button" value="..."/>                                                                                               |
|                                |                      | <input style="border: 1px solid #0072bc; background-color: #0072bc; color: white; padding: 2px 10px; border-radius: 5px; font-weight: bold;" type="button" value="Add"/> |

3. Check to make sure your load balancer backend pool setting displays both the VMs **VM1** and **VM2**.

| Virtual machine | Virtual machine status | Network interface | Private IP address |
|-----------------|------------------------|-------------------|--------------------|
| myVM1           | Running                | myvm1908          | 10.0.0.4           |
| myVM2           | Running                | myvm211           | 10.0.0.5           |

### 29.1.6 Task 6: Create a health probe

To allow the load balancer to monitor the status of your app, you use a health probe. The health probe dynamically adds or removes VMs from the load balancer rotation based on their response to health checks. Create a health probe *myHealthProbe* to monitor the health of the VMs.

1. On the Load Balancer blade, under **Settings**, click **Health probes**, then click **Add**.

| Name        |
|-------------|
| No results. |

2. Use these values to create the health probe:

- *myHealthProbe* - for the name of the health probe.
- **HTTP** - for the protocol type.
- **80** - for the port number.
- **/** - for the URI path.
- **15** - for number of **Interval** in seconds between probe attempts.
- **2** - for number of **Unhealthy threshold** or consecutive probe failures that must occur before a VM is considered unhealthy.

## Add health probe

myLoadBalancer

Name \*

myHealthProbe



Protocol ⓘ

HTTP



Port \* ⓘ

80

Path \* ⓘ

/

Interval \* ⓘ

15



seconds

Unhealthy threshold \* ⓘ

2

consecutive failures

3. Click **OK**.

### 29.1.7 Task 7: Create a load balancer rule

A load balancer rule is used to define how traffic is distributed to the VMs. You define the frontend IP configuration for the incoming traffic and the backend IP pool to receive the traffic, along with the required source and destination port. Create a load balancer rule *myLoadBalancerRuleWeb* for listening to port 80 in the frontend *FrontendLoadBalancer* and sending load-balanced network traffic to the backend address pool *myBackEndPool* also using port 80.

1. On the Load Balancer blade, under **Settings**, click **Load balancing rules**, then click **Add**.

The screenshot shows the Azure portal interface for managing load balancing rules. The main title is "myLoadBalancer - Load balancing rules". On the left, there's a sidebar with icons for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Frontend IP configuration, Backend pools, Health probes, and Load balancing rules. The "Load balancing rules" item is highlighted with a red box. The main content area has a search bar at the top, followed by an "Add" button (also highlighted with a red box). Below that is a search bar for "Search load balancing r" and a "Name" input field. A message "No results." is displayed.

2. Use these values to configure the load balancing rule:

- *myHTTPRule* - for the name of the load balancing rule.
- **TCP** - for the protocol type.
- *80* - for the port number.
- *80* - for the backend port.
- *myBackendPool* - for the name of the backend pool.
- *myHealthProbe* - for the name of the health probe.

## Add load balancing rule

myLoadBalancer

Name \*

myHTTPRule

IP Version \*

IPv4  IPv6

Frontend IP address \* ⓘ

52.224.191.157 (LoadBalancerFrontEnd)



Protocol

TCP  UDP

Port \*

80

Backend port \* ⓘ

80

Backend pool ⓘ

myBackendPool (2 virtual machines)



Health probe ⓘ

myHealthProbe (HTTP:80)



Session persistence ⓘ

None



Idle timeout (minutes) ⓘ

0 — 4

4

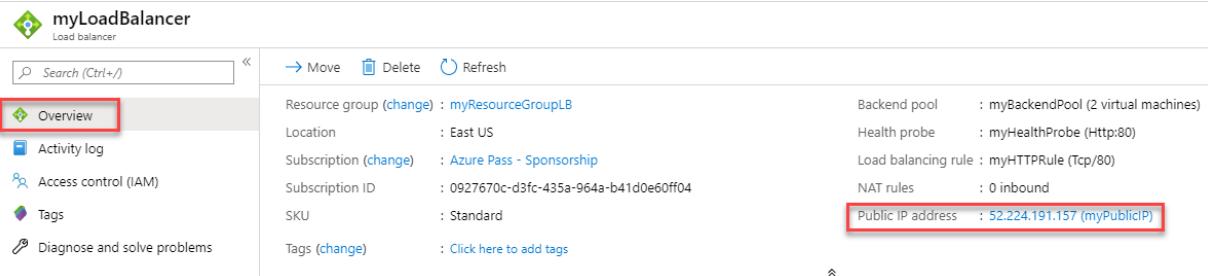
Floating IP (direct server return) ⓘ

Disabled  Enabled

3. Click **OK**.

### 29.1.8 Task 8: Test the load balancer

1. Find the public IP address for the Load Balancer on the **Overview** screen.



myLoadBalancer  
Load balancer

Search (Ctrl+F)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Move Delete Refresh

Resource group (change) : myResourceGroupLB

Location : East US

Subscription (change) : Azure Pass - Sponsorship

Subscription ID : 0927670c-d3fc-435a-964a-b41d0e60ff04

SKU : Standard

Tags (change) : Click here to add tags

Backend pool : myBackendPool (2 virtual machines)

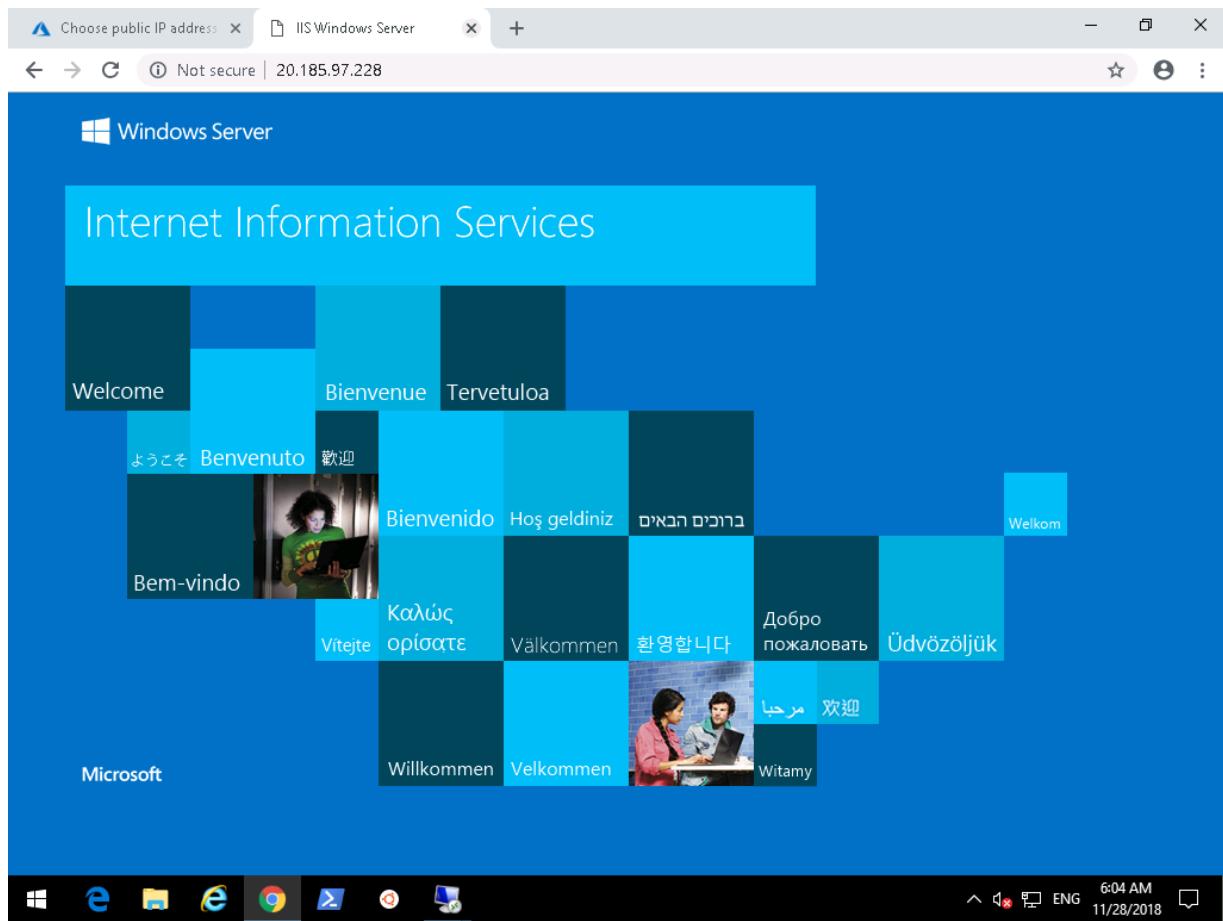
Health probe : myHealthProbe (Http:80)

Load balancing rule : myHTTPRule (Tcp/80)

NAT rules : 0 inbound

Public IP address : 52.224.191.157 (myPublicIP)

2. Copy the public IP address, and then paste it into the address bar of your browser. The default page of IIS Web server is displayed on the browser.



3. Notice the IIS default page loads.
4. In the Azure Portal click on **Virtual Machines** in the hub menu. Select myVM1 and in the **Overview** blade click **Stop** and confirm **Yes**.

| Resource group (change) : myResourceGroupLB |                                        |
|---------------------------------------------|----------------------------------------|
| Status                                      | : Running                              |
| Location                                    | : East US                              |
| Subscription (change)                       | : Azure Pass - Sponsorship             |
| Subscription ID                             | : 0927670c-d3fc-435a-964a-b41d0e60ff04 |

5. Wait until the myVM1 Virtual Machine has stopped then go back to the browser tab with the load balancer public IP and click refresh to confirm myVM2 is continuing to service the requests and the load balancer is functioning as expected.

## 29.2 Exercise 2: Load Balancer ARM Deployments

### 29.2.1 Task 1: Deploy an ARM template

This template allows you to create 2 Virtual Machines under a Load balancer and configure a load balancing rule on Port 80. This template also deploys a Storage Account, Virtual Network, Public IP address, Availability Set and Network Interfaces. In this template, we use the resource loops capability to create the network interfaces and virtual machines

1. In a new tab in your browser, navigate to the following URL <https://aka.ms/2E2MAjh>
2. Click **Deploy to Azure**

3. On the template blade that opens, enter the following details:

- Resource group: **myResourceGroupLB**
- Admin Username: **localadmin**
- Admin Password: **Pa55w.rd1234**

4. Click **I agree....** and click **Purchase**.

## 30 Exercise 3: Deploying Application Gateways

### 30.0.1 Task 1: Create an application gateway

A virtual network is needed for communication between the resources that you create. Two subnets are created in this example: one for the application gateway, and the other for the backend servers. You can create a virtual network at the same time that you create the application gateway.

1. First you need to create a subnet for the Application Gateway to reside in. Click **Virtual networks** on hub menu and select **myVNet**.

2. Click **Subnets** and click **+** **Subnet**.

myVnet - Subnets

Virtual network

Search (Ctrl+ /)

+ Subnet + Gateway subnet

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Address space

Connected devices

Subnets

Search subnets

| Name            | ↑↓ |
|-----------------|----|
| myBackendSubnet |    |

3. Enter **myAppGWSubnet** as the name and click **OK**.

**Add subnet** X

myVnet

Name \*  
 ✓

Address range (CIDR block) \* ⓘ  
 ✓  
10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

Add an IPv6 address space

Network security group

Route table

Service endpoints

Services ⓘ

Subnet delegation  
Delegate subnet to a service ⓘ

4. Click **Create a resource** found on the upper left-hand corner of the Azure portal.
5. Click **Networking** and then click **Application Gateway** in the Featured list.

## New

 Search the Marketplace

Azure Marketplace [See all](#)

Get started

Recently created

AI + Machine Learning

Analytics

Blockchain

Compute

Containers

Databases

Developer Tools

DevOps

Identity

Integration

Internet of Things

Media

Mixed Reality

IT & Management Tools

**Networking**

Software as a Service (SaaS)

Security

Storage

Web

Featured [See all](#)



Virtual network

[Quickstart tutorial](#)



Check Point CloudGuard IaaS R80.10

Cluster (preview)

[Learn more](#)



Load Balancer

[Learn more](#)



Application Gateway

[Learn more](#)



Front Door

[Learn more](#)



Firewall

[Learn more](#)



Virtual WAN

[Learn more](#)



Network security group

[Quickstart tutorial](#)



ExpressRoute

[Learn more](#)



Connection

[Learn more](#)

6. Enter these values for the application gateway basics blade then click **Next**:

- *myAppGateway* - for the name of the application gateway.
- *myResourceGroupLB* - select the already existing Resource Group.
- *myVnet* - select the already existing Virtual network.

## Create an application gateway

Basics    Frontends    Backends    Configuration    Tags    Review + create

An application gateway is a web traffic load balancer that enables you to manage traffic to your web application. [Learn more about application gateway](#)

**Project details**

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

Subscription \* ⓘ Azure Pass - Sponsorship

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

**Instance details**

Application gateway name \* myAppGateway

Region \* (US) East US

Tier ⓘ Standard V2

Enable autoscaling  Yes  No

Minimum autoscale instances \* ⓘ 0

Maximum autoscale instances 10

Availability zone ⓘ None

HTTP/2 ⓘ  Disabled  Enabled

**Configure virtual network**

Virtual network \* ⓘ myVnet [Create new](#)

- Under **Frontend configuration** blade, ensure **IP address type** is set to **public**, and under **Public IP address**, click **Create new**. Type **myAGPublicIPAddress** for the public IP address name and then click **OK**.

## Create an application gateway

✓ Basics   2 Frontends   3 Backends   4 Configuration   5 Tags   6 Review + create

Traffic enters the application gateway via its frontend IP address. An application gateway can use a public IP address, private IP address, or one of each type.

Frontend IP address type ⓘ  Public  Private  Both

Public IP address \*

Add a public IP address

Name \* myAGPublicIPAddress ✓

SKU \*  Basic  Standard

Assignment \*  Dynamic  Static

8. Click **Next**.
9. Select **+Add a backend pool**.
10. Enter the name **appGatewayBackendPool**. Under backend targets select **Virtual Machine** and add myVM1 and myVM2 virtual machines and their associated network interfaces then click **Add**.

## Add a backend pool

&gt;

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, IP addresses, or a valid Internet hostname.

Name \*  ✓

Add backend pool without targets Yes  No

Backend targets  
2 items

| Target type     | Target   |                                                |
|-----------------|----------|------------------------------------------------|
| Virtual machine | myvm1908 | <span style="font-size: 2em;">trash</span> ... |
| Virtual machine | myvm211  | <span style="font-size: 2em;">trash</span> ... |

IP address or hostname ▼

11. Click **Next**.
12. On the **Configuration** tab, you'll connect the frontend and backend pool you created using a routing rule.
13. Select **Add a rule** in the **Routing rules** column.
14. In the **Add a routing rule** window that opens, enter *myRoutingRule* for the **Rule name**.
15. A routing rule requires a listener. On the **Listener** tab within the **Add a routing rule** window, enter the following values for the listener:
  - **Listener name:** Enter *myListener* for the name of the listener.
  - **Frontend IP:** Select **Public** to choose the public IP you created for the frontend.Accept the default values for the other settings on the **Listener** tab, then select the **Backend targets** tab to configure the rest of the routing rule.

## Add a routing rule

&gt;

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name \*

myRoutingRule



Listener \*

Backend targets \*

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name \* ⓘ

myListener



Frontend IP \* ⓘ

Public



Protocol ⓘ

HTTP  HTTPS

Port \* ⓘ

80



### Additional settings

Listener type ⓘ

Basic  Multiple sites

Error page url

Yes  No

16. On the **Backend targets** tab, select **appGatewayBackendPool** for the **Backend target**.
17. For the **HTTP setting**, select **Add new** to create a new HTTP setting. The HTTP setting will determine the behavior of the routing rule. In the **Add an HTTP setting** window that opens, enter *myHTTPSetting* for the **HTTP setting name**. Accept the default values for the other settings in the **Add an HTTP setting** window, then select **Add** to return to the **Add a routing rule** window.

## Add an HTTP setting

X

[← Save changes and go back to routing rules](#)

HTTP setting name \*  ✓

Backend protocol  HTTP  HTTPS

Backend port \*  ✓

### Additional settings

Cookie-based affinity  ⓘ   Enable  Disable

Connection draining  ⓘ   Enable  Disable

Request time-out (seconds)  
\*  ⓘ   ✓

Override backend path  ⓘ   ✓

### Host name

By default, Application Gateway does not change the incoming HTTP host header from the client and sends the header unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header.

Override with new host name  Yes  No

Host name override  Pick host name from backend target  
 Override with specific domain name

e.g. contoso.com

Create custom probes  Yes  No

**Add**

**Cancel**

18. On the **Add a routing rule** window, select **Add** to save the routing rule and return to the **Configuration** tab.

## Add a routing rule

X

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name \*

myRoutingRule



Listener \* Backend targets \*

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

appGatewayBackendPool



Backend target \* ⓘ

Create new

myHTTPSetting



HTTP setting \* ⓘ

Create new

### Path-based routing

You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of HTTP settings based on the URL path.

| Path                             | Path rule name | HTTP setting | Backend Pool |
|----------------------------------|----------------|--------------|--------------|
| No additional targets to display |                |              |              |

[Add multiple targets to create a path-based rule](#)

19. Select **Add**

20. Select **Next: Tags** and then **Next: Review + create**, then select **Create**.

### 30.0.2 Task 2: Test the application gateway

- Find the public IP address for the application gateway on the Overview screen. Click **All resources** and then click **myAGPublicIPAddress**.

myAppGateway  
Application Gateway

Search (Ctrl+ /)

Move Delete

Updating

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource group (change) : myResourceGroupLB

Location : East US

Subscription (change) : Azure Pass - Sponsorship

Subscription ID : 0927670c-d3fc-435a-964a-b41d0e60ff04

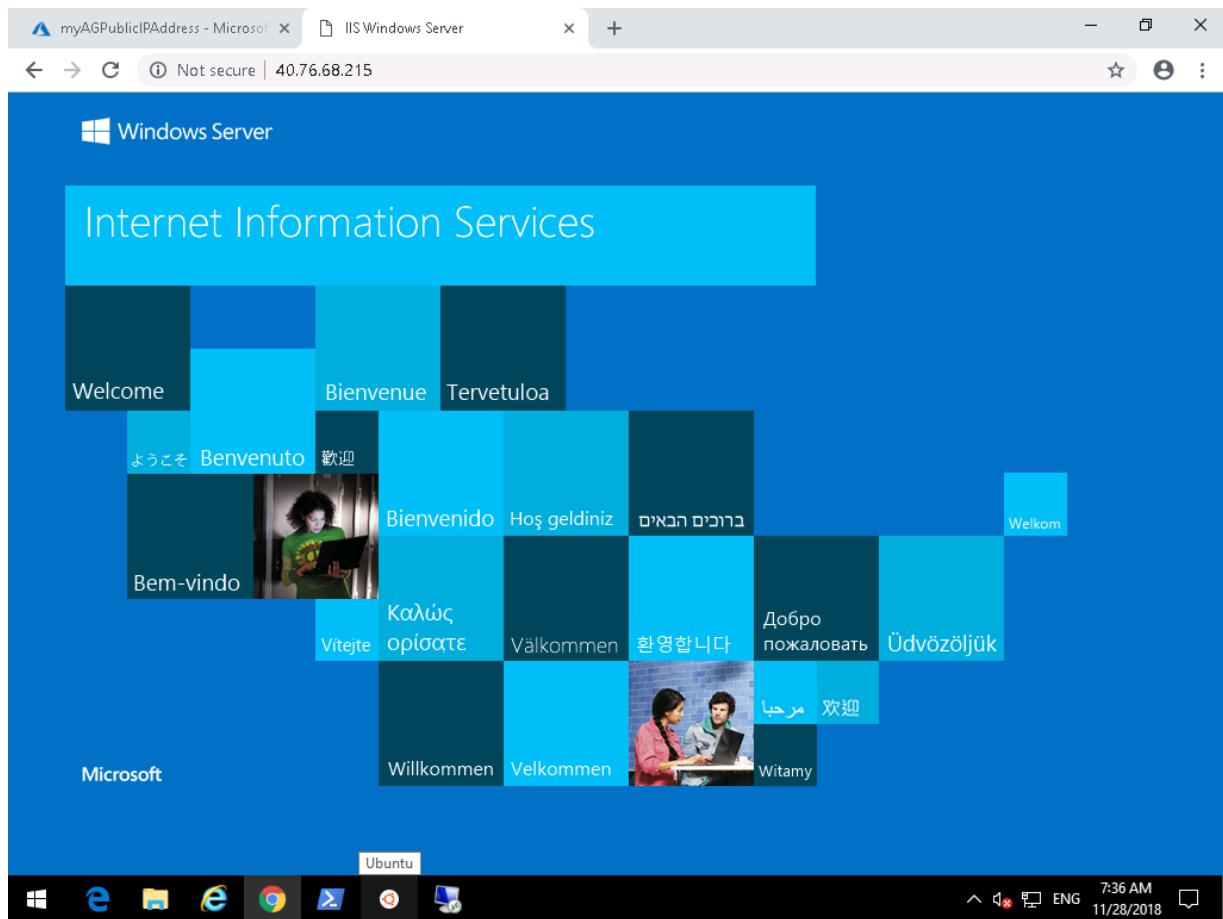
Tier : Standard V2

Virtual network/subnet : myVnet/myAppGWSubnet

Frontend private IP addr... : -

Frontend public IP addr... : 52.188.140.128 (myAGPublicIPAddress)

- Copy the public IP address, and then paste it into the address bar of your browser.



3. To verify, go to Network Watcher, choose Topology then choose myResourceGroupLB to see the overall network diagram.

---

**WARNING:** Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Results**:

**Results:** You have now completed this lab.

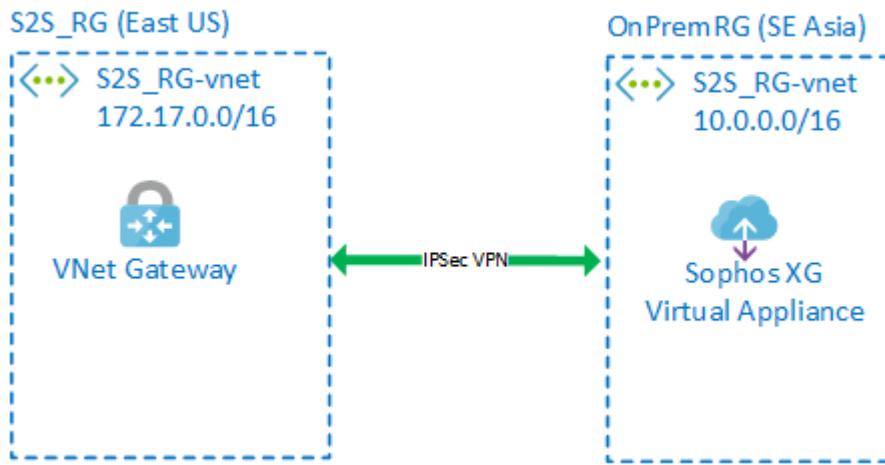
---

## 31 Module 2: Lab 11: On-Prem to Azure Connections - VPN Gateways and Tunnelling

### 31.1 Exercise 1: Deploy Virtual Appliances and Gateways for intersite connectivity.

#### 31.1.1 Task 1: Deploy a Virtual Appliance.

In this task you will create a Sophos XG Virtual Appliance which will emulate an on-premises device. The layout of this is depicted in the diagaram below



1. In your browser, navigate to the following URL to open the ARM template:

<https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2F>

2. Login to the portal if required.
3. On the Custom deployment enter or select the following details:

| Setting        | Value                      |
|----------------|----------------------------|
| Resource Group | Create New <b>OnPremRG</b> |
| Location       | <b>Southeast Asia</b>      |
| Admin Password | <b>Pa55w.rd1234</b>        |
| Public IP DNS  | <i>Enter a unique name</i> |
| Storage Name   | <i>Enter a unique name</i> |

4. Scroll to the bottom of the blade and click the check box next to I agree to the terms and conditions..... and click **Purchase**.

### 31.1.2 Task 2: Create a Resource Group and VNet.

In this task you will create a Virtual Machine and a Virtual Network inside a new Resource group which will be used to connect to your emulated On-Prem environment.

1. Login to your Azure Portal <https://portal.azure.com>
2. Click **Create a resource > Networking > Virtual Network**
3. Change the values in the **Create virtual network** blade change the values to be the same as the output below:
  - **Name** S2S\_RG-vnet
  - **Resource group** Create New: S2S\_RG
  - **Location:** East US

Click the IP Addresses tab and enter the following values:

- **Address space** 172.17.0.0/16
- **Subnet address range** 172.17.0.0/24

4. Click **Create**. **Note:** You can continue to the next task without having to wait for the deployment to complete.

### 31.1.3 Task 3: Create a Gateway Subnet and a Virtual network Gateway.

In this task you will Create a Gateway Subnet and a Virtual network Gateway which will enable you to create a connection between On-Prem and your Azure VNet.

1. In the Azure Portal click **Resource Groups** on the Hub Menu.
2. Click the **S2S\_RG** resource group that has been created for you.

3. In the S2S\_RG Resource Group blade click the **S2S\_RG-vnet**.

4. On the **S2S\_RG-vnet** menu click **Subnets**.

5. Click **+ Gateway subnet**.

**Note:** You need to create a Gateway subnet for the Gateway machines to reside in. All the routing is done by the Azure Software Defined Networking.

6. Leave the default options on the **Add subnet** blade and click **OK**.

7. Click **+ Create a resource**.

8. Search for Virtual Network Gateway and select **Virtual network gateway**.

9. Click **Create**.

10. On the **Create virtual network gateway** blade enter the following information:

- **Name:** S2S-GW
- **Name:** (US) East US
- **Gateway type:** VPN
- **VPN Type:** Route-based
- **SKU:** Basic
- **Virtual network:** Select the S2S\_RG-vnet (this was created earlier when you deployed the VM)
- **Public IP address:** (Create New) Name: S2S-GW-PIP

## Create virtual network gateway

### Project details

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

\* Subscription

Azure Pass - Sponsorship

Resource group 

S2S\_RG (derived from virtual network's resource group)

### Instance details

\* Name

S2S-GW 

\* Region

(US) East US

\* Gateway type 

VPN  ExpressRoute

\* VPN type 

Route-based  Policy-based

\* SKU 

Basic

 Only virtual networks in the currently selected subscription and region are listed.

### VIRTUAL NETWORK

\* Virtual network 

S2S\_RG-vnet

Gateway subnet address range

172.17.1.0/24

### Public IP address

\* Public IP address 

Create new  Use existing

\* Public IP address name

S2S-GW-PIP 

Public IP address SKU

Basic

\* Assignment

Dynamic  Static

**Review + create**

< Previous

Next : Tags >

Download a template for automation

11. Click **Review + create** then on the summary screen click **Create**

**Note:** The gateway may take up to 45 minutes to deploy, although in most cases it is much quicker. Monitor this by clicking on the Bell Icon. You can continue to the next task whilst the Gateway is deploying.

### 31.1.4 Task 4: Configure the Sophos virtual appliance.

1. On the Azure Portal Hub menu click **Resource Groups**.
2. Select the **OnPremRG** Resource Group.
3. Select the **PublicIP** Resource.

OnPremRG

Subscription (change)  
Azure Pass - Sponsorship

Subscription ID  
f155263b-b8c7-4a72-965a-930e06f2a5fe

Tags (change)  
Click here to add tags

Deployments  
9 Succeeded

| NAME            | TYPE                   | LOCATION       |
|-----------------|------------------------|----------------|
| AvailabilitySet | Availability set       | Southeast Asia |
| myOnPremFW      | Virtual machine        | Southeast Asia |
| myonpremstorage | Storage account        | Southeast Asia |
| PortA           | Network interface      | Southeast Asia |
| PortB           | Network interface      | Southeast Asia |
| PublicIP        | Public IP address      | Southeast Asia |
| SecurityGroup   | Network security group | Southeast Asia |
| VNET            | Virtual network        | Southeast Asia |

4. Make a note of the assigned Public IP address.

PublicIP

Resource group (change)  
OnPremRG

Location  
Southeast Asia

Subscription (change)  
Azure Pass - Sponsorship

Subscription ID  
f155263b-b8c7-4a72-965a-930e06f2a5fe

SKU  
Basic

IP address  
**13.76.228.200**

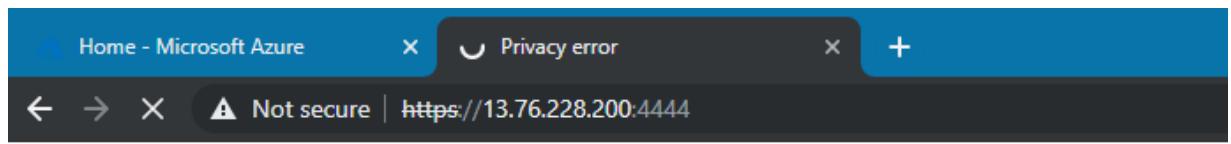
DNS name  
myonpremgw.southeastasia.cloudapp.azure.com

Associated to  
PortB

Virtual machine  
myOnPremFW

Tags (change)  
Click here to add tags

5. Open a new browser session and navigate to <https://x.x.x.x:4444> (where x.x.x.x is the public IP address you noted above).
6. Depending on your browser there may be different options to proceed with the connection. Select Details then Go to web page (not recommended)



## Your connection is not private

Attackers might be trying to steal your information (passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID



[Hide advanced](#)

This server could not prove that it is **13.76.228.200**. Your computer's operating system. This may be caused by an attacker intercepting your connection.

[Proceed to 13.76.228.200 \(unsafe\)](#)

7. Log into the Firewall with the following credentials:

- Admin
- Pa55w.rd1234

8. Accept the licence agreement.

9. On the Register your firewall page click **I don't have a serial number (start a trial)** and select **I do not want to register now** then click **Continue**.

The screenshot shows the Sophos Firewall registration interface. It includes fields for entering an existing serial number or starting a trial, and options for migrating UTM 9 licenses or skipping registration. A red box highlights the 'Serial Number' field in the 'License Schedule' section of the portal, which contains the value 'C160703HBRQMRCE'. A blue arrow points from the registration form to this specific field.

10. On the Warning pop up click **Continue**.
11. Return back to the Azure Portal. Open the **S2S\_RG** Resource Group and select the **S2S-GW-PIP** Public IP and make a note of it.

**Note:** This is your Public IP you will connect your Sophos virtual appliance to via IPSec VPN. If the IP Address field is empty, continue to wait for the template deployment to complete, periodically checking the deployment status and refreshing the **S2S-GW-PIP** blade.

The screenshot shows the Azure Resource Group Overview page for 'S2S\_RG'. It displays details such as Location (East US), Subscription (Azure Pass - Sponsorship), and a Public IP address of 40.85.178.89. The IP address field is highlighted with a red box.

| SKU             | Basic        |
|-----------------|--------------|
| IP address      | 40.85.178.89 |
| DNS name        | -            |
| Associated to   | S2S-GW       |
| Virtual machine | -            |

12. Return back to the Sophos Portal.
13. Go to **VPN > IPsec Connections**, select **Add** and configure the following settings: *If in doubt see the screenshots below*

#### General Settings Section:

- **Name:** On\_Prem\_to\_Azure
- **IP Version:** IPv4.
- **Activate on Save:** Selected.
- **Create firewall rule:** Selected.
- **Description:** Site to Site connection from On Prem to Azure VNet.
- **Connection Type:** Site-to-Site.
- **Gateway Type:** Respond Only.

## General settings

|                                                                                                 |                                                                                |                                                                                                                  |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Name<br><input type="text" value="On_Prem_to_Azure"/>                                           | IP version<br><input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 | <input checked="" type="checkbox"/> Activate on save<br><input checked="" type="checkbox"/> Create firewall rule |
| Description<br><input type="text" value="Site to Site connection from On Prem to Azure VNet."/> | Connection type<br><input type="text" value="Site-to-site"/>                   | Gateway type<br><input type="text" value="Respond only"/>                                                        |

## Encryption Section:

- **Policy:** Microsoft Azure.
- **Authentication Type:** Preshared Key.
- **Preshared Key:** 123456789
- **Repeat Preshared Key:** 123456789

## Encryption

|                                                            |                                                                   |
|------------------------------------------------------------|-------------------------------------------------------------------|
| Policy<br><input type="text" value="Microsoft Azure"/>     | Authentication type<br><input type="text" value="Preshared key"/> |
| Preshared key<br><input type="text" value="....."/>        |                                                                   |
| Repeat preshared key<br><input type="text" value="....."/> |                                                                   |

## Gateway Settings Section:

- **Listening Interface:** Select the default.
- **Gateway Address:** Input the public IP of the Azure VPN gateway noted earlier.
- **Local ID:** IP Address.
- **Remote ID:** IP Address.
- **Local ID:** Enter the public IP of the on-premises Sophos XG Firewall.
- **Remote ID:** Input the public IP of the Azure VPN gateway that you noted earlier.
- **Local Subnet:** Enter the local subnet of 10.0.0.0 /16 (255.255.0.0)

|                                                                                                                                          |                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>Add IP host</b>                                                                                                                       |                                                                                  |
| Name *<br><input type="text" value="On Prem"/>                                                                                           | IP version *<br><input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| Type *<br><input type="radio"/> IP <input checked="" type="radio"/> Network <input type="radio"/> IP range <input type="radio"/> IP list | IP address *<br><input type="text" value="10.0.0.0"/>                            |
| IP host group<br><input type="text"/>                                                                                                    | Subnet<br><input type="text" value="/16 (255.255.0.0)"/>                         |
| <input type="button" value="Add new item"/>                                                                                              |                                                                                  |
| <input type="button" value="Save"/> <input type="button" value="Cancel"/>                                                                |                                                                                  |

- **Remote Subnet:** Enter the remote subnet 172.17.0.0 /16 (255.255.0.0)

**Add IP host**

|                                                                           |                                                                                                                                |        |                   |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------|-------------------|
| Name *                                                                    | Azure                                                                                                                          |        |                   |
| IP version *                                                              | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6                                                               |        |                   |
| Type *                                                                    | <input type="radio"/> IP <input checked="" type="radio"/> Network <input type="radio"/> IP range <input type="radio"/> IP list |        |                   |
| IP address *                                                              | 172.17.0.0                                                                                                                     | Subnet | /16 [255.255.0.0] |
| IP host group                                                             | <input type="button" value="Add new item"/>                                                                                    |        |                   |
| <input type="button" value="Save"/> <input type="button" value="Cancel"/> |                                                                                                                                |        |                   |

1. **Advanced:** leave the default settings.
2. Upon clicking **Save**, the IPsec connection is activated.

**Note:** Do not click on the button under the **Connection** column as it will override the configuration settings set on the IPsec connection (**Gateway type: Respond only**). This is to avoid issues since Azure must initiate the tunnel.

### 31.1.5 Task 5: Creating Azure connection.

In this task you will create a connection on your Azure Gateway to the On-Prem firewall and establish the connection.

1. Click on **Resource Groups** on the **Hub Menu**.
2. Select the **S2S\_RG** Resource Group.
3. Select your **S2S-GW** Gateway.
4. Click **Connections** from the S2S-GW menu.
5. Click **Add**.
6. Enter the following information in the **Add connection** blade:
  - **Name:** GWConnection
  - **Connection type:** Site-to-site (IPSec)
  - **Virtual Network Gateway:** S2S-GW
7. Click the **Local network gateway**
8. Click **Create new**.
9. Enter the following information in the **Create local network gateway** blade:
  - **Name:** OnPremGW
  - **IP address:** *Enter your IP address of your Sophos on prem firewall you recorded earlier*
  - **Address space:** 10.0.0.0/16 (*Note: This is the IP range of your On-Prem servers*)

10. Click **OK**.
  11. In the **Shared key (PSK)** box enter 123456789 then click **OK**.
- Note:** This key is just for this lab. In the real world you would use something with greater complexity.
12. Refresh the page and the connection should be established.
- Note:** It may take 30 seconds to establish the connection. If the connection still fails to connect, return to the Sophos Portal and click

The screenshot shows the Azure portal interface for managing connections. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area is titled 'S2S-GW - Connections' under 'Virtual network gateway'. It has a search bar and a 'Add' button. A table lists connections with columns for NAME, STATUS, and CONNECTION TYPE. One row shows 'GWConnection' with 'Connected' highlighted in a red box. The 'STATUS' column has a dropdown set to 'Active'.

**Note:** If the connection still fails to connect, return to the Sophos Portal and click the red/orange icon to force the connection to be established.

The screenshot shows the Sophos Firewall interface for managing site-to-site connections. It has filters for Policy, Connection type, Status (set to Active), and Connection. A table lists connections with columns for Microsoft Azure and Site-to-site. The 'Site-to-site' connection has a status indicator that is red, indicating it is disconnected. A red arrow points to this indicator.

**WARNING:** Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**

**Results:** You have now completed this lab.

## 32 Module 2: Lab 12 - Azure Firewall

### Scenario

Controlling outbound network access is an important part of an overall network security plan. For example, you may want to limit access to web sites, or the outbound IP addresses and ports that can be accessed.

One way you can control outbound network access from an Azure subnet is with Azure Firewall. With Azure Firewall, you can configure:

- Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
- Network rules that define source address, protocol, destination port, and destination address.

Network traffic is subjected to the configured firewall rules when you route your network traffic to the firewall as the subnet default gateway.

### 32.1 Exercise 1: Deploy an Azure Firewall

#### 32.1.1 Task 1: Lab Setup

1. In your browser, navigate to the following URL to open the ARM template:

<https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2F>

2. Click **Create new** under the Resource Group and use the resource group name of **Test-FW-RG**
3. Select the location of **East US**
4. Leave all the other fields as the pre-populated defaults
5. Select the I agree.... check box and click **Purchase** and wait for the deployment to complete.

This lab setup template will set up the following resources for the lab

| Name              | Type                   | Location |
|-------------------|------------------------|----------|
| azureFirewalls-ip | Public IP address      | East US  |
| Firewall-route    | Route table            | East US  |
| Srv-Jump          | Virtual machine        | East US  |
| Srv-Jump_OsDisk   | Disk                   | East US  |
| srv-jump121       | Network interface      | East US  |
| Srv-Jump-nsg      | Network security group | East US  |
| Srv-Jump-PIP      | Public IP address      | East US  |
| Srv-Work          | Virtual machine        | East US  |
| Srv-Work_OsDisk_1 | Disk                   | East US  |
| srv-work267       | Network interface      | East US  |
| Srv-Work-nsg      | Network security group | East US  |
| Test-FW-VN        | Virtual network        | East US  |

### 32.1.2 Task 2: Deploy the firewall

In this task you will deploy the Azure firewall into the VNet.

1. In the Azure portal, click **All services** and search for and select **Firewalls**.

The screenshot shows the Microsoft Azure portal's 'All services' blade. On the left is a navigation sidebar with 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The main area has a search bar at the top with 'Firewall' typed in. Below it, there are two tabs: 'Overview' and 'Firewalls'. The 'Firewalls' tab is highlighted with a red box. Underneath are sections for 'Categories' and 'All'.

2. On the **Firewalls** blade click **Create firewall**.

The screenshot shows the 'Firewalls' blade in the Azure portal. The left sidebar includes 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', and 'Azure Active Directory'. The main area shows a table with columns for Name, Type, Resource group, and Location, all currently sorted by Name. A large cloud icon is in the center. At the bottom, a message says 'No firewalls to display' and 'Cloud-native network security to protect your Azure Virtual Network resources [Learn more](#)'. A prominent red box surrounds the blue 'Create firewall' button at the bottom right.

3. On the **Create a Firewall** blade, use the following table to configure the firewall:

| Setting        | Value                           |
|----------------|---------------------------------|
| Subscription   | <i>your subscription</i>        |
| Resource group | <b>Use existing:</b> Test-FW-RG |
| Name           | Test-FW01                       |
| Location       | East US                         |

| Setting                  | Value                                                                            |
|--------------------------|----------------------------------------------------------------------------------|
| Choose a virtual network | <b>Use existing:</b> Test-FW-VN                                                  |
| Public IP address        | <b>Add new.</b> TEST-FW-PIP The Public IP address must be the Standard SKU type. |

### Create a firewall

\* Subscription: Azure Pass - Sponsorship

\* Resource group: Test-FW-RG  
Create new

**INSTANCE DETAILS**

\* Name: Test-FW01

\* Region: (US) East US

Choose a virtual network:  Create new  Use existing

Virtual network: Test-FW-VN (Test-FW-RG)

**PUBLIC IP ADDRESS**

\* Public IP address:  Create new  Use existing

\* Public IP address name: Test-FW-PIP

Public IP address SKU: Standard

4. Click **Review + create**.

5. Review the summary, and then click **Create** to create the firewall.

## Create a firewall

**i Validation passed**

Basics Tags Review + create

Summary

Basics

|                   |                          |
|-------------------|--------------------------|
| Subscription      | Azure Pass - Sponsorship |
| Resource group    | Test-FW-RG               |
| Region            | (US) East US             |
| Virtual network   | Test-FW-VN               |
| Address space     | 10.0.0.0/16              |
| Public IP address | Test-FW-PIP              |

---

[Create](#) [Previous](#) [Next](#) [Download a template for .](#)

This will take a few minutes to deploy.

6. After the deployment completes, go to the **Test-FW-RG** resource group, and click the **Test-FW01** firewall.
7. Make a note of the **Private IP** address. You'll use it later when you create the default route.

[Delete](#) [Lock](#)

---

|                                                                           |                                                    |
|---------------------------------------------------------------------------|----------------------------------------------------|
| Resource group ( <a href="#">change</a> )<br>Test-FW-RG                   | Virtual network/subnet<br>Test-FW-VN/AzureFirewall |
| Location<br>East US                                                       | Private IP address<br>10.0.1.4                     |
| Subscription ( <a href="#">change</a> )<br>Azure Pass - Sponsorship       | Public IP address<br>Test-FW-PIP                   |
| Subscription ID<br>2fb8fe99-e79a-4f40-a05b-735eadca7bc9                   | Provisioning state<br>Succeeded                    |
| Tags ( <a href="#">change</a> )<br><a href="#">Click here to add tags</a> |                                                    |

### 32.1.3 Task 3: Create a default route

For the **Workload-SN** subnet, configure the outbound default route to go through the firewall.

1. From the Azure portal home page, click **All services**.
2. Under **Networking**, click **Route tables**.
3. Click **Add**.
4. For **Name**, type **Firewall-route**.
5. For **Subscription**, select your subscription.
6. For **Resource group**, select **Use existing**, and select **Test-FW-RG**.
7. For **Location**, select **East US**.
8. Click **Create**.
9. Click **Refresh**, and then click the **Firewall-route** route table.
10. Click **Subnets > Associate**.
11. Click **Virtual network > Test-FW-VN**.
12. For **Subnet**, click **Workload-SN**. Make sure that you select only the **Workload-SN** subnet for this route, otherwise your firewall won't work correctly.
13. Click **OK**.
14. Click **Routes > Add**.
15. For **Route name**, type **FW-DG**.
16. For **Address prefix**, type **0.0.0.0/0**
17. For **Next hop type**, select **Virtual appliance**.

Azure Firewall is actually a managed service, but virtual appliance works in this situation.

18. For **Next hop address**, type the private IP address for the firewall that you noted previously.
19. Click **OK**.

#### **32.1.4 Task 4: Configure an application rule**

In this task you will create an application rule that allows outbound access to `msn.com`.

1. Open the **Test-FW-RG** resource group and click the **Test-FW01** firewall.
2. On the **Test-FW01** page, under **Settings** section, click **Rules**.
3. Click the **Application rule collection** tab.
4. Click **Add application rule collection**.
5. For **Name**, type **App-Coll01**.
6. For **Priority**, type **200**.
7. For **Action**, select **Allow**.
8. Under **Rules**, **Target FQDNs**, for **Name**, type **AllowGH**.
9. For **Source Addresses**, type **10.0.2.0/24**.
10. For **Protocol:port**, type **http, https**.
11. For **Target FQDNs**, type **msn.com**
12. Click **Add**.

Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes.

### **32.1.5 Task 5: Configure a network rule**

In this task you will create a network rule that allows outbound access to two IP addresses on port 53 (DNS).

1. Click the **Network rule collection** tab.
2. Click **Add network rule collection**.
3. For **Name**, type **Net-Coll01**.
4. For **Priority**, type **200**.
5. For **Action**, select **Allow**.
6. Under **Rules** in the **IP Addresses** section, for **Name**, type **AllowDNS**.
7. For **Protocol**, select **UDP**.
8. For **Source Addresses**, type **10.0.2.0/24**.
9. For Destination address, type **209.244.0.3,209.244.0.4**
10. For **Destination Ports**, type **53**.
11. Click **Add**.

### **32.1.6 Task 6: Change the primary and secondary DNS address for the Srv-Work network interface**

For testing purposes in this tutorial, you configure the primary and secondary DNS addresses. This isn't a general Azure Firewall requirement.

1. From the Azure portal, open the **Test-FW-RG** resource group.
2. Click the network interface for the **Srv-Work** virtual machine.
  1. Under **Settings**, click **Networking**.
  2. Select the NIC
3. Under **DNS servers**, click **Custom**.
4. Type **209.244.0.3** in the **Add DNS server** text box, and **209.244.0.4** in the next text box.
5. Click **Save** and wait until it has successfully saved..
6. Restart the **Srv-Work** virtual machine.

### **32.1.7 Task 7: Test the firewall**

In this task you will test the firewall to confirm that it works as expected.

1. From the Azure portal, review the network settings for the **Srv-Work** virtual machine and note the private IP address.
  2. Connect to the **Srv-Jump** virtual machine using RDP, and from there open a remote desktop connection to the **Srv-Work** private IP address.
    - **Username:** localadmin
    - **Password:** Pa55w.rd1234
  3. Open Internet Explorer and browse to <https://www.msn.com>
  4. Click **OK > Close** on the security alerts.
- You should see the MSN home page.
5. Browse to <https://msn.com>
    - You should be blocked by the firewall.
    - So now you've verified that the firewall rules are working:
      - You can browse to the one allowed FQDN, but not to any others.
      - You can resolve DNS names using the configured external DNS server.
  6. To troubleshoot, go to **Network Watcher**, choose **Topology** then choose **TEST-FW-RG** to see the overall network diagram.

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

**Results:** You have now completed this lab.

## 33 Module 2 - Implement Platform Protection

### 33.1 Lab 13 - Secure Admin Access

SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections. SSH is the default connection protocol for Linux VMs hosted in Azure. Although SSH itself provides an encrypted connection, using passwords with SSH connections still leaves the VM vulnerable to brute-force attacks or guessing of passwords. A more secure and preferred method of connecting to a VM using SSH is by using a public-private key pair, also known as SSH keys.

- The public key is placed on your Linux VM, or any other service that you wish to use with public-key cryptography.
- The private key on your local system is used by an SSH client to verify your identity when you connect to your Linux VM. Protect this private key. Do not share it.
- Depending on your organization's security policies, you can reuse a single public-private key pair to access multiple Azure VMs and services. You do not need a separate pair of keys for each VM or service you wish to access.

Your public key can be shared with anyone, but only you (or your local security infrastructure) should possess your private key.

### 33.2 Exercise 1: Deploy and connect to an Azure VM securely.

#### 33.2.1 Task 1: Create SSH keys with PuTTYgen

1. Open a browser and navigate to the following URL:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

2. Download and install the **Putty Installer**.

#### Download PuTTY: latest release (0.70)

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#) | [Keys](#) | [Links](#) | [Team](#)  
Download: **Stable** · [Snapshot](#) | [Docs](#) | [Changes](#) | [Wishlist](#)

This page contains download links for the latest released version of PuTTY. Currently this is 0.70, released on 2017-07-08.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a [permanent link to the 0.70 release](#).

Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date version of the code available. If you have a problem with this release, then it might be worth trying out the [development snapshots](#), to see if the problem has already been fixed in those versions.

**Package files**

You probably want one of these. They include all the PuTTY utilities.  
(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

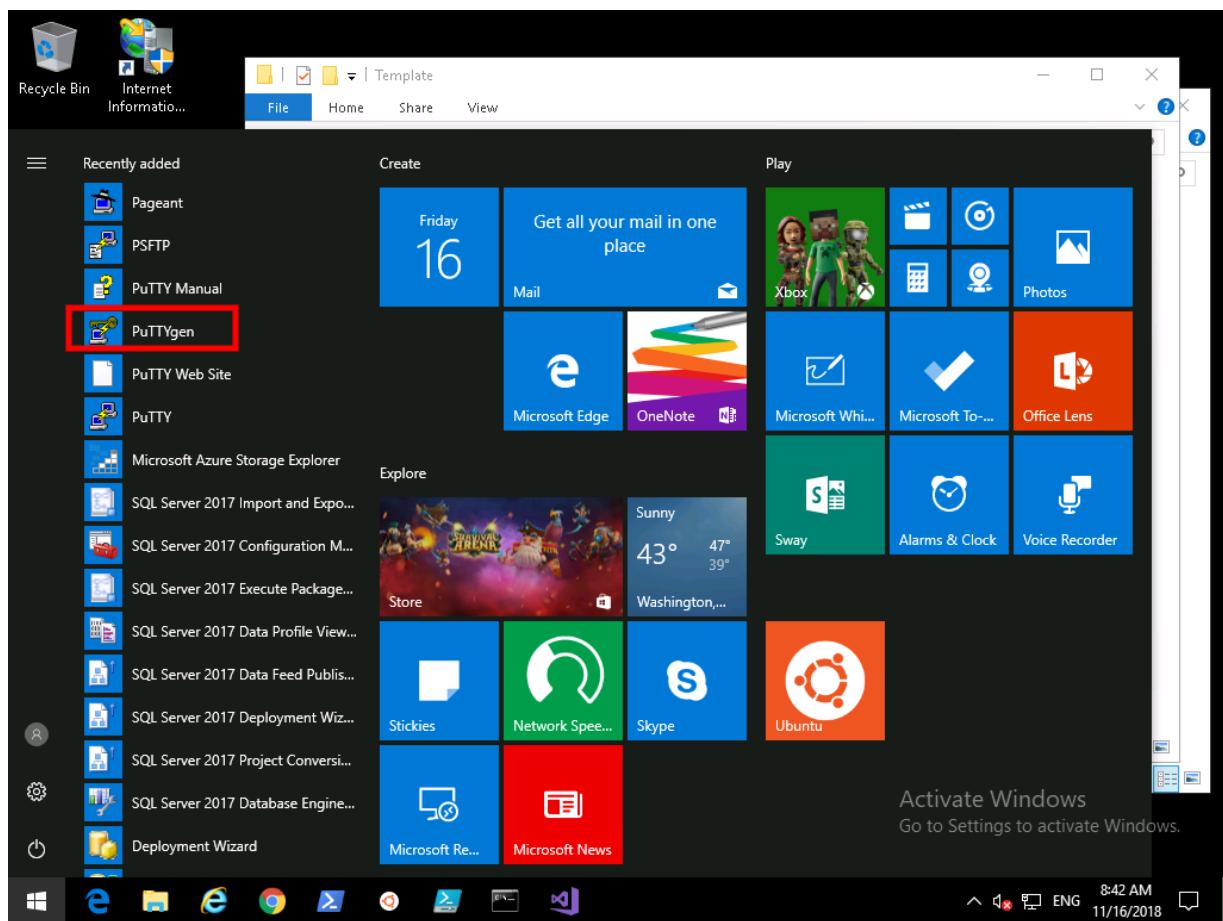
**MSI ("Windows Installer")**

|         |                                                |                              |                               |
|---------|------------------------------------------------|------------------------------|-------------------------------|
| 32-bit: | <a href="#">putty-0.70-installer.msi</a>       | (or by <a href="#">FTP</a> ) | ( <a href="#">signature</a> ) |
| 64-bit: | <a href="#">putty-64bit-0.70-installer.msi</a> | (or by <a href="#">FTP</a> ) | ( <a href="#">signature</a> ) |

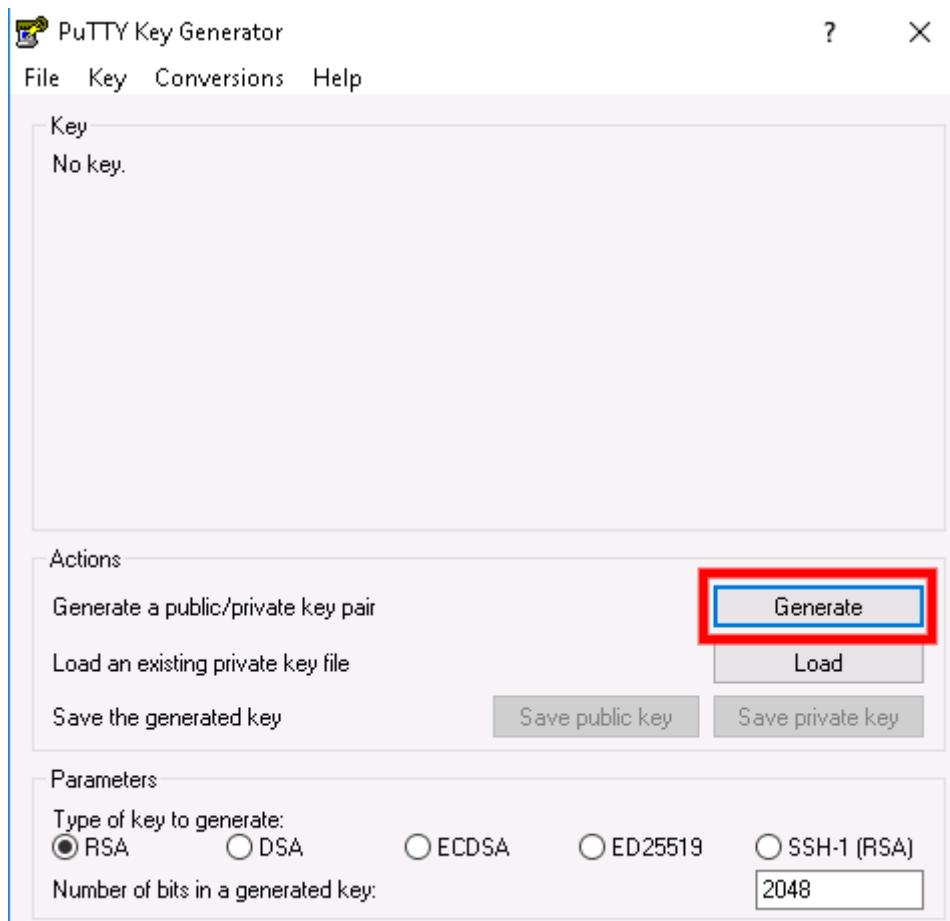
**Unix source archive**

|          |                                   |                               |                               |
|----------|-----------------------------------|-------------------------------|-------------------------------|
| .tar.gz: | <a href="#">putty-0.70.tar.gz</a> | ( <a href="#">or by FTP</a> ) | ( <a href="#">signature</a> ) |
|----------|-----------------------------------|-------------------------------|-------------------------------|

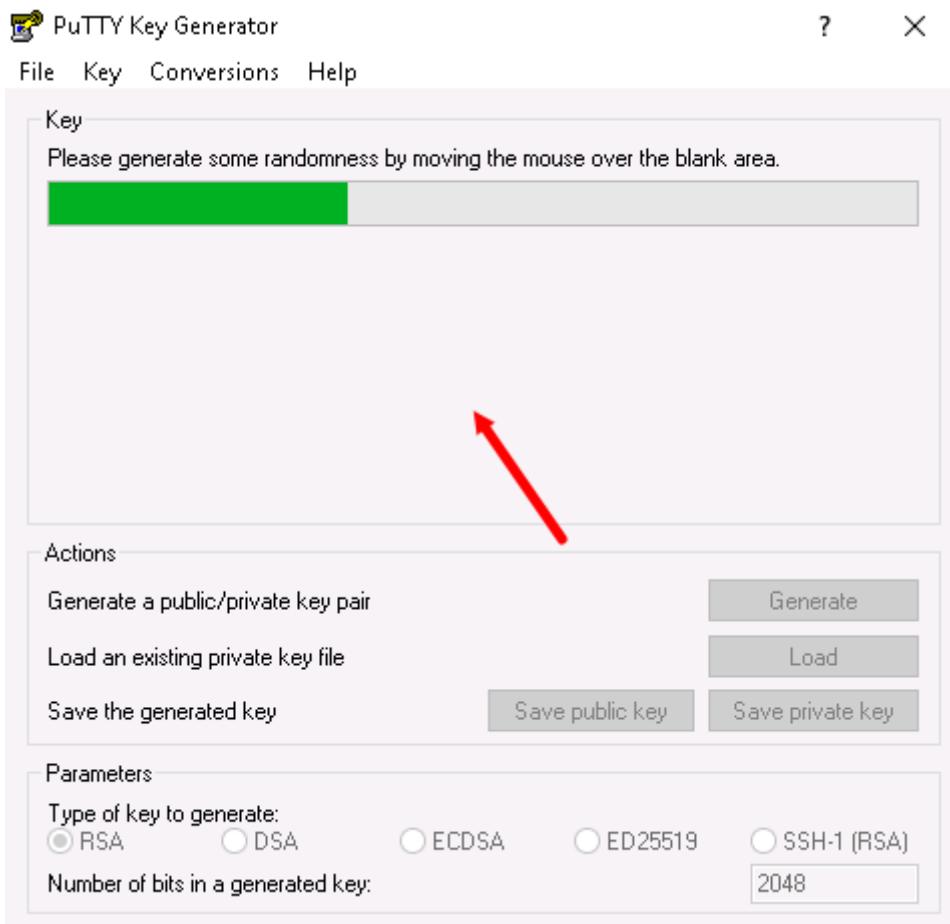
3. Click **Start** and navigate to **PuTTYgen**.



- Click Generate. By default PuTTYgen generates a 2048-bit SSH-2 RSA key.



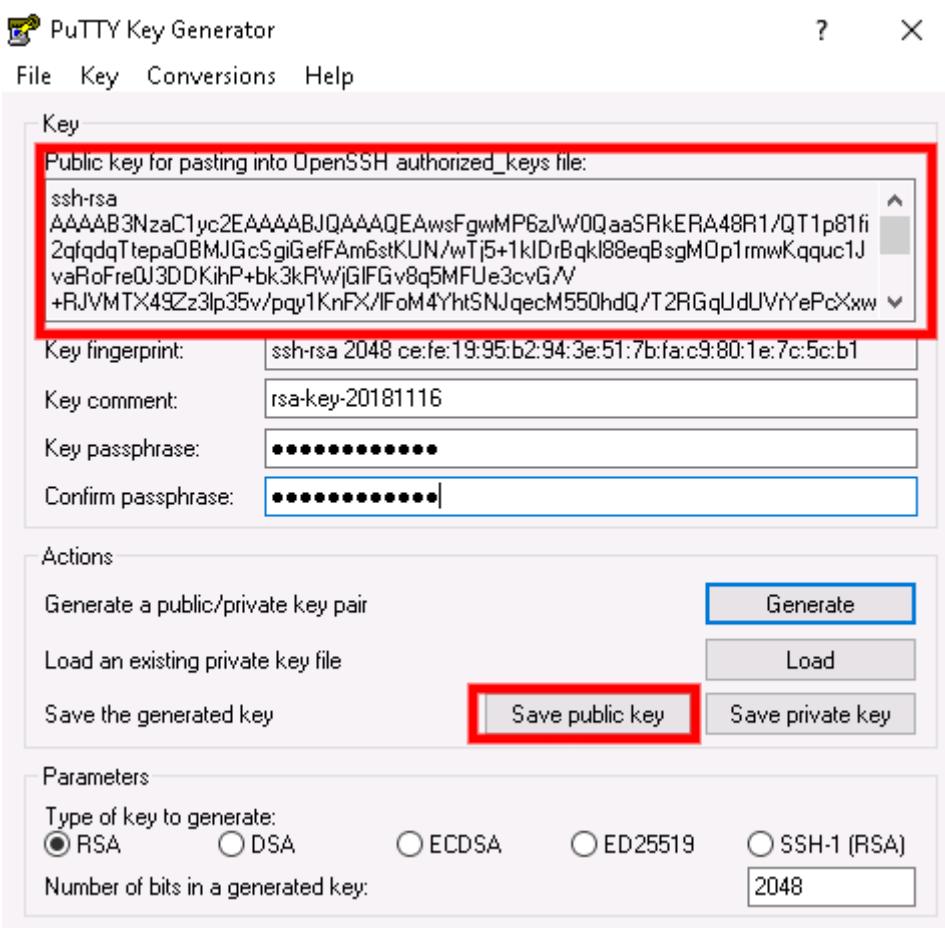
- Move the mouse around in the blank area to provide randomness for the key.



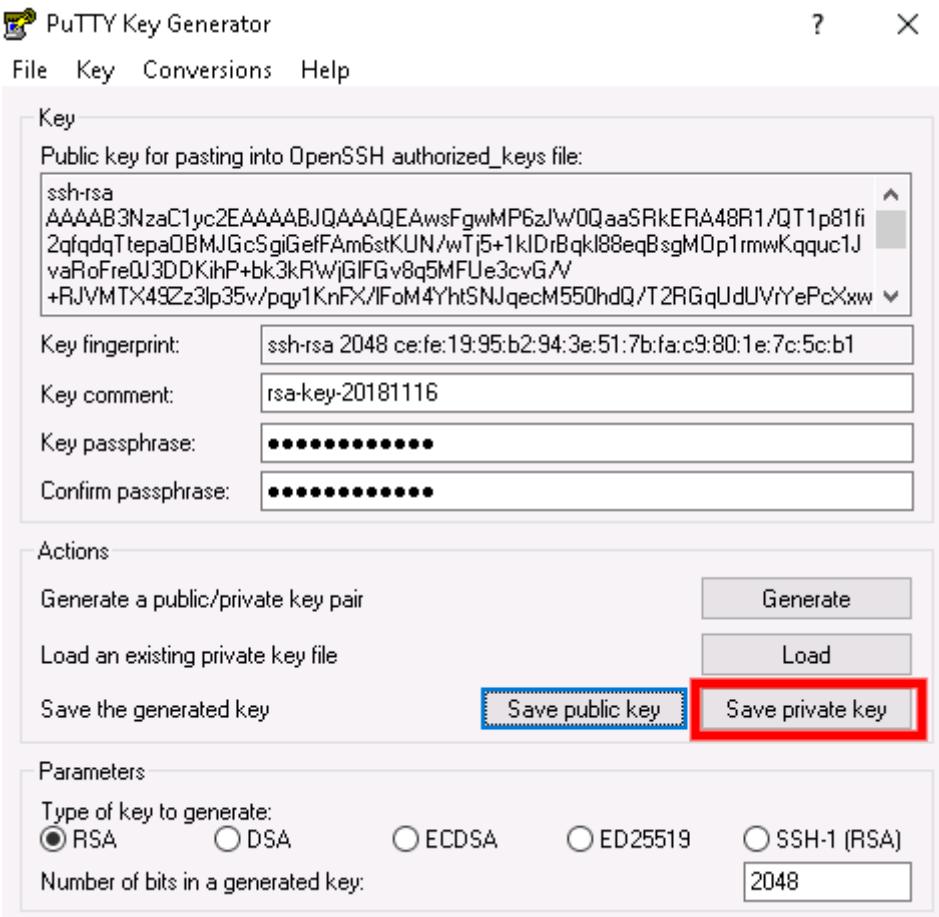
- After the public key is generated, optionally enter and confirm a passphrase. You will be prompted for the passphrase when you authenticate to the VM with your private SSH key. Enter **Pa55w.rd1234** as the passphrase.

Without a passphrase, if someone obtains your private key, they can log in to any VM or service that uses that key. We recommend you create a passphrase. However, if you forget the passphrase, there is no way to recover it.

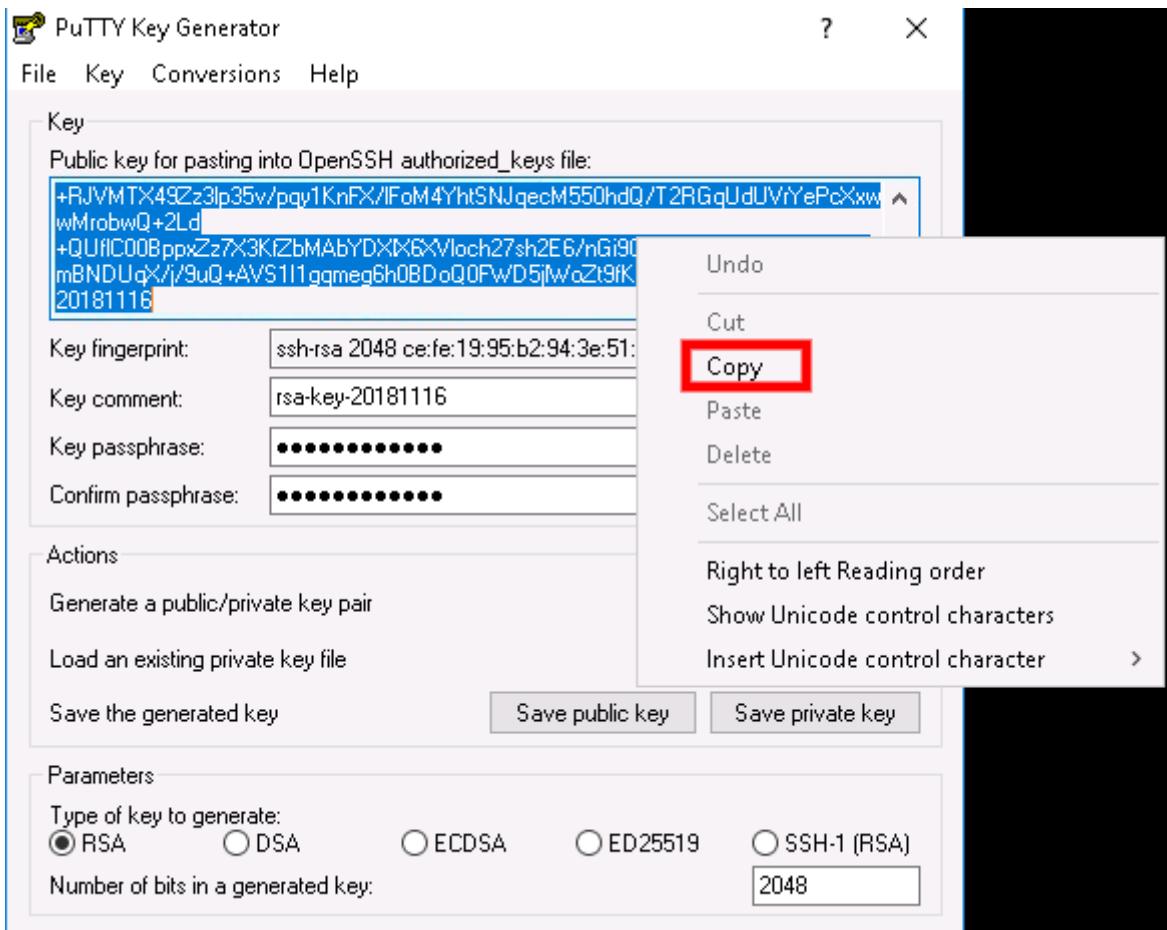
- The public key is displayed at the top of the window. You can copy this entire public key and then paste it into the Azure portal or an Azure Resource Manager template when you create a Linux VM. Save the public key to a location on your machine and call the file **public**:



8. Save the private key to the same location but with the filename **private**.



9. Highlight and copy the public key from the top window.



### 33.2.2 Task 2: Create a Linux virtual machine in the Azure portal

1. Navigate back to the **Azure Portal**.
2. Choose **Create a resource** in the upper left corner of the Azure portal.
3. In the search box above the list of Azure Marketplace resources, search for and select **Ubuntu Server 18.04 LTS** by Canonical, then choose **Create**.
4. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and then choose the **Resource group** *myResourceGroup*.

## Create a virtual machine

Basics Disks Networking Management Guest config Tags

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace. Complete the Basics tab then Review + create to provision a virtual machine with deployment customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

### PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups to organize resources.

\* Subscription [?](#)

Azure Pass

  └ \* Resource group [?](#)

myResourceGroup

[Create new](#)

5. Under **Instance details**, type *myVM-Linux* for the **Virtual machine name** and choose *East US* for your **Region**. Leave the other defaults.

## Create a virtual machine

\* Subscription [?](#)

Azure Pass

  └ \* Resource group [?](#)

myResourceGroup

[Create new](#)

### INSTANCE DETAILS

\* Virtual machine name [?](#)

myVM-Linux

6. Under **Administrator account**, select **SSH public key**, type the user name **localadmin**, then paste your public key into the text box. Remove any leading or trailing white space in your public key.

### ADMINISTRATOR ACCOUNT

Authentication type [?](#)

Password  SSH public key

\* Username [?](#)

localadmin

\* SSH public key [?](#)

nFX/IFoM4YhtSNJqecM550hdQ/T2RGqUdUVrYePcXwwwMrobwQ+2Ld+QUfIC00B  
ppxZz7X3KFZbMAbYDXDX6XMoCh27sh2E6/nGi9C0wNe1/B5IlzOE6xC4h1mBNDUqX  
/j/uQ+A/VSII1gqmeg6h0BD0Q0FWD5jIWoZt9fKPbiTTfQ== rsa-key-20181116

Login with Azure Active Directory (Preview) [?](#)  On  Off

7. Under **Inbound port rules > Public inbound ports**, choose **Allow selected ports** and then select **SSH (22)** and **HTTP (80)** from the drop-down.

### Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \* ⓘ

None  Allow selected ports

Select inbound ports \*

| HTTP (80), SSH (22)                 |             |
|-------------------------------------|-------------|
| <input checked="" type="checkbox"/> | HTTP (80)   |
| <input type="checkbox"/>            | HTTPS (443) |
| <input checked="" type="checkbox"/> | SSH (22)    |

8. Click the **Management** tab and select **No** or **Off** for all options.

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

#### Azure Security Center

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

Enable basic plan for free ⓘ

Yes  No

This will apply to every VM in the selected subscription

#### Monitoring

Boot diagnostics ⓘ

On  Off

OS guest diagnostics ⓘ

On  Off

#### Identity

System assigned managed identity ⓘ

On  Off

#### Azure Active Directory

Login with AAD credentials (Preview) ⓘ

On  Off

**⚠** This preview capability is not for production use. When you sign in, verify the name of the app on the sign-in screen is "Azure Linux VM sign in" and the IP address of the target VM is correct.

#### Auto-shutdown

Enable auto-shutdown ⓘ

On  Off

9. Leave the remaining defaults and then select the **Review + create** button at the bottom of the page.
10. On the **Create a virtual machine** page, you can see the details about the VM you are about to create. When you are ready, select **Create**.

## Create a virtual machine

✓ Validation passed

Basics Disks Networking Management Guest config

### PRODUCT DETAILS

Ubuntu Server 18.04 LTS  
by Canonical  
[Terms of use](#) | [Privacy policy](#)

Pricing not available for this offer.  
View [Pricing details](#) for more information.

Standard D2s v3  
by Microsoft  
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply  
**0.0715 GBP/hr**  
Pricing for other VM sizes

### TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s); (b) authorize Microsoft to bill my current payment method for the fees associated with my Azure subscription; and (c) agree that Microsoft may share my contact information with partners and other third parties to provide me with offers for support, billing and other transactional activities. Microsoft's [Azure Marketplace Terms](#) for additional details.

### BASICS

Create

Previous

Next

It will take a few minutes for your VM to be deployed. When the deployment is finished, move on to the next section.

### 33.2.3 Task 3: Connect to your VM

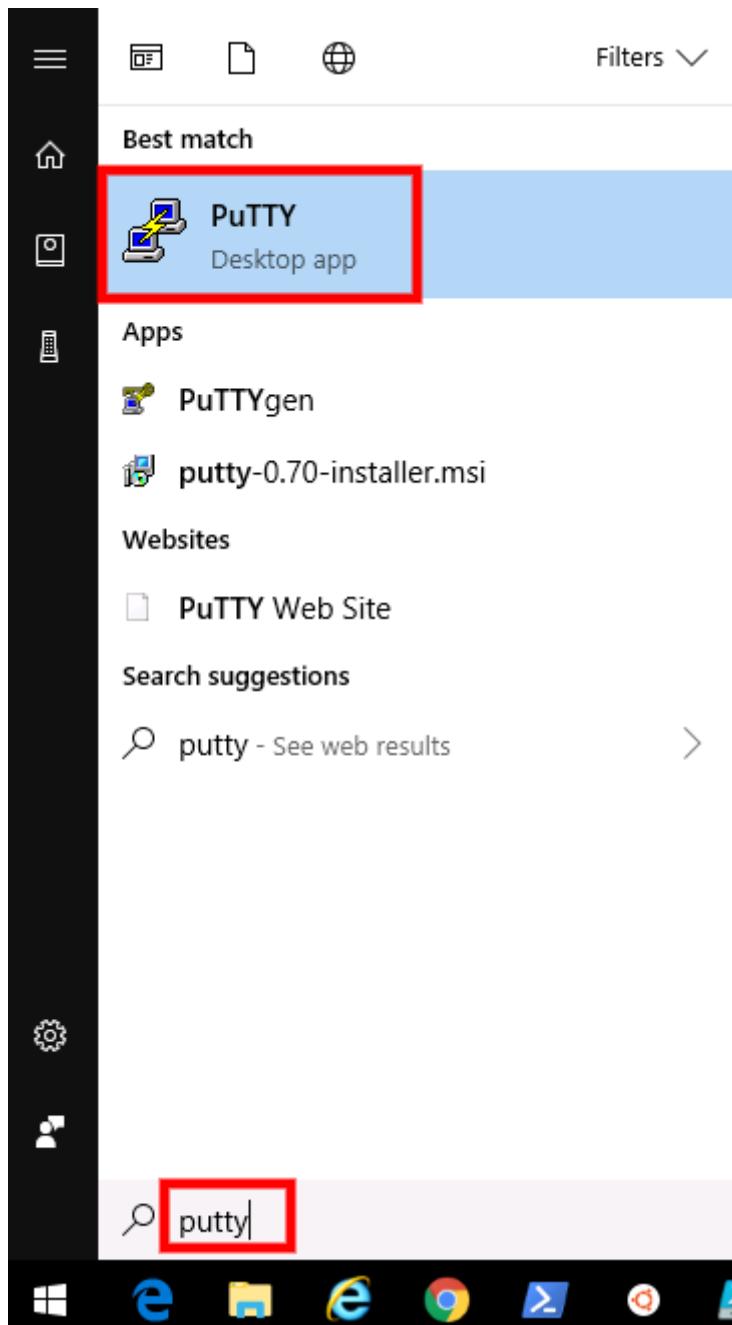
One way to make an SSH connection to your Linux VM from Windows is to use an SSH client. This is the preferred method if you have an SSH client installed on your Windows system, or if you use the SSH tools in Bash in Azure Cloud Shell. If you prefer a GUI-based tool, you can connect with PuTTY. In this task you will use PuTTY.

1. In the **Azure Portal Hub Menu** click **Virtual Machines** then select your **myVM-Linux** machine.
2. In the Overview blade, note down or copy the **Public IP Address** of your virtual machine *If this does not display, refresh your browser.*

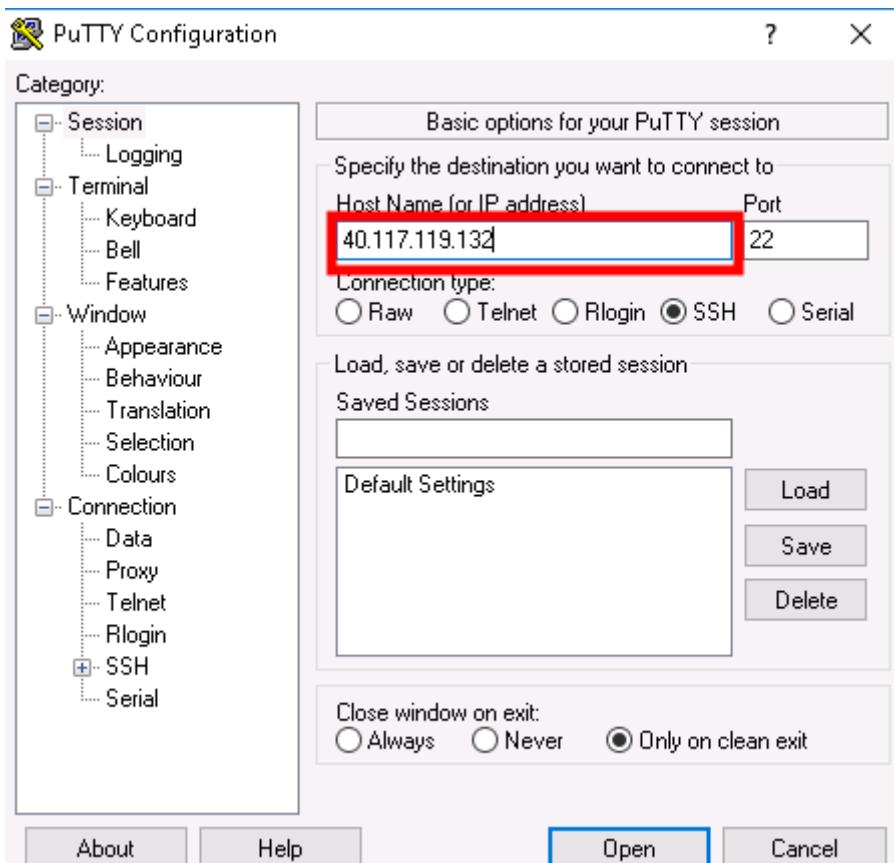
**Note:** Your public IP will be different to what is shown in the screenshot.

|                                           |                                           |
|-------------------------------------------|-------------------------------------------|
| Resource group ( <a href="#">change</a> ) | Computer name                             |
| <a href="#">myResourceGroup</a>           | myVM-Linux                                |
| Status                                    | Operating system                          |
| Running                                   | Linux                                     |
| Location                                  | Size                                      |
| East US                                   | Standard D2s v3 (2 vcpus, 8 GB memory)    |
| Subscription ( <a href="#">change</a> )   | Public IP address                         |
| <a href="#">Azure Pass</a>                | <a href="#">40.117.119.132</a>            |
| Subscription ID                           | Virtual network/subnet                    |
| 419b8e86-46ba-4bad-83a5-521ed3e985ba      | <a href="#">myImageVnet/myImageSubnet</a> |
|                                           | DNS name                                  |
|                                           | <a href="#">Configure</a>                 |
| Tags ( <a href="#">change</a> )           |                                           |
| <a href="#">Click here to add tags</a>    |                                           |

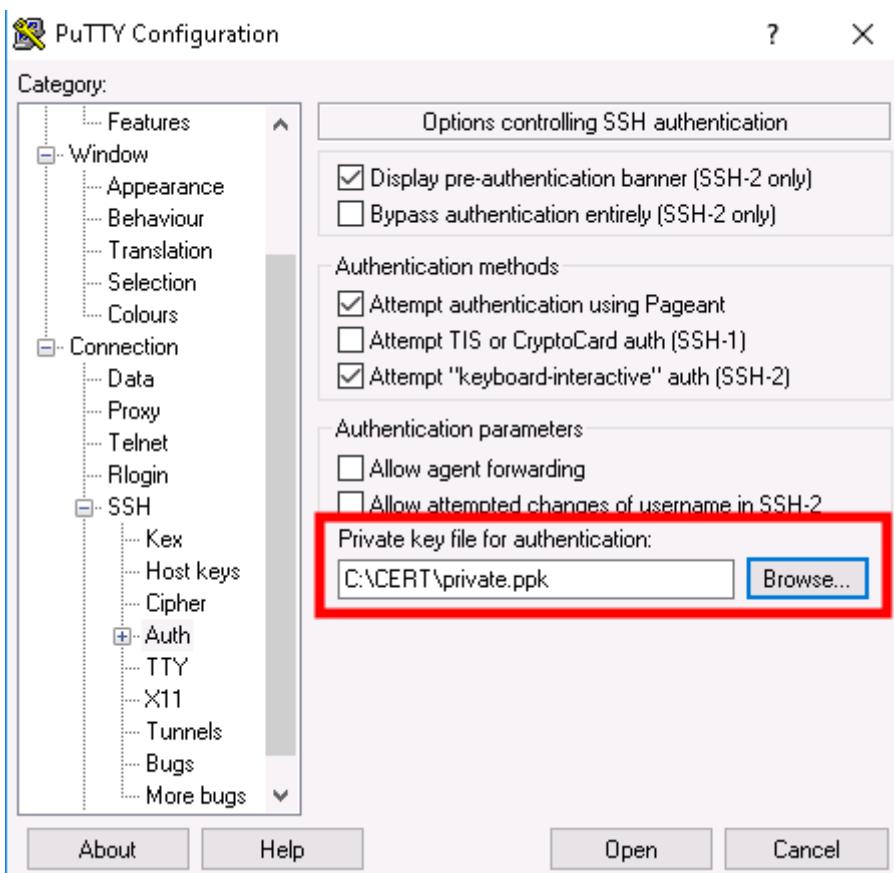
3. Start **PuTTY** by clicking the start menu and searching for PuTTY.



4. Type in or paste in your Public IP Address of your Linux Azure Linux VM:

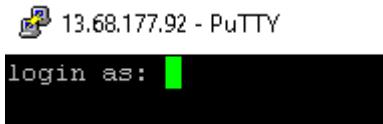


5. Select the **Connection > SSH > Auth** category. Browse to and select your PuTTY private key (.ppk file):

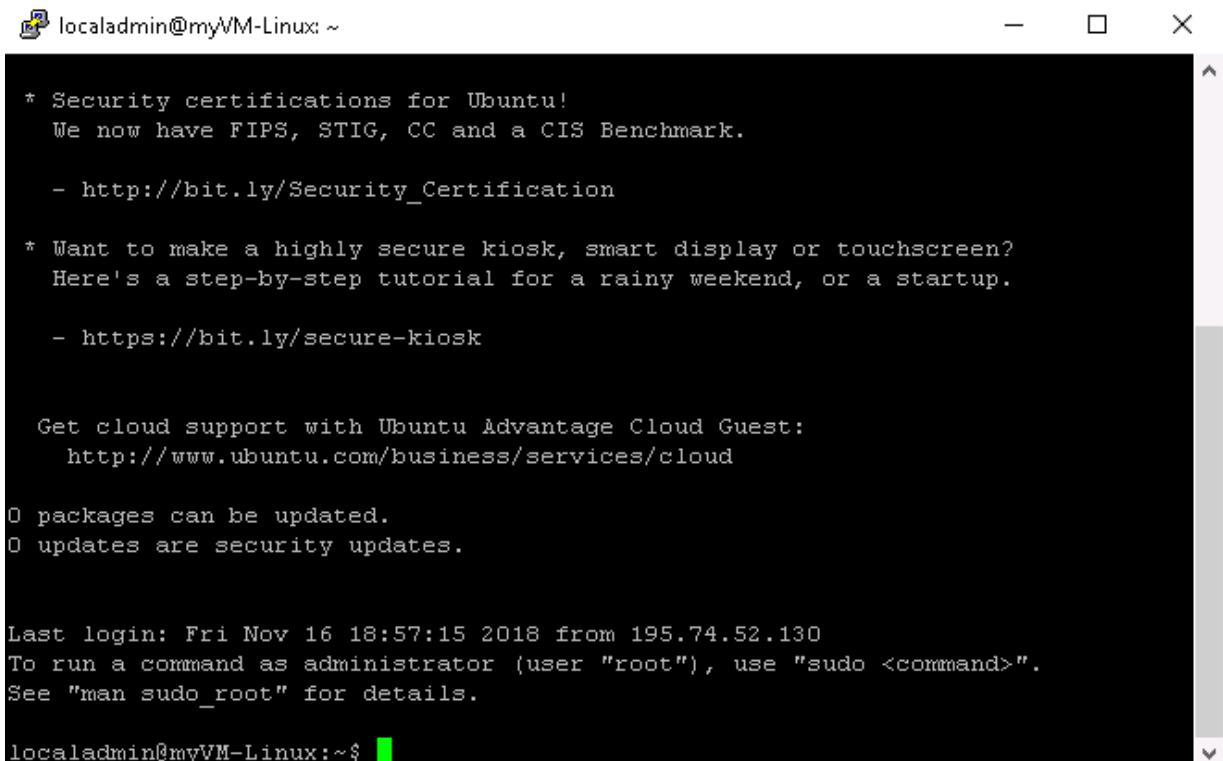


6. Click **Open** to connect to your VM.
7. Click **Yes** to continue on the pop up.

8. On the login as screen enter **localadmin** and press **Enter** then enter the password Pa55w.rd1234 and press **Enter**. *Note: As you type the password the cursor will not move*



9. You are now logged into the Linux VM hosted in Azure.



```
* Security certifications for Ubuntu!
 We now have FIPS, STIG, CC and a CIS Benchmark.

 - http://bit.ly/Security_Certification

* Want to make a highly secure kiosk, smart display or touchscreen?
 Here's a step-by-step tutorial for a rainy weekend, or a startup.

 - https://bit.ly/secure-kiosk

Get cloud support with Ubuntu Advantage Cloud Guest:
 http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

Last login: Fri Nov 16 18:57:15 2018 from 195.74.52.130
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

localadmin@myVM-Linux:~$
```

**WARNING:** Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**.

**Results:** You have now completed this Lab.

## 34 Module 2: Lab 14 - Azure Bastion

### Scenario

The Azure Bastion service is a new fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over SSL. When you connect via Azure Bastion, your virtual machines do not need a public IP address.

Bastion provides secure RDP and SSH connectivity to all VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to outside world while still providing secure access using RDP/SSH. With Azure Bastion, you connect to the virtual machine directly from the Azure portal. You don't need an additional client, agent, or piece of software.

### 34.1 Exercise 1: Implement Azure Bastion

#### 34.1.1 Task 1: Enable Azure Bastion on your subscription

1. Open a browser and navigate to <https://portal.azure.com>
2. Open the **Cloud Shell** in PowerShell mode and create storage if required.
3. Run the following 2 commands to create a Resource Group and Virtual Machine and VNet to test the Azure Bastion service.

```
New-AzResourceGroup -Name myResourceGroup -Location "East US"
New-AzVm -ResourceGroupName "myResourceGroup" -Name "myVM" -Location "East US" -VirtualNetworkName
```

**Note:** The VM is being created without a Public IP Address.

4. When prompted enter **LocalAdmin** and **Pa55w.rd1234** for the credentials.
5. In the Azure Portal navigate to your **myVnet** and click **Subnets**.

The screenshot shows the Microsoft Azure portal interface. On the left, there is a navigation sidebar with various options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (which includes 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', and 'Monitor'), and 'Subnets'. The main content area is titled 'myVnet - Subnets' under 'Virtual network'. It contains a search bar, a list of management links ('Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems'), a 'Settings' section with 'Address space', 'Connected devices', and a highlighted 'Subnets' link (which is also outlined in red in the screenshot). Below these are 'DDoS protection', 'Firewall', 'Security', 'DNS servers', and 'Metrics'.

6. Click **+** **Subnet** and create a subnet with the following details:
  - Name: **AzureBastionSubnet** (*Note this is case sensitive*)
  - Address Range: **192.168.2.0/24**
7. Click **OK**.

**Add subnet**

myVnet

\* Name  
AzureBastionSubnet ✓

\* Address range (CIDR block) ⓘ  
192.168.2.0/24 ✓  
192.168.2.0 - 192.168.2.255 (251 + 5 Azure reserved addresses)

Network security group  
None ▾

Route table  
None ▾

Service endpoints

Services ⓘ  
0 selected ▾

Subnet delegation

Delegate subnet to a service ⓘ  
None ▾

#### 34.1.2 Task 2: Create a bastion host

1. From the home page in the **Azure portal** click **+ Create a resource**.
2. On the **New** page, in the *Search the Marketplace* field, type **Bastion**, then click **Enter** to get to the search results.
3. From the results, click **Bastion**.

The screenshot shows the Microsoft Azure Marketplace interface. On the left, there's a sidebar with links like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (which includes 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', and 'Load balancers'), and a search bar at the top right with the word 'bastion' typed in.

The main area is titled 'Marketplace' and shows a search result for 'bastion'. It includes a 'My Saved List' section with 'Recently created' and 'Service Providers' links. Below that is a 'Categories' section with links to 'Get Started', 'AI + Machine Learning', 'Analytics', 'Blockchain', 'Compute', and 'Containers'. The 'Bastion' service by Microsoft is highlighted with a blue dashed border. It features a blue icon with a white 'X' shape, the name 'Bastion', the provider 'Microsoft', and a description: 'Bastion can be used to configure web based access to your vm.' There's also a small blue heart icon in the bottom right corner of the card.

4. On the **Bastion** page, click **Create** to open the **Create a bastion** page.

This screenshot shows the 'Bastion' service page on the Microsoft Azure Marketplace. At the top, it says 'Bastion' and 'Microsoft'. Below that is a large blue square icon with a white 'X' shape. To the right of the icon, the word 'Bastion' is displayed again, followed by a 'Save for later' button with a heart icon. Underneath is another 'Create' button, which is highlighted with a red rectangular box.

5. On the **Create a bastion** page, configure a new Bastion resource. Specify the configuration settings below.

- **Subscription:** Select your Subscription
- **Resource Group:** myResourceGroup
- **Name:** Bastion
- **Region:** East US
- **Virtual network:** myVnet
- **Subnet:** AzureBastionSubnet
- **Public IP address:** The public IP of the Bastion resource on which RDP/SSH will be accessed (over port 443). Create a new public IP, or use an existing one. The public IP address must be in the same region as the Bastion resource you are creating.
- **Public IP address name:** Leave as default
- **Public IP address SKU:** Prepopulated by default to **Standard**. Azure Bastion uses/supports only the Standard Public IP SKU.
- **Assignment:** Prepopulated by default to **Static**.

1. When you have finished specifying the settings, click **Review + Create**. This validates the values. Once validation passes, you can begin the creation process.

## Create a bastion

Basics Tags Review + create

Bastion allows web based RDP access to your vnet VM. [Learn more.](#)

**Project details**

\* Subscription: Azure Pass - Sponsorship

\* Resource group: myResourceGroup [Create new](#)

**Instance details**

\* Name: Bastion ✓

\* Region: East US

**Configure virtual networks**

\* Virtual network: myVnet [Create new](#)

\* Subnet: AzureBastionSubnet (192.168.2.0/24) [Manage subnet configuration](#)

**Public IP address**

\* Public IP address:  Create new  Use existing

\* Public IP address name: myVnet-ip ✓

Public IP address SKU: Standard

\* Assignment:  Dynamic  Static

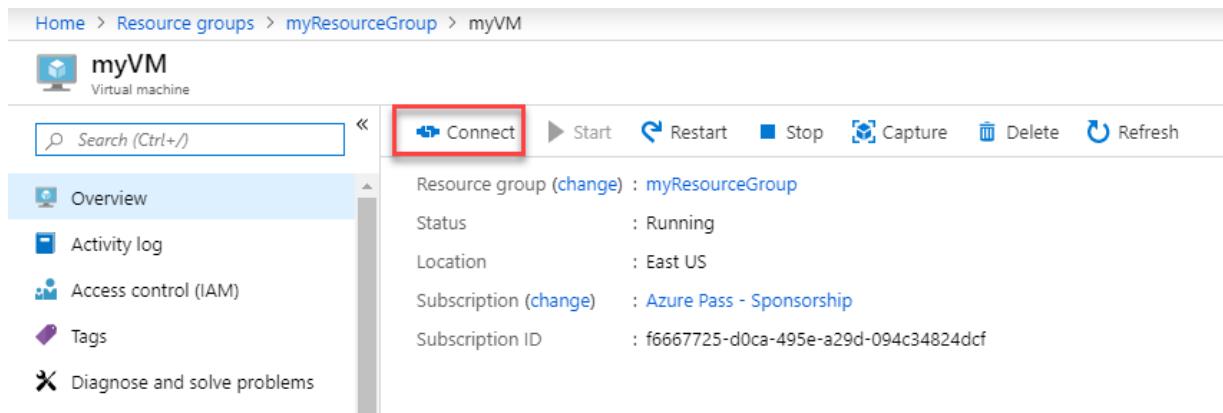


2. On the Create a bastion page, click **Create**.
3. You will see a message letting you know that your deployment is underway. Status will display on this page as the resources are created. It takes about 5 mins for the Bastion resource to be created and deployed.

### 34.1.3 Task 3: Connect to a VM using a bastion host

If you create a bastion host in the portal by using an existing VM, various settings will automatically default corresponding to your virtual machine and/or virtual network.

1. In the **Azure portal**, navigate to your virtual machine, then click **Connect**.



Home > Resource groups > myResourceGroup > myVM

**myVM** Virtual machine

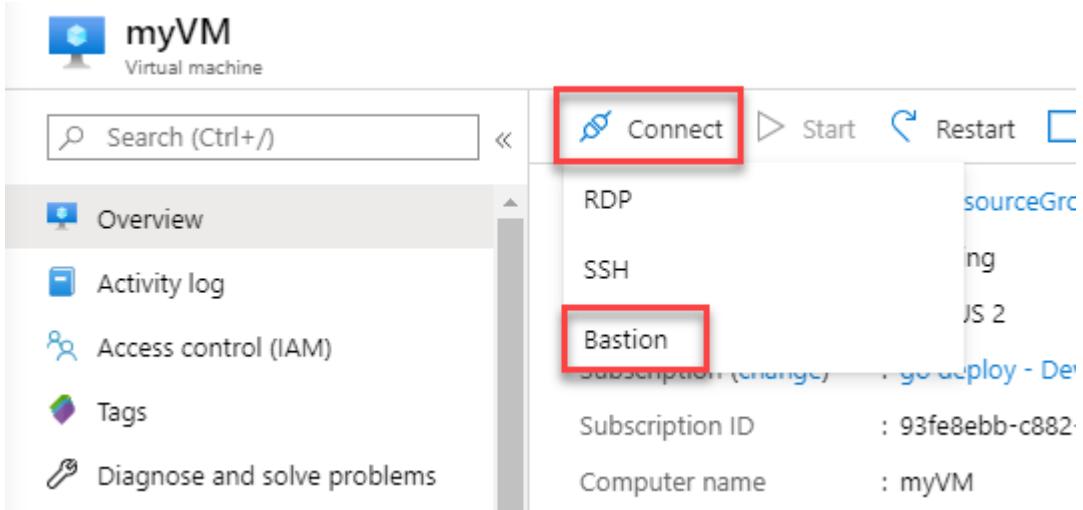
Search (Ctrl+ /)

**Connect** Start Restart Stop Capture Delete Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Resource group (change) : myResourceGroup  
Status : Running  
Location : East US  
Subscription (change) : Azure Pass - Sponsorship  
Subscription ID : f6667725-d0ca-495e-a29d-094c34824dcf

2. On the dropdown, click **Bastion**.



3. De-select Open in new window and then enter **LocalAdmin** and **Pa55w.rd1234** for the credentials and click **Connect**.

**Connect using Azure Bastion**  
Azure Bastion Service enables you to secure and seamless or any piece of software. [Learn more about Azure Bastion](#).

Please enter username and password to your virtual machine to conn

Using Bastion: **Bastion**, Provisioning State: **Succeeded**

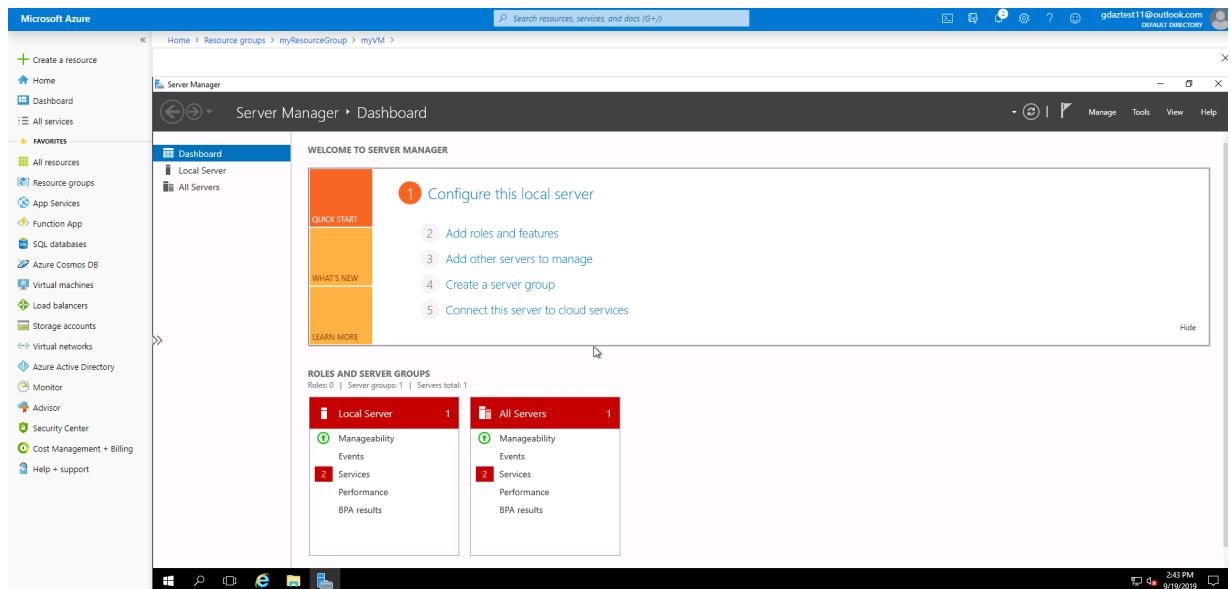
Open in new window

\* Username ⓘ  
LocalAdmin

\* Password ⓘ  
.....

**Connect**

4. You should now be connected to your VM.



**WARNING:** Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**

**Results:** You have now completed this lab.

## 35 Module 2: Lab 15 - Manage Azure DDoS Protection Standard

In this lab you will learn how to enable and disable distributed denial of service (DDoS) protection, and use telemetry to mitigate a DDoS attack with Azure DDoS Protection Standard. DDoS Protection Standard protects Azure resources such as virtual machines, load balancers, and application gateways that have an Azure public IP address assigned to it.

### 35.1 Exercise 1: Implement DDoS protection in Azure.

#### 35.1.1 Task 1: Create a DDoS protection plan

A DDoS protection plan defines a set of virtual networks that have DDoS protection standard enabled, across subscriptions. You can configure one DDoS protection plan for your organization and link virtual networks from multiple subscriptions to the same plan. The DDoS Protection Plan itself is also associated with a subscription, that you select during the creation of the plan. The DDoS Protection Plan works across regions and subscriptions. Example -you can create the plan in Region East-US and link to subscription #1 in your tenant. The same plan can be linked to virtual networks from other subscriptions in different regions, across your tenant. The subscription the plan is associated to incurs the monthly recurring bill for the plan, as well as overage charges, in case the number of protected public IP addresses exceed 100.

Creation of more than one plan is not required for most organizations. A plan cannot be moved between subscriptions. If you want to change the subscription a plan is in, you have to delete the existing plan and create a new one.

1. Select **Create a resource** in the upper left corner of the Azure portal.
2. Search for **DDoS**. When **DDos protection plan** appears in the search results, select it.
3. Select **Create**.
4. Enter or select your own values, or enter, or select the following example values, and then select **Create**:

| Setting        | Value                                                     |
|----------------|-----------------------------------------------------------|
| Name           | myDdosProtectionPlan                                      |
| Subscription   | Select your subscription.                                 |
| Resource group | Select <b>Create new</b> and enter <i>myResourceGroup</i> |
| Location       | East US                                                   |

### 35.1.2 Task 2: Enable DDoS for a new virtual network

1. Select **Create a resource** in the upper left corner of the Azure portal.
2. Select **Networking**, and then select **Virtual network**.
3. Enter or select your own values, or enter or select the following example values, accept the remaining defaults, and then select **Review + create**, then click **Create**:

| Setting         | Value                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| Name            | myVirtualNetwork                                                                                                              |
| Subscription    | Select your subscription.                                                                                                     |
| Resource group  | Select <b>Use existing</b> , and then select <b>myResourceGroup</b>                                                           |
| Location        | East US                                                                                                                       |
| DDoS protection | Select the <b>Security Tab</b> . Select <b>Standard</b> and then under <b>DDoS protection</b> , select <b>myDdosProtected</b> |

You cannot move a virtual network to another resource group or subscription when DDoS Standard is enabled for the virtual network. If you need to move a virtual network with DDoS Standard enabled, disable DDoS Standard first, move the virtual network, and then enable DDoS standard. After the move, the auto-tuned policy thresholds for all the protected public IP addresses in the virtual network are reset.

4. Click **All Services** and search for and select **Public IP addresses**.
5. Click **+ Add** and create an **IPv4** Public IP address in your **myResourceGroup** Resource Group.

### 35.1.3 Task 3: Disable DDoS for a virtual network

1. Enter the name of the virtual network you want to disable DDoS protection standard for in the **Search resources, services, and docs** box at the top of the portal. When the name of the virtual network appears in the search results, select it.
2. Select **DDoS protection**, under **SETTINGS**.
3. Select **Basic** under **DDoS protection plan** and then select **Save**.

### 35.1.4 Task 4: Work with DDoS protection plans

1. Select **All services** on the top, left of the portal.
2. Enter **DDoS** in the **Filter** box. When **DDoS protection plans** appear in the results, select it.
3. Select the protection plan you want to view from the list.
4. All virtual networks associated to the plan are listed.
5. If you want to delete a plan, you must first dissociate all virtual networks from it.

### 35.1.5 Task 5: Configure alerts for DDoS protection metrics

You can select any of the available DDoS protection metrics to alert you when there's an active mitigation during an attack, using the Azure Monitor alert configuration. When the conditions are met, the address specified receives an alert email:

1. Select **All services** on the top, left of the portal.
2. Enter **Monitor** in the **Filter** box. When **Monitor** appears in the results, select it.
3. Select **Alerts**.
4. On the **Monitor** blade click **Alerts** then click **+ New alert rule**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar 'Search resources, services, and docs (G+)', and a breadcrumb trail 'All services > Monitor | Alerts'. On the left, there's a sidebar with links like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Azure Cosmos DB', and 'SQL databases'. The main content area is titled 'Monitor | Alerts' and contains sections for 'Overview', 'Activity log', 'Alerts' (which is highlighted with a red box), 'Metrics', 'Logs', 'Service Health', and 'Workbooks'. A 'New alert rule' button is also highlighted with a red box.

5. Click **Select resource**.
6. Select your Subscription and then in the Filter by resource type drop down, select **Public IP addresses** then select **myPublicIP** (or the name of your public ip address you created earlier) then click **Done**.

The left screenshot shows the 'Create alert rule' blade with a 'Scope' section containing a 'Select resource' button, which is highlighted with a red box. The right screenshot shows the 'Select a resource' blade with a 'Filter by resource type' dropdown set to 'Public IP addresses', which is also highlighted with a red box. Below it, the 'myPublicIP' resource is listed.

7. Click **Select condition**.
8. Search for **attack** and select **Under DDoS attack or not**.

The screenshot shows the 'Configure signal logic' blade. At the top, there's a search bar with 'attack' typed into it. Below the search bar is a table with a single row. The table has columns for 'Signal name' (containing 'Under DDoS attack or not'), 'Signal type' (with a downward arrow), 'Monitor service' (with a downward arrow), and 'Platform'.

9. Scroll down the **Configure signal logic** blade and in the **Threshold value** enter **1 - 1** means you are under attack. **0** means you are not under attack. Click **Done**.

**Alert logic**

Threshold ⓘ

Static Dynamic

Operator ⓘ Greater than

Aggregation type \* ⓘ Maximum

Threshold value \* ⓘ 1 count

Condition preview

Whenever the maximum under ddos attack or not is greater than 1 count

Evaluated based on

Aggregation granularity (Period) \* ⓘ 5 minutes

Frequency of evaluation ⓘ Every 1 Minute

**Done**

- On the **Create alert rule** blade, click **Select action group** then click **+ Create action group**. and enter the following details.

| Setting           | Value                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------|
| Action group name | <b>DDOS AG</b>                                                                                       |
| Short Name        | <b>ddosag</b>                                                                                        |
| Subscription      | Select your subscription                                                                             |
| Resource Group    | Select <b>myResourceGroup</b>                                                                        |
| Action Name       | DDOS Alert Email                                                                                     |
| Action Type       | Select <b>Email/SMS message/Push/Voice</b> then select email and enter a valid email address and cli |

- Back on the Add action group blade click **OK**.
- Give the Alert a name and click **Create alert rule**.

Within a few minutes of an attack detection, you would receive an email from Azure Monitor metrics that looks similar to the following screenshot:

The screenshot shows the Azure Monitor Metrics blade. At the top, it displays summary statistics: **Alerts fired: 1**, **Activity log errors: 0**, and **Service Health** status. Under Service Health, there are three items: **Service Issues: 0**, **Planned Maintenance: 0**, and **Health Advisories: 0**. Below this, there are two tabs: **Alert sources (1)** and **Application Insights (2)**. A search bar labeled **Filter alerts...** is present. A table below lists the alert details:

| NAME                        | STATUS    | CONDITION             | SOURCE  |
|-----------------------------|-----------|-----------------------|---------|
| DDoS Attack -App Gateway... | ⚠ Warning | Failed locations >= 3 | Metrics |

### 35.1.6 Task 6: Use DDoS protection telemetry

Telemetry for an attack is provided through Azure Monitor in real time. The telemetry is available only for the duration that a public IP address is under mitigation. You don't see telemetry before or after an attack is

mitigated.

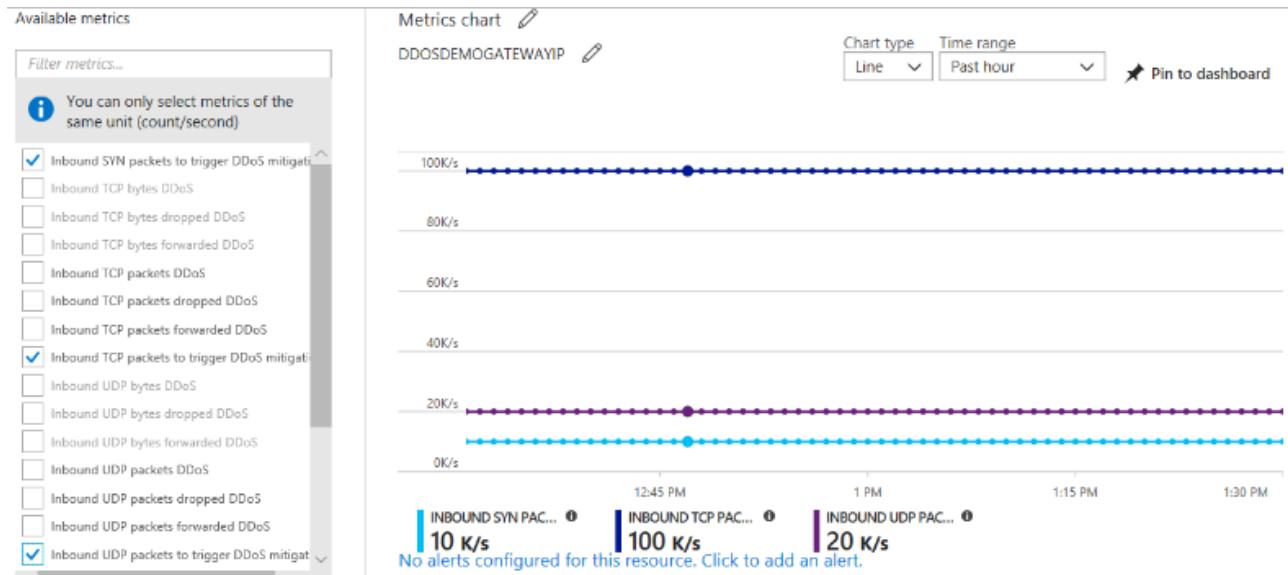
1. Select **All services** on the top, left of the portal.
2. Enter **Monitor** in the **Filter** box. When **Monitor** appears in the results, select it.
3. Select **Metrics**.
4. Select the **Subscription** and **Resource group** that contain the public IP address that you want telemetry for then click **Apply**.
5. A series of **Available Metrics** appear on the top of the screen. These metrics, when selected, are graphed in the **Azure Monitor Metrics Chart** on the overview screen.
6. Select the Public IP Address you created earlier and select the **Under DDoS attack or not** Metric and under **aggregation** select **Max**

The metric names present different packet types, and bytes vs. packets, with a basic construct of tag names on each metric as follows:

- **Dropped tag name** (for example, **Inbound Packets Dropped DDoS**): The number of packets dropped/scrubbed by the DDoS protection system.
- **Forwarded tag name** (for example **Inbound Packets Forwarded DDoS**): The number of packets forwarded by the DDoS system to the destination VIP - traffic that was not filtered.
- **No tag name** (for example **Inbound Packets DDoS**): The total number of packets that came into the scrubbing system - representing the sum of the packets dropped and forwarded.

### 35.1.7 Task 7: View DDoS mitigation policies

DDoS Protection Standard applies three auto-tuned mitigation policies (TCP SYN, TCP & UDP) for each public IP address of the protected resource, in the virtual network that has DDoS enabled. You can view the policy thresholds by selecting the **Inbound TCP packets to trigger DDoS mitigation** and **Inbound UDP packets to trigger DDoS mitigation** metrics with **aggregation** type as 'Max', as shown in the following picture:



Policy thresholds are auto-configured via Azure machine learning-based network traffic profiling. Only when the policy threshold is breached does DDoS mitigation occur for the IP address under attack.

### 35.1.8 Task 8: Configure DDoS attack mitigation reports

Attack mitigation reports uses the Netflow protocol data which is aggregated to provide detailed information about the attack on your resource. Anytime a public IP resource is under attack, the report generation will start as soon as the mitigation starts. There will be an incremental report generated every 5 mins and a post-mitigation report for the whole mitigation period. This is to ensure that in an event the DDoS attack continues for a longer duration of time, you will be able to view the most current snapshot of mitigation report every 5 minutes and a complete summary once the attack mitigation is over.

1. Select **All services** on the top, left of the portal.

2. Enter **Monitor** in the **Filter** box. When **Monitor** appears in the results, select it.
3. Under **SETTINGS**, select **Diagnostic Settings**.
4. Select the **Subscription** and **Resource group** that contain the public IP address you want to log.
5. Select **Public IP Address** for **Resource type**, then select the specific public IP address you want to log metrics for.
6. Select **+ Add diagnostic setting** to collect the DDoSMitigationReports log and give the Diagnostic setting the name **DDoSLog** and then select as many of the following options as you require then click **Save**:
  - **Archive to a storage account:** Data is written to an Azure Storage account.
  - **Stream to an event hub:** Allows a log receiver to pick up logs using an Azure Event Hub. Event hubs enable integration with Splunk or other SIEM systems.
  - **Send to Log Analytics:** Writes logs to the Azure Monitor service.

Both the incremental & post-attack mitigation reports include the following fields

- Attack vectors
- Traffic statistics
- Reason for dropped packets
- Protocols involved
- Top 10 source countries or regions
- Top 10 source ASNs

### **35.1.9 Task 9: Configure DDoS attack mitigation flow logs**

Attack Mitigation Flow Logs allow you to review the dropped traffic, forwarded traffic and other interesting datapoints during an active DDoS attack in near-real time. You can ingest the constant stream of this data into your SIEM systems via event hub for near-real time monitoring, take potential actions and address the need of your defense operations.

1. Select **All services** on the top, left of the portal.
2. Enter **Monitor** in the **Filter** box. When **Monitor** appears in the results, select it.
3. Under **SETTINGS**, select **Diagnostic Settings**.
4. Select the **Subscription** and **Resource group** that contain the public IP address you want to log.
5. Select **Public IP Address** for **Resource type**, then select the specific public IP address you want to log metrics for.
6. Select **Turn on diagnostics to collect the DDoSMitigationFlowLogs log** and then select as many of the following options as you require:
  - **Archive to a storage account:** Data is written to an Azure Storage account. To learn more about this option.
  - **Stream to an event hub:** Allows a log receiver to pick up logs using an Azure Event Hub. Event hubs enable integration with Splunk or other SIEM systems.
  - **Send to Log Analytics:** Writes logs to the Azure Monitor service.
7. To view the flow logs data in Azure analytics dashboard.

Flow logs will have the following fields:

- Source IP
- Destination IP
- Source Port
- Destination port
- Protocol type
- Action taken during mitigation

### **35.1.10 Task 10: Validate DDoS detection (Optional and not part of the AZ-500 course)**

**Note:** Only carry out this task if you feel comfortable to do so. This task does not form part of the course and is a stretch exercise for those students who wish to do so.

Microsoft has partnered with [BreakingPoint Cloud](#) to build an interface where you can generate traffic against DDoS Protection-enabled public IP addresses for simulations. The BreakPoint Cloud simulation allows you to:

- Validate how Microsoft Azure DDoS Protection protects your Azure resources from DDoS attacks
- Optimize your incident response process while under DDoS attack
- Document DDoS compliance
- Train your network security teams

## Permissions

To work with DDoS protection plans, your account must be assigned to the network contributor role or to a role that is assigned the appropriate actions listed in the following table:

| Action                                            | Name                                    |
|---------------------------------------------------|-----------------------------------------|
| Microsoft.Network/ddosProtectionPlans/read        | Read a DDoS protection plan             |
| Microsoft.Network/ddosProtectionPlans/write       | Create or update a DDoS protection plan |
| Microsoft.Network/ddosProtectionPlans/delete      | Delete a DDoS protection plan           |
| Microsoft.Network/ddosProtectionPlans/join/action | Join a DDoS protection plan             |

To enable DDoS protection for a virtual network, your account must also be assigned the appropriate actions for virtual networks.

**WARNING:** Prior to continuing you should remove all resources used for this lab. To do this in the [Azure Portal](#) click **R**

**Results:** You have now completed this lab.

## 36 Module 2: Lab 16 - Antimalware for VMs

### Scenario

Azure Security Center monitors the status of antimalware protection and reports this on the Endpoint protection issues blade. Security Center notes issues, such as detected threats and insufficient protection, that might make your VMs and computers vulnerable to malware threats. By using the information on Endpoint protection issues, you can make a plan to address any identified issues.

Security Center reports the following endpoint protection issues:

- Endpoint protection not installed on Azure VMs. A supported antimalware solution isn't installed on these Azure VMs.
- Endpoint protection not installed on non-Azure computers. A supported antimalware solution isn't installed on these non-Azure computers.
- Endpoint protection health issues:
- **Signature out of date.** An antimalware solution is installed on these VMs and computers, but the solution doesn't have the latest antimalware signatures.
  - **No real time protection.** An antimalware solution is installed on these VMs and computers, but it isn't configured for real-time protection. The service might be disabled, or Security Center might be unable to obtain the status because the solution isn't supported.
- **Not reporting.** An antimalware solution is installed but not reporting data.
- **Unknown.** An antimalware solution is installed, but either its status is unknown or it's reporting an unknown error.

### 36.1 Exercise 1: Deploy Antimalware for Azure VMs.

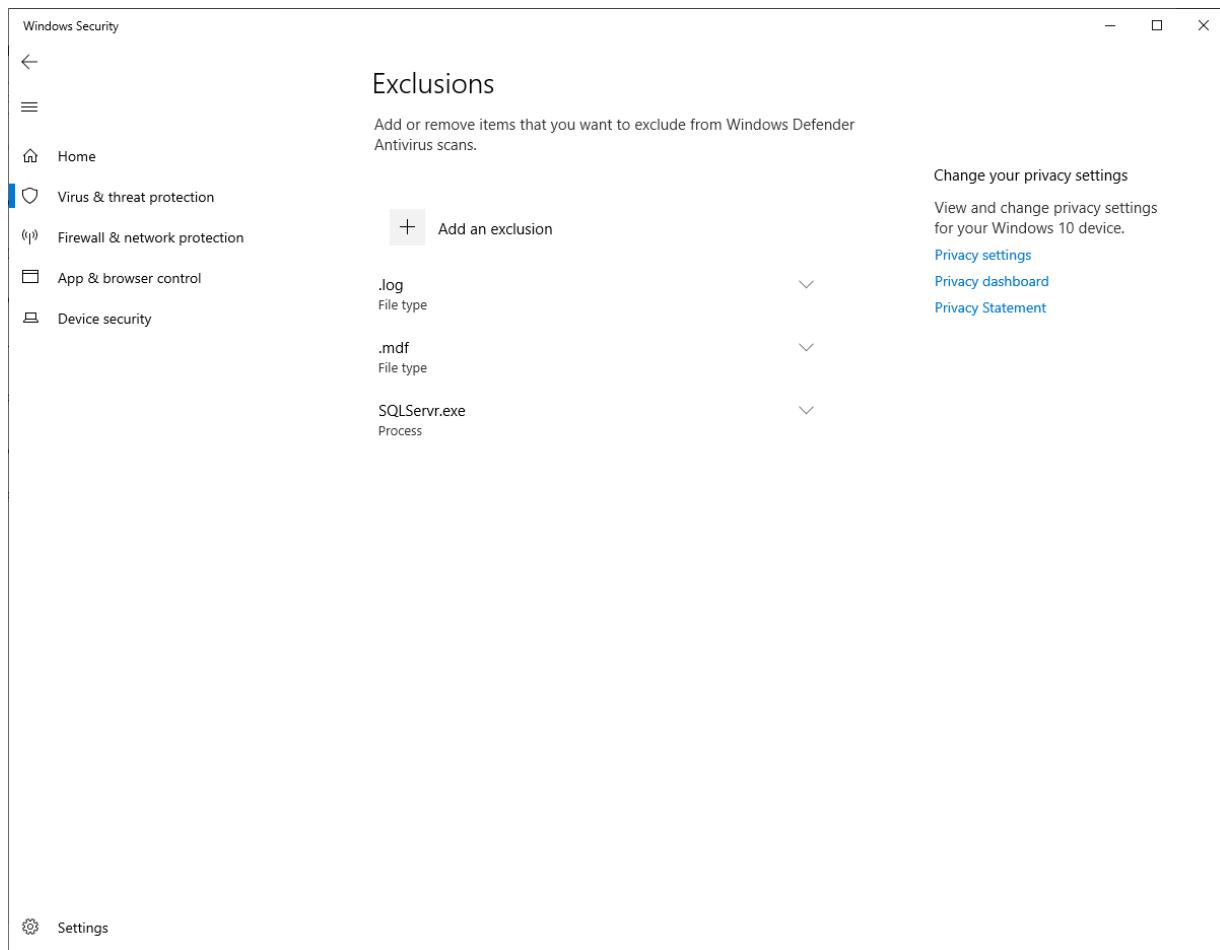
### 36.2 Task 1: Create an Azure Virtual Machine with the Antimalware extension

Enable and configure antimalware for VMs To enable and configure Microsoft Antimalware for Azure VMs by using the Azure portal while provisioning a VM, complete the following steps:

1. Sign in to the **Azure portal** at <https://portal.azure.com>
2. To create a new VM, navigate to **Virtual machines**, select **Add**, and then select **Windows Server 2019 Datacenter** under the image dropdown.
3. Enter the following details for the VM:

| Option               | Answer                                |
|----------------------|---------------------------------------|
| Resource Group       | Create new > <b>myResourceGroup</b>   |
| VM Name              | <b>myVM</b>                           |
| Region               | <b>East US</b>                        |
| Image                | <b>Windows Server 2019 Datacenter</b> |
| Username             | <b>localadmin</b>                     |
| Password             | <b>Pa55w.rd1234</b>                   |
| Public inbound ports | <b>RDP (3389)</b>                     |

4. Click the **Management** Tab and ensure all the radio buttons are set to **Off**.
5. Click the **Advanced** Tab and click **Select an extension to install**.
6. Select the **Microsoft Antimalware** extension. *You may need to click Load More at the bottom of the list to see the extension.*
7. On the **Microsoft Antimalware** blade click **Create**.
8. In the Install extension section, you can configure files, locations, process exclusions, and other scan options.
9. In the Excluded file extensions enter **.mdf;.log**
10. In the Excluded processes enter **SQLServr.exe**
11. Select **OK**.
12. Back in the Settings section, select **Review + create**.
13. Click **Create** on the validation screen.
14. Once the VM has created log onto the VM via RDP.
15. Open the Settings app and select **Update & Security > Windows Security > Virus and Threat Protection > Manage Settings > Add or remove exclusions** to verify the deployment was successful.



WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the [Azure Portal](#) click [Remove](#).

**Results:** You have now completed this lab.

## 37 Module 2: Lab 17 - Manage Windows updates by using Azure Automation

### Scenario

You can use the Update Management solution to manage updates and patches for your virtual machines. In this tutorial, you learn how to quickly assess the status of available updates, schedule installation of required updates, review deployment results, and create an alert to verify that updates apply successfully.

### 37.1 Exercise 1: Use Azure Automation to manage Windows Updates.

#### 37.1.1 Task 1: Create a Resource Group

1. Click **Resource Groups** on the Azure hub menu.
2. Click **Add**.
3. Name the resource group **RunBooks**
4. Change the region to **East US**
5. Click **Review + create**, then click **Create**.

#### 37.1.2 Task 2: Create Automation account

1. Click the **Create a resource** button found on the upper left-hand corner of Azure.

2. Select **IT & Management Tools**, and then select **Automation**.

3. Enter the following information.

| Name         | Resource Group | Location | Create Azure Run As account |
|--------------|----------------|----------|-----------------------------|
| MyAutomation | RunBooks       | EastUS2  | Yes                         |

4. Click **Create**

5. When the deployment has completed, click **All Services**, select **Automation Accounts** and select the Automation Account you created.

### 37.1.3 Task 3: Create a VM for use

1. Click **Virtual Machines**

2. Click **Add**

3. Fill in the following details to create the VM

| Resource Group | Virtual Machine Name | Region | Image               | Username   | Password     |
|----------------|----------------------|--------|---------------------|------------|--------------|
| RunBooks       | UpdateVM             | EastUS | Windows Server 2016 | localadmin | Pa55w.rd1234 |

4. Click **Review+Create**

5. Click **Create**

**Note:** Wait for the VM to deploy before moving on

### 37.1.4 Task 4: Enable Update Management

1. In the portal click Virtual machines

2. Select the VM you created in the previous steps

3. Under **Operations** click **Update management**

4. Click **Enable**

Validation is performed to determine whether Update Management is enabled for this VM. This validation includes checks for an Azure Log Analytics workspace and linked Automation account, and whether the Update Management solution is in the workspace.

A Log Analytics workspace is used to collect data that's generated by features and services like Update Management. The workspace provides a single location to review and analyze data from multiple sources.

The validation process also checks to see whether the VM is provisioned with the Microsoft Monitoring Agent (MMA) and Automation Hybrid Runbook Worker. This agent is used to communicate with Azure Automation and to obtain information about the update status. The agent requires port 443 to be open to communicate with the Azure Automation service and to download updates.

If any of the following prerequisites were found to be missing during onboarding, they're automatically added:

- **Log Analytics workspace**
- **An Automation account**
- **A Hybrid Runbook Worker (enabled on the VM)**

**Note:** Enabling the solution can take up to a few minutes. During this time, don't close the browser window. After the solution is enabled, information about missing updates on the VM flows to Azure Monitor logs. It can take between 30 minutes and 6 hours for the data to be available for analysis.

### 37.1.5 Task 5: View Update assessment

1. After the update management is enabled the **Update Management** pane will open

- If updates are missing they will display here

**Note:** If your VM has been created from the previous steps this is a template VM from Microsoft that will include all the latest Windows updates so you may not see any required updates for the VM

- If there are updates available they will be listed with a link under the Information Link column that will allow you to view the details of that update and link to the Kb article of the update from Microsoft.

### 37.1.6 Task 6: Configure Alerts

- Return to the resource group you created earlier
- Select the **MyAutomation** automation account
- Under **Monitoring** click **Alerts**
- Click **New Alert Rule**
- Click **Select condition**
- Select **Total Update Deployment Runs** from the list
- Click the **Select \*** checkbox next to **Update Deployment Name and Status**
- Under **Alert logic**, for **Threshold**, enter 1
- Click **Done**
- Under **Alert Details**, fill in the **Alert Rule name** with **UpdateAlert**
- Set the Severity to **Sev2**
- Under **Action groups** click **Select action group** then click **Create action group**
- Fill in the following details

| Action Group name       | Short Name | Resource Group | Action Name | Action Type          |
|-------------------------|------------|----------------|-------------|----------------------|
| VM Updates Action group | VMUp       | Runbooks       | Email       | Email/SMS/Push/voice |

- Click **edit details** next to email and fill in **your email** that will be used for the alerts
- Click **OK**
- Click **OK** under **Create Action Group**
- Verify your action group is listed
- Click **Create alert rule**

### 37.1.7 Task 7: Schedule an Update Deployment

- Return to your list of VMs
- Select the VM you created earlier in the lab
- Click **Update management**
- Select **Schedule update deployment**
- In new update deployment fill in the following settings
  - Name** - ScheduledUpdates
  - Schedule Settings** - Recurrence > recurring
- Click **OK** and then click **Create**
- Click **deployment schedules** to view the list of active **deployment schedules**

### 37.1.8 Task 8: View results of an update deployment

**Note:** After the scheduled deployment starts, you can see the status for that deployment on the Update deployments tab under Update management. The status is In progress when the deployment is currently

running. When the deployment finishes, if it's successful, the status changes to Succeeded. When there are failures with one or more updates in the deployment, the status is partially failed.

---

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

---

**Results:** You have now completed adding a scheduled Windows Update management with an alert system for a VM running Windows server in Azure

## 38 Module 2: Lab 18 - Custom Domains

### Scenario

Every new Azure AD tenant comes with an initial domain name, domainname.onmicrosoft.com. You can't change or delete the initial domain name, but you can add your organization's names to the list. Adding custom domain names helps you to create user names that are familiar to your users, such as [alain@contoso.com](mailto:alain@contoso.com).

#### 38.0.1 Exercise 1: Add your custom domain name using the Azure Active Directory portal

#### 38.0.2 Task 1: Add your custom domain name to Azure AD

1. In the Azure Portal, select **Azure Active Directory**.
2. Select **Custom domain names**, and then select **Add custom domain**.

The screenshot shows the 'Default Directory - Custom domain names' page in the Azure Active Directory portal. The left sidebar lists various administrative options, with 'Custom domain names' selected and highlighted by a red box. At the top right, there is a prominent 'Add custom domain' button, also highlighted with a red box. The main content area includes a search bar, a help message about moving on-premises applications to the cloud, and a table where a new domain has been added.

3. Navigate to the DNS tab in the Lab Environment to identify the unique custom domain name you have been allocated. This will be in the form of labxxxxxx.customdomainname.com.
4. In the Custom Domain name field type in your domain name you identified in the previous step and click **Add domain**.

The unverified domain is added and the **labxxxxxx.customdomainname.com** page appears showing you your DNS info.

5. Copy the DNS info from the **labxxxxxx.customdomainname.com** page. For example, MS=ms64983159.

## lab418407.godeploylabs.com

Custom domain name

 Delete

 To use lab418407.godeploylabs.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE

TXT

MX

ALIAS OR HOST NAME

@



DESTINATION OR POINTS TO ADDRESS

MS=ms81337938



TTL

3600



[Share these settings via email](#)

Verification will not succeed until you have configured your domain with your registrar as described above.

### 38.0.3 Task 2: Add your DNS information to the domain registrar

After you add your custom domain name to Azure AD, you must return to your domain registrar and add the Azure AD DNS information from your copied TXT file. Creating this TXT record for your domain "verifies" ownership of your domain name.

1. Go back to the DNS tab in the Lab environment and create a new TXT record for your domain based on your copied DNS information. You only need to enter the value record. Leave the name field blank and click **Save**.

**Note:** You can register as many domain names as you want. However, each domain gets its own TXT record from Azure AD. Be careful when entering your TXT file information at the domain registrar. If you enter the wrong, or duplicate information by mistake, you'll have to wait until the TTL times out (60 minutes) before you can try again.

### 38.0.4 Task 2: Verify your custom domain name

After you register your custom domain name, you need to make sure it's valid in Azure AD. The propagation from your domain registrar to Azure AD can be instantaneous or it can take up to a few days, depending on your domain registrar.

1. Return back to the Azure Portal **labxxxxx.customdomainname.com** page and click **Verify**.

## lab418407.godeploylabs.com

Custom domain name

 Delete

 To use lab418407.godeploylabs.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE

**TXT**

MX

ALIAS OR HOST NAME

@



DESTINATION OR POINTS TO ADDRESS

MS=ms81337938



TTL

3600



[Share these settings via email](#)

Verification will not succeed until you have configured your domain with your registrar as described above.

**Verify**

2. Your domain should now be verified.

## lab418407.godeploylabs.com

Custom domain name

 Make primary  Delete

 Verification succeeded!

Type Custom

Status Verified

Federated No

To configure lab418407.godeploylabs.com for federated sign-on to your Azure Active Directory, run Azure AD Connect on your local network.

[Download Azure AD Connect](#)

Primary domain No 

In use No

3. After you've verified your custom domain name, you can delete your verification TXT record.

**Results:** You have now completed this lab.

## 39 Module 2: Lab 19 - Private DNS

### Scenario

A DNS zone is used to host the DNS records for a particular domain. To start hosting your domain in Azure DNS, you need to create a DNS zone for that domain name. Each DNS record for your domain is then created inside this DNS zone. To publish a private DNS zone to your virtual network, you specify the list of virtual networks that are allowed to resolve records within the zone. These are called *linked* virtual networks. When autoregistration is enabled, Azure DNS also updates the zone records whenever a virtual machine is created, changes its' IP address, or is deleted.

In this lab, you learn how to:

- Create a private DNS zone
- Create a virtual network
- Link the virtual network
- Create test virtual machines
- Create an additional DNS record
- Test the private zone

### 39.1 Exercise 1: Create an Azure private DNS zone using the Azure portal

#### 39.1.1 Task 1: Create a private DNS zone

The following example creates a DNS zone called **private.contoso.com** in a resource group called **MyAzureResourceGroup**.

A DNS zone contains the DNS entries for a domain. To start hosting your domain in Azure DNS, you create a DNS zone for that domain name.

1. On the portal search bar, type **private dns zones** in the search text box and press **Enter**.
2. Select **Private DNS zone**.
3. Select **Create private dns zone**.
4. On the **Create Private DNS zone** page, type or select the following values:
  - **Resource group:** Select **Create new**, enter *MyAzureResourceGroup*, and select **OK**. The resource group name must be unique within the Azure subscription.
  - **Name:** Type *private.contoso.com* for this example.
5. For **Resource group location** select **West Central US**.
6. Select **Review + Create**.
7. Select **Create**.

It may take a few minutes to create the zone.

#### 39.1.2 Task 2: Create a virtual network

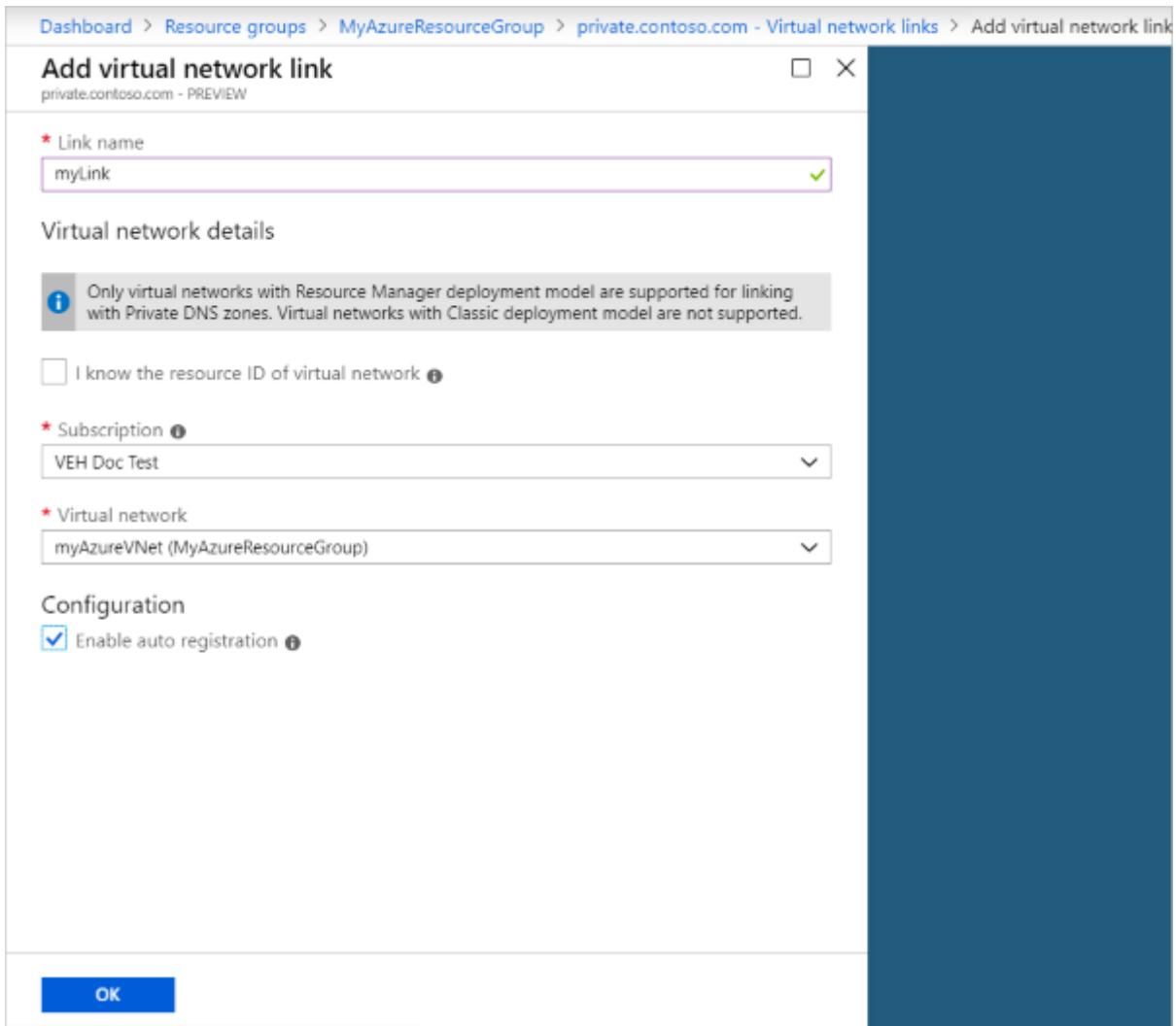
1. On the portal page upper left, select **Create a resource**, then **Networking**, then select **Virtual network**.
2. For **Name**, type **myAzureVNet**.
3. For **Resource group**, select **MyAzureResourceGroup**.
4. For **Location**, select **East US**.
5. Accept the other default values and select **Review + create**, then select **Create**.

#### 39.1.3 Task 3: Link the virtual network

To link the private DNS zone to a virtual network, you create a virtual network link.

1. Open the **MyAzureResourceGroup** resource group and select the **private.contoso.com** private zone.
2. On the left pane, select **Virtual network links**.
3. Select **Add**.

4. Type **myLink** for the **Link name**.
5. For **Virtual network**, select **myAzureVNet**.
6. Select the **Enable auto registration** check box.
7. Select **OK**.



#### 39.1.4 Task 4: Create the test virtual machines

Now, create two virtual machines so you can test your private DNS zone:

1. On the portal page upper left, select **Create a resource**, and then select **Windows Server 2016 Datacenter**.
2. Select **MyAzureResourceGroup** for the resource group.
3. Type **myVM01** - for the name of the virtual machine.
4. Select **East US** for the **Region**.
5. Type **LocalAdmin** for the administrator user name.
6. Type **Pa55w.rd1234** for the password and confirm the password.
7. For **Public inbound ports**, select **Allow selected ports**, and then select **RDP (3389)** for **Select inbound ports**.
8. Accept the other defaults for the page and then click **Next: Disks >**.
9. Accept the defaults on the **Disks** page, then click **Next: Networking >**.
10. Make sure that **myAzureVNet** is selected for the virtual network.

11. Accept the other defaults for the page, and then click **Next: Management >**.
12. For **Boot diagnostics**, select **Off**, accept the other defaults, and then select **Review + create**.
13. Review the settings and then click **Create**.
14. Repeat these steps and create another virtual machine named **myVM02**.

It will take a few minutes for both virtual machines to complete.

### 39.1.5 Task 5: Create an additional DNS record

The following example creates a record with the relative name **db** in the DNS Zone **private.contoso.com**, in resource group **MyAzureResourceGroup**. The fully qualified name of the record set is **db.private.contoso.com**. The record type is "A", with the IP address of **myVM01**.

1. Open the **MyAzureResourceGroup** resource group and select the **private.contoso.com** private zone.
2. Select **+ Record set**.
3. For **Name**, type **db**.
4. For **IP Address**, type the IP address you see for **myVM01**. This should be auto registered when the virtual machine started and should be **10.0.0.4**.
5. Select **OK**.

### 39.1.6 Task 6: Test the private zone

Now you can test the name resolution for your **private.contoso.com** private zone.

You can use the ping command to test name resolution. So, configure the firewall on both virtual machines to allow inbound ICMP packets.

1. Connect to myVM01, and open a Windows PowerShell window with administrator privileges.
  2. Run the following command:
- ```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```
3. Repeat for myVM02.

39.1.7 Task 7: Ping the VMs by name

1. From the myVM02 Windows PowerShell command prompt, ping myVM01 using the automatically registered host name:

```
ping myVM01.private.contoso.com
```

You should see output that looks similar to this:

```
Pinging myvm01.private.contoso.com [10.2.0.4] with 32 bytes of data:  
Reply from 10.2.0.4: bytes=32 time<1ms TTL=128  
Reply from 10.2.0.4: bytes=32 time=1ms TTL=128  
Reply from 10.2.0.4: bytes=32 time<1ms TTL=128  
Reply from 10.2.0.4: bytes=32 time<1ms TTL=128
```

2. Now ping the **db** name you created previously:

```
ping db.private.contoso.com
```

You should see output that looks similar to this:

```
PS C:\> ping db.private.contoso.com  
  
Pinging db.private.contoso.com [10.2.0.4] with 32 bytes of data:  
Reply from 10.2.0.4: bytes=32 time<1ms TTL=128  
  
Ping statistics for 10.2.0.4:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
PS C:\>
```

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **Remove**.

Results: You have now completed this lab.

40 Module 2: Lab 20 - Azure Blueprints

Scenario

When you learn how to create and assign blueprints, you can define common patterns to develop reusable and rapidly deployable configurations based on Azure Resource Manager templates, policy, security, and more. In this tutorial, you learn to use Azure Blueprints to do some of the common tasks related to creating, publishing, and assigning a blueprint within your organization. These tasks include:

- Create a new blueprint and add various supported artifacts
- Make changes to an existing blueprint still in Draft
- Mark a blueprint as ready to assign with Published
- Assign a blueprint to an existing subscription
- Check the status and progress of an assigned blueprint
- Remove a blueprint that has been assigned to a subscription

40.1 Exercise 1: Create a blueprint in the portal

40.1.1 Task 1: Create a blueprint

The first step in defining a standard pattern for compliance is to compose a blueprint from the available resources. In this example, create a new blueprint named **MyBlueprint** to configure role and policy assignments for the subscription. Then add a new resource group, and create a Resource Manager template and role assignment on the new resource group.

1. Select **All services** in the left pane. Search for and select **Blueprints**.
2. Select **Blueprint definitions** from the page on the left and select the **+ Create blueprint** button at the top of the page.
Or, select **Create** from the **Getting started** page to go straight to creating a blueprint.

5. Verify that the information is correct. The **Blueprint name** and **Definition location** fields can't be changed later. Then select **Next : Artifacts** at the bottom of the page or the **Artifacts** tab at the top of the page.
6. Add a role assignment at the subscription level:
7. Select the **+ Add artifact** row under **Subscription**. The **Add artifact** window opens on the right side of the browser.
8. Select **Role assignment** for **Artifact type**.
9. Under **Role**, select **Contributor**. Leave the **Add user, app or group** box with the check box that indicates a dynamic parameter.
10. Select **Add** to add this artifact to the blueprint.

The screenshot shows the 'Add artifact' window with the following configuration:

- * Artifact type:** Role assignment
- Role:** Contributor
- Add user, app or group:** Search by name or email
- Note:** You can choose to fill these parameters in now or when assigning the blueprint.
- Parameter setting:** This value should be specified when the blueprint is assigned (checkbox checked)

Note: Most artifacts support parameters. A parameter that's assigned a value during blueprint creation is a *static parameter*. If the parameter is assigned during blueprint assignment, it's a *dynamic parameter*.

11. Add a policy assignment at the subscription level:
12. Select the **+ Add artifact** row under the role assignment artifact.
13. Select **Policy assignment** for **Artifact type**.
14. Change **Type** to **Built-in**. In **Search**, enter **tag**.
15. Click out of **Search** for the filtering to occur. Select **Append tag and its value to resource groups**.
16. Select **Add** to add this artifact to the blueprint.
17. Select the row of the policy assignment **Append tag and its value to resource groups**.
18. The window to provide parameters to the artifact as part of the blueprint definition opens and allows setting the parameters for all assignments (static parameters) based on this blueprint instead of during assignment (dynamic parameters). This example uses dynamic parameters during blueprint assignment, so leave the defaults and select **Cancel**.
19. Add a resource group at the subscription level:
20. Select the **+ Add artifact** row under **Subscription**.
21. Select **Resource group** for **Artifact type**.
22. Leave the **Artifact display name**, **Resource Group Name**, and **Location** boxes blank, but make sure that the check box is checked for each parameter property to make them dynamic parameters.
23. Select **Add** to add this artifact to the blueprint.
24. Add a template under the resource group:

25. Select the **+ Add artifact** row under the **ResourceGroup** entry.
26. Select **Azure Resource Manager template** for **Artifact type**, set **Artifact display name** to **StorageAccount**, and leave **Description** blank.
27. On the **Template** tab in the editor box, paste the following Resource Manager template. After you paste the template, select the **Parameters** tab and note that the template parameters **storageAccountType** and **location** were detected. Each parameter was automatically detected and populated, but configured as a dynamic parameter.

```
```json
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "storageAccountType": {
 "type": "string",
 "defaultValue": "Standard_LRS",
 "allowedValues": [
 "Standard_LRS",
 "Standard_GRS",
 "Standard_ZRS",
 "Premium_LRS"
],
 "metadata": {
 "description": "Storage Account type"
 }
 },
 "location": {
 "type": "string",
 "defaultValue": "[resourceGroup().location]",
 "metadata": {
 "description": "Location for all resources."
 }
 }
 },
 "variables": {
 "storageAccountName": "[concat('store', uniqueString(resourceGroup().id))]"
 },
 "resources": [
 {
 "type": "Microsoft.Storage/storageAccounts",
 "name": "[variables('storageAccountName')]",
 "location": "[parameters('location')]",
 "apiVersion": "2018-07-01",
 "sku": {
 "name": "[parameters('storageAccountType')]"
 },
 "kind": "StorageV2",
 "properties": {}
 }
],
 "outputs": {
 "storageAccountName": {
 "type": "string",
 "value": "[variables('storageAccountName')]"
 }
 }
}
```

```

28. Under the Parameters tab, clear the **storageAccountType** check box and note that the drop-down list contains only values included in the Resource Manager template under **allowedValues**. Select the box to set it back to a dynamic parameter.

29. Select **Add** to add this artifact to the blueprint.

Template **Parameters**

storageAccountType ⓘ
Standard_LRS

This value should be specified when the blueprint is assigned

location ⓘ
[resourceGroups('ResourceGroup').location]

This value should be specified when the blueprint is assigned

30. Your completed blueprint should look similar to the following. Notice that each artifact has **x out of y parameters populated** in the **PARAMETERS** column. The dynamic parameters are set during each assignment of the blueprint.

Create blueprint

Basics **Artifacts**

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

| NAME | ARTIFACT TYPE | PARAMETERS |
|--|---------------------------------|---------------------------------|
| Subscription | | |
| [User group or application name] : Contributor | Role assignment | 0 out of 1 parameters populated |
| Apply tag and its default value to resource groups | Policy assignment | 0 out of 2 parameters populated |
| + Add artifact... | | |
| ResourceGroup | | |
| StorageAccount | Azure Resource Manager template | 0 out of 2 parameters populated |
| + Add artifact... | | |

31. Now that all planned artifacts have been added, select **Save Draft** at the bottom of the page.

40.1.2 Task 2: Edit a blueprint

In Create a blueprint, you didn't provide a description or add the role assignment to the new resource group. You can fix both by following these steps:

1. Select **Blueprint definitions** from the page on the left.
2. In the list of blueprints, right-click the one that you previously created and select **Edit blueprint**.
3. In **Blueprint description**, provide some information about the blueprint and the artifacts that compose it. In this case, enter something like: **This blueprint sets tag policy and role assignment on the subscription, creates a ResourceGroup, and deploys a resource template and role assignment to that ResourceGroup.**
4. Select **Next : Artifacts** at the bottom of the page or the **Artifacts** tab at the top of the page.
5. Add a role assignment under the resource group:
6. Select the **+ Add artifact** row directly under the **ResourceGroup** entry.
7. Select **Role assignment** for **Artifact type**.

8. Under **Role**, select **Owner**, and clear the check box under the **Add user, app or group** box.
9. Search for and select a user, app, or group to add. This artifact uses a static parameter set the same in every assignment of this blueprint.
10. Select **Add** to add this artifact to the blueprint.

* Artifact type

Role assignment

You can choose to fill these parameters in now or when assigning the blueprint.

Role ⓘ

Owner

Add user, app or group ⓘ

Contoso

This value should be specified when the blueprint is assigned

11. Your completed blueprint should look similar to the following. Notice that the newly added role assignment shows **1 out of 1 parameters populated**. That means it's a static parameter.

Edit blueprint

| NAME | ARTIFACT TYPE | PARAMETERS |
|--|---------------------------------|---------------------------------|
| Subscription | | |
| [User group or application name] : Contributor | Role assignment | 0 out of 1 parameters populated |
| Apply tag and its default value to resource groups | Policy assignment | 0 out of 2 parameters populated |
| + Add artifact... | | |
| ResourceGroup | | |
| StorageAccount | Azure Resource Manager template | 0 out of 2 parameters populated |
| Contoso : Owner | Role assignment | 1 out of 1 parameters populated |
| + Add artifact... | | |

12. Select **Save Draft** now that it has been updated.

40.1.3 Task 3: Publish a blueprint

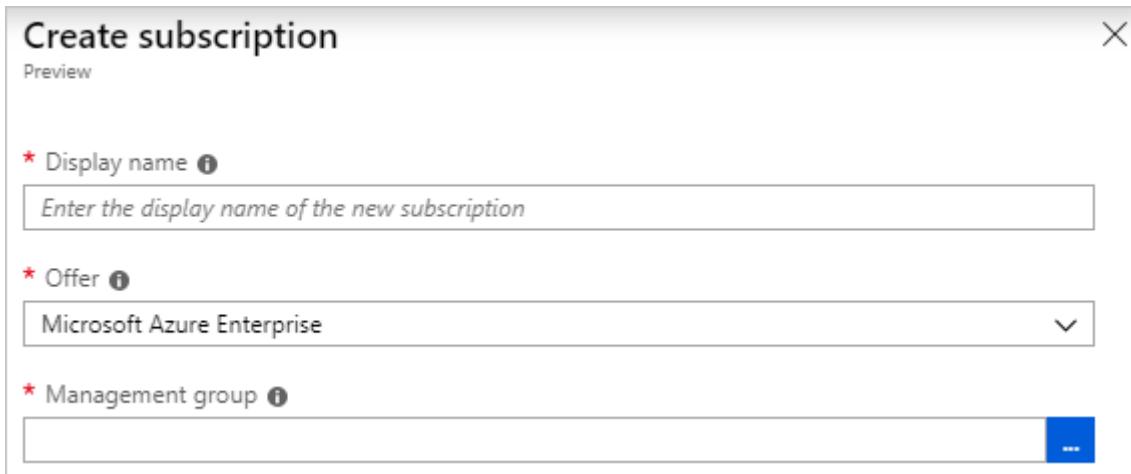
Now that all the planned artifacts have been added to the blueprint, it's time to publish it. Publishing makes the blueprint available to be assigned to a subscription.

1. Select **Blueprint definitions** from the page on the left.
2. In the list of blueprints, right-click the one you previously created and select **Publish blueprint**.
3. In the pane that opens, provide a **Version** (letters, numbers, and hyphens with a maximum length of 20 characters), such as **v1**. Optionally, enter text in **Change notes**, such as **First publish**.
4. Select **Publish** at the bottom of the page.

40.1.4 Task 4: Assign a blueprint

After a blueprint has been published, it can be assigned to a subscription. Assign the blueprint that you created to one of the subscriptions under your management group hierarchy. If the blueprint is saved to a subscription, it can only be assigned to that subscription.

1. Select **Blueprint definitions** from the page on the left.
2. In the list of blueprints, right-click the one that you previously created (or select the ellipsis) and select **Assign blueprint**.
3. On the **Assign blueprint** page, in the **Subscription** drop-down list, select the subscriptions that you want to deploy this blueprint to. *Skip this step if you are using an Azure Pass or lab Hoster solution*
If there are supported Enterprise offerings available from Azure Billing, a **Create new** link is activated under the Subscription box. Follow these steps:
 - a. Select the **Create new** link to create a new subscription instead of selecting existing ones.
 - b. Provide a **Display name** for the new subscription.
 - c. Select the available **Offer** from the drop-down list.
 - d. Use the ellipsis to select the management group that the subscription will be a child of.
 - e. Select **Create** at the bottom of the page.



Important: The new subscription is created immediately after you select **Create**.

Note: An assignment is created for each subscription that you select. You can make changes to a single subscription assignment at a later time without forcing changes on the remainder of the selected subscriptions.

4. For **Assignment name**, provide a unique name for this assignment.
5. In **Location**, select a region for the managed identity and subscription deployment object to be created in. Azure Blueprint uses this managed identity to deploy all artifacts in the assigned blueprint.
6. Leave the **Blueprint definition version** drop-down selection of **Published** versions on the **v1** entry. (The default is the most recently published version.)
7. For **Lock Assignment**, leave the default of **Don't Lock**.

Lock Assignment

Don't Lock **Read Only** **Do Not Delete**

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources.
[Learn more](#)

Managed Identity ?

- System assigned
 User assigned

8. Under **Managed Identity**, leave the default of **System assigned**.
9. For the subscription level role assignment [**User group or application name**] : **Contributor**, search for and select a user, app, or group. *You may skip this step if you have no users or groups*
10. For the subscription level policy assignment, set **Tag Name** to **CostCenter** and the **Tag Value** to **ContosoIT**.
11. For **ResourceGroup**, provide a **Name** of **StorageAccount** and a **Location** of **East US 2** from the drop-down list.
- Note:** For each artifact that you added under the resource group during blueprint definition, that artifact is indented to align with the resource group or object that you'll deploy it with. Artifacts that either don't take parameters or have no parameters to be defined at assignment are listed only for contextual information.
12. On the Azure Resource Manager template **StorageAccount**, select **Standard_GRS** for the **storageAccountType** parameter.
13. Read the information box at the bottom of the page, and then select **Assign**. *Due to the limitations of lab environments you may receive an error. This can be ignored and continue to the next task*

40.1.5 Task 5: Track deployment of a blueprint

When a blueprint has been assigned to one or more subscriptions, two things happen:

- The blueprint is added to the **Assigned blueprints** page for each subscription.
- The process of deploying all the artifacts defined by the blueprint begins.

Now that the blueprint has been assigned to a subscription, verify the progress of the deployment:

1. Select **Assigned blueprints** from the page on the left.
2. In the list of blueprints, right-click the one that you previously assigned and select **View assignment details**.

3. On the **Blueprint assignment** page, validate that all artifacts were successfully deployed and that there were no errors during the deployment. If errors occurred, see [Troubleshooting blueprints](#) for steps to determine what went wrong.

40.1.6 Task 6: Unassign a blueprint

If you no longer need a blueprint assignment, remove it from a subscription. The blueprint might have been replaced by a newer blueprint with updated patterns, policies, and designs. When a blueprint is removed, the artifacts assigned as part of that blueprint are left behind. To remove a blueprint assignment, follow these steps:

1. Select **Assigned blueprints** from the page on the left.
2. In the list of blueprints, select the blueprint that you want to unassign. Then select the **Unassign blueprint** button at the top of the page.
3. Read the confirmation message and then select **OK**.

40.1.7 Task 6: Delete a blueprint

1. Select **Blueprint definitions** from the page on the left.
2. Right-click the blueprint that you want to delete, and select **Delete blueprint**. Then select **Yes** in the confirmation dialog box.

Note: Deleting a blueprint in this method also deletes all published versions of the selected blueprint. To delete a single version, open the blueprint, select the **Published versions** tab, select the version that you want to delete, and then select **Delete This Version**. Also, you can't delete a blueprint until you've deleted all blueprint assignment of that blueprint definition.

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**

Results: You have now completed this lab.

41 Module 2: Lab 1 - Monitor & Autoscale

Autoscale is a built-in feature of Cloud Services, Mobile Services, Virtual Machines, and Websites that helps applications perform their best when demand changes. Of course, performance means different things for different applications. Some apps are CPU-bound, others memory-bound. For example, you could have a web app that handles millions of requests during the day and none at night. Autoscale can scale your service by any of these—or by a custom metric you define.

41.1 Exercise 1: Lab setup

1. Go to the following URL in the browser:

https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FMicrosoft%2F500-Azure-Security%2Fmaster%2FAllfiles%2FLabs%2FMod2_Lab01%2Ftemplate.json

This will deploy a new app and app service plan from a template that can then be used to demonstrate the scale up options in AZ500 Mod2 Lab 1.

2. Select **Create a new Resource Group**
3. Type a **unique** name for the **Site Name** and **Service Plan**.
4. Agree to the terms and click **Purchase**

41.2 Exercise 2: Create your first Autoscale setting

Let's now go through a simple step-by-step walkthrough to create your first Autoscale setting.

1. Open the **Autoscale** blade in Azure Monitor and select a resource that you want to scale. You can select the app service plan that you created during the setup
2. Note that the current instance count is 1. Click **Custom autoscale**.
3. Provide a name for the scale setting, and then click **Add a rule**.
4. Notice the scale rule options that open as a context pane on the right side. By default, this sets the option to scale your instance count by 1 if the CPU percentage of the resource exceeds 70 percent. Leave it at its default values and click **Add**.
5. You've now created your first scale rule. Note that the UI recommends best practices and states that "It is recommended to have at least one scale in rule." To do so:
 - Click **Add a rule**.
 - Set **Operator** to **Less than**.
 - Set **Threshold** to **20**.
 - Set **Operation** to **Decrease count by**.
6. Click **Add**
7. Click **Save**.

Note: If you receive an error "Microsoft.insights not registered" (Add button grayed out) go to your Subscription blade and under Resource Providers register "Microsoft.insights" and wait a few minutes for registration then retry. If it does not register, continue to the next exercise.

Congratulations! You've now successfully created your first scale setting to autoscale your web app based on CPU usage.

41.3 Exercise 3: Scale based on a schedule

In addition to scale based on CPU, you can set your scale differently for specific days of the week.

1. Click **Add a scale condition**.
2. Setting the scale mode and the rules is the same as the default condition.
3. Select **Repeat specific days** for the schedule.
4. Select the days and the start/end time for when the scale condition should be applied.

41.4 Exercise 4: Scale differently on specific dates

In addition to scale based on CPU, you can set your scale differently for specific dates.

1. Click **Add a scale condition**.
2. Setting the scale mode and the rules is the same as the default condition.
3. Select **Specify start/end dates** for the schedule.

4. Select the start/end dates and the start/end time for when the scale condition should be applied. Click **Save**.

41.5 Exercise 5: View the scale history of your resource

1. Whenever your resource is scaled up or down, an event is logged in the activity log. You can view the scale history of your resource for the past 24 hours by switching to the **Run history** tab.
2. If you want to view the complete scale history (for up to 90 days), select **View more details in the Activity Log**. The activity log opens, with Autoscale pre-selected for your resource and category.

41.6 Exercise 6: View the scale definition of your resource

1. Autoscale is an Azure Resource Manager resource. You can view the scale definition in JSON by switching to the **JSON** tab.
2. You can make changes in **JSON** directly, if required. These changes will be reflected after you save them.

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**

Results: You have now completed this lab.

42 Module 3: Classify a SQL Database

42.1 Exercise 1: Classify your SQL Database

42.1.1 Task 1: Lab Setup

1. In your browser, navigate to the following URL to open the ARM template:
<https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2Faz-quickstart-templates%2F101-sql-database%2Fazuredeploy.json>
2. Under **Resource group** click create new and use the default name "**Mod3Lab1**"
3. You can use the default populated **SQL server name** with a **unique** string added to make a **globally unique** name
4. Click **Purchase**. warning **Note:** You must wait for the SQL database with the test data to deploy
5. Sign-in to the Azure portal.
6. **Select** the resource group of **Mod3Lab1**
7. **Click** your unique **SQL server name**
8. Under the **Security** heading in the **Azure SQL Database** pane, navigate to **Advanced Data Security**.
9. Select **ON** under **Advanced Data Security**
10. **Click Save**
11. Return to the **Mod3Lab1** resource group
12. **Select** the **SQL databse AZ500LabDb** (your unique **SQL server name/AZ500LabDb**)
13. **Click** Advanced Data Security again
14. **Click** the bar at the top **Complete Advanced Data Security setup by selecting a storage account for Vulnerability Assesment**
15. Make sure the option for **Advanced Data Security** is set to **On**
16. **Click** storage account
17. **Click** create new
18. For the name use **mod3lab1yourname** replacing **yourname** with your name to make it unique but memorable

19. Click **OK**
20. Select the **save** option
21. Return to the previous **Advanced Data Security** pane
22. Select the **Data discovery** and **classification** card.

42.2 Exercise 2: Begin Classification

1. To begin classifying your data, select the **Classification tab** at the top of the window.
2. The classification engine scans your database for columns containing potentially sensitive data and provides a list of recommended column classifications.
3. To view and apply classification recommendations:
 - View the list. To view the list of recommended column classifications, select the **recommendations** panel at the top of the window. (**Blue Bar**)
4. Click **Select all** in the top left to select all recommendations
 - To manually classify columns as an alternative to or in addition to the recommendation-based classification, in the top menu of the window, select Add classification.
 - In the Add classification blade, configure the five fields that display, and then select Add classification:
 - **Schema name**
 - **Table name**
 - **Column name**
 - **Information type**
 - **Sensitivity label**.
5. Click **Accept Selected Reccomendations**
6. To complete your classification and persistently label (**tag**) the database columns with the new classification metadata, select **Save**.
7. Upon returning to the **Advanced Data Security** pane you will be able to see in the overview pane for Data classification an overview of the data that was classified.

Results: You have now classified information in a SQL database on Azure for GDPR and data protection compliance

43 Module 3: Auditing a Database

43.1 Exercise 1: Enable auditing on your database

43.1.1 Task 1: Lab Setup

1. In your browser, navigate to the following URL to open the ARM template:


```
https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2F
```
2. Under **Resource group** click create new and use the default name "**Mod3Lab2**"
3. You can use the default **populated SQL server** name with a **unique** string added to make a **globally unique** name
4. Click **Purchase** warning **Note:** You must wait for the SQL database with the test data to deploy

43.1.2 Task 2: Enable auditing on your database

1. Select your resource group created in the lab setup
2. Select the SQL server **your unique SQL Server name**
3. Under **Security**, select **Auditing**
4. Switch **Auditing** to **ON**.
5. Select **storage** as the location to send the audit logs to

6. Click **Configure**
7. Select **Your Subscription**
8. Click **Storage account** then if necessary click **Create New**. The Create storage account blade should open..
9. Name the storage account **mod3lab2yourname** ensuring you replace **yourname** with a unique name using lowercase letters
10. **Click OK.**
11. Change the retention days to **5** and click **OK**
12. Click **Save** to save the **auditing configuration**

43.2 Exercise 2: Review audit logs

43.2.1 Task 1: Review audit logs on the SQL DB.

1. To review audit logs for a database return to the resource group created in the lab setup
2. Click **AZ500LabDb (your unique SQL Server name/AZ500LabDb)** to select your test database
3. Under **Security**, select **Auditing**

Note: The Auditing looks off here but it is set on the underlying server level so it is turned on for this database
4. Click **View Audit Logs.**

Note: Here you will review the output of the audit logs of the database including any attempted SQL injections. Since this is a test database created recently, there will be minimal audits if any in the log at the current time.

If server auditing is enabled, the database-configured audit will exist side-by-side with the server audit. Notice that you can select for audit logs to be written to an Azure storage account, to a Log Analytics workspace for consumption by Azure Monitor logs, or to Event Hub for consumption using an event hub. You can configure any combination of these options, and audit logs will be written to each.

Results: You have now setup up auditing on a SQL database and reviewed where to view the auditing output

44 Module 3: Analyze audit logs and reports

44.1 Exercise 1: Get started with SQL database auditing

44.1.1 Task 0: Lab Setup

1. In your browser, navigate to the following URL to open the ARM template:
<https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2Faz-quickstart-templates%2F101-sql-audit%2Fazuredeploy.json>
2. Under **Resource group** click create new and use the default name "**Mod3Lab3**"
3. You can use the default populated SQL server name with a unique string added to make a globally unique name.
4. Click **Purchase**

44.1.2 Task 1 - Set up auditing for your database

1. **Navigate to Resource Groups**
2. **Select** your resource group created above ("**Mod3Lab3**" if you chose the same name as the instructions)
3. **Click** your **SQL Server** name
4. On the left pane click auditing
5. **Change** auditing to **ON** from **OFF**. warning **Note:** You now have the option to select where you wish audit logs to be written to.
6. **Select** all **3** options, **Storage**, **Log analytics**, **Event hub**.

7. Under Storage, Click configure.
8. Click subscription and select your subscription
9. Click storage account
10. Under create storage account input a unique name (**e.g. mod3lab3yourname**)
11. Click OK.
12. When validated click OK again
13. Under Log analytics click configure
14. Click create new workspace
15. Enter the following settings

| Log Analytics Workspace | Subscription | Resource Group | Location | Pricing Tier |
|-------------------------|-------------------|-------------------------------------|----------|---------------|
| Mod3Lab3YOURNAME | Your Subscription | The RG you created in the lab setup | East US | Per GB (2018) |

16. Click OK. warning **Note:** Setting up Event Hub requires extra steps as the Azure portal does not allow you to create an event hub from this location
17. To set up an **Event Hub** for configuration, click **Azure Cloud Shell** at the top of the **Portal**.
18. Enter the following **Powershell Commands**.

Note Replace the section **{GlobalUniqueName}** with a globally unique name

```
New-AzEventHubNamespace -ResourceGroupName Mod3Lab3 -NamespaceName {GlobalUniqueName} -Location e
New-AzEventHub -ResourceGroupName Mod3Lab3 -NamespaceName {GlobalUniqueName} -EventHubName Mod3La
```

Return to the Advanced Data Security blade in portal. (**Note** The Event Hub Namespace will be the unique name you specified).
19. When these commands have completed click **configure under event hubs**
20. Select the following information

| Subscription | Hub Namespace | Hub Name | Hub Policy Name |
|-------------------|---------------|----------|---------------------------|
| Your Subscription | Mod3Lab3 | mod3lab3 | RootManageSharedAccessKey |

21. Click OK
22. You can now click **Save** on the **Auditing Settings** page

Result: You have now turned on auditing for your SQL database
23. To access the logs return to the **Resource group** where the **SQL Database** and **Server** reside
24. Select the **Mod3Lab3** Log analytics workspace you created earlier
25. Click logs
26. Click **Get Started**
27. In the query space enter the following code and click **Run**.


```
Event | where Source == "MSSQLSERVER"
```
28. You will not see any results, please read the below warning **Note:** Because we have set up logs on a new database with test data, there are minimal log entries available to see. To show how logs are displayed, we can use the example log analytics website that is populated with example data.

44.1.3 Task 2 - Analyze audit logs and reports

1. Visit <https://portal.loganalytics.io/demo> in a new web browser tab, this will direct you to a demo log analytics workspace with demo data populated

2. In the query space enter the following code and **click Run**.

```
Event | where Source == "MSSQLSERVER"
```

3. From here you can expand some of the example audit logs to view what they would look like in a live system

4. In the query space enter the following code and **Click Run**.

```
Event  
| where EventLevelName == "Error"  
| where TimeGenerated > ago(1d)  
| where Source != "HealthService"  
| where Source != "Microsoft-Windows-DistributedCOM"  
| summarize count() by Source
```

5. **Click chart**

6. From here you can review how log data can be displayed as chart data

7. **Click the Stacked Column** drop down and select **Pie**

8. Here you can see the same data as a different chart

9. From the top right of the window you can **Click Export** to export the data as **CSV**.

The query language used by log analytics is called the Kusto query language. The full documentation for this language can be found here <https://docs.microsoft.com/en-us/azure/kusto/query/>

Results: You have now completed the setup of logs on a SQL database and run queries against the log analytics workspace to view the audit logs that will be generated

45 Module 4: Lab 1 - Azure Monitor

Azure Monitor maximizes the availability and performance of your applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

In this lab you will configure Azure Monitor to:

- Collect data from an Azure virtual machine.
- Use Application Insights to monitor your website.

45.1 Exercise 1: Collect data from an Azure virtual machine with Azure Monitor

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation. Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs. This exercise shows you how to configure and collect data from your Azure Linux or Windows VMs using the VM extension with a few easy steps.

45.1.1 Task 1: Deploy an Azure VM to monitor.

1. Open the Azure Cloud Shell and run the following two commands to create a Resource Group and Azure VM that you will use to monitor:

```
New-AzResourceGroup -Name myResourceGroup -Location EastUS
```

```
New-AzVm -ResourceGroupName "myResourceGroup" -Name "myVM" -Location "East US" -VirtualNetworkName
```

2. When prompted for credentials enter **LocalAdmin** as the User and use the password **Pa55w.rd1234**

45.1.2 Task 2: Create a workspace

1. In the Azure portal, select **All services**. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics workspaces**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with options like 'Create a resource', 'Home', 'Dashboard', 'All services' (which is selected and highlighted in blue), 'FAVORITES', 'All resources', and 'Resource groups'. The main area is titled 'All services' with a search bar containing 'Log Anal'. Below the search bar, there's a category 'All' under 'General'. To the right, a list of services is shown with their icons, names, and star ratings. The first item in the list is 'Log Analytics workspaces'.

| Service | Description | Rating |
|---|-------------------------------------|--------|
| Log Analytics workspaces | Keywords: Microsoft Log Analytics | ★ |
| SignalR | | ★ |
| Service catalog managed application definitions | | ★ |
| Managed Desktop | Keywords: Microsoft Managed Desktop | ★ |

2. Select **+ Add**, and then select choices for the following items:

- Select a **Subscription** to link to by selecting from the drop-down list if the default selected is not appropriate.
- For **Resource Group**, select **myResourceGroup** which is the Resource Group that contains the VM you created in Task 1.
- Provide a name for the new **Log Analytics workspace**, such as *myWorkspaceDemo*.
- Select the **EastUS** as the location.
- Click **Next: Pricing tier**

Create Log Analytics workspace

Basics Pricing tier Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) X

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription * ⓘ [REDACTED] ▼

Resource group * ⓘ (New) myResourceGroup ▼

[Create new](#)

Instance details

Name * ⓘ myWorkspaceDemo2222 ✓

Region * ⓘ (US) East US ▼

[Review + Create](#)

[« Previous](#)

[Next : Pricing tier >](#)

- Leave the pricing Tier as **Per Gb (2018)**

Create Log Analytics workspace

Basics **Pricing tier** Tags Review + Create

The cost of your workspace depends on the pricing tier and what solutions you use.
To learn more about Log Analytics pricing [click here](#)

Pricing tier

You can change to a Capacity Reservation tier after your workspace is created. [Learn more](#)
To learn more about access to legacy pricing tiers [click here](#)

Pricing tier *

Pay-as-you-go (Per GB 2018)

3. After providing the required information on the **Log Analytics workspace** pane, select **Review + Create** then click **Create**.
4. While the information is verified and the workspace is created, you can track its progress under **Notifications** from the menu.

45.1.3 Task 2: Enable the Log Analytics VM Extension

For Windows and Linux virtual machines already deployed in Azure, you install the Log Analytics agent with the Log Analytics VM Extension. Using the extension simplifies the installation process and automatically configures the agent to send data to the Log Analytics workspace that you specify. The agent is also upgraded automatically when a newer version is released, ensuring that you have the latest features and fixes. Before proceeding, verify the VM is running otherwise the process will fail to complete successfully.

1. In the Azure portal, select **All services** found in the upper left-hand corner. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics workspaces**.
2. In your list of Log Analytics workspaces, select **myWorkspaceDemo** created earlier.
Note: The name of your workspace may be different to **myWorkspaceDemo**.
3. On the left-hand menu, under Workspace Data Sources, select **Virtual machines**.
4. In the list of **Virtual machines**, select a virtual machine you want to install the agent on. Notice that the **Log Analytics connection status** for the VM indicates that it is **Not connected**.
5. In the details for your virtual machine, select **Connect**. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the **Status** shows **Connecting**.
6. After you install and connect the agent, the **Log Analytics connection status** will be updated with **This workspace**.

45.1.4 Task 3: Collect event and performance of a Windows VM.

Azure Monitor can collect events from the Windows event logs or Linux Syslog and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows system log and Linux Syslog, and several common performance counters to start with.

1. On the Log Analytics workspaces blade, select **Advanced settings**.

2. Select **Data**, and then select **Windows Event Logs**.
3. You add an event log by typing in the name of the log. Type **System** and then select the plus sign +.
4. In the table, check the severities **Error** and **Warning**.
5. Select **Save** at the top of the page to save the configuration.
6. Select **Windows Performance Counters** to enable collection of performance counters on a Windows computer.
7. When you first configure Windows Performance counters for a new Log Analytics workspace, you are given the option to quickly create several common counters. They are listed with a checkbox next to each.

Select **Add the selected performance counters**. They are added and preset with a ten second collection sample interval.

8. Select **Save** at the top of the page to save the configuration.

45.1.5 Task 4: View data collected

Now that you have enabled data collection, lets run a simple log search example to see some data from the target VMs.

1. In the selected workspace, from the left-hand pane, select **Logs**.
2. Click Get started. On the Logs query page, type **Perf** in the query editor and select **Run**.

For example, the query in the following image returned 10,000 performance records. Your results will be significantly less due to the VM having only been ran for a few minutes.

| Perf | | | | | | |
|--|----------|-----------------------|------------------------|---|--|-----------------|
| Completed. Showing partial results from the last 24 hours. ? | | | | | ⌚ 00:00:01.328 | 💾 10000 records |
| TABLE | | CHART | | Columns ▼ | Display time (UTC+00:00) ▼ | |
| Drag a column header and drop it here to group by that column | | | | | | |
| TimeGenerated [UTC] | Computer | ObjectName | CounterName | InstanceName | | |
| 2019-08-22T15:33:06.917 | SVR01 | Network Adapter | Bytes Sent/sec | Microsoft Hyper-V Network Adapter _2 | | |
| 2019-08-22T15:33:06.917 | SVR01 | Network Adapter | Bytes Sent/sec | Microsoft Hyper-V Network Adapter | | |
| 2019-08-22T15:33:06.917 | SVR01 | Network Adapter | Bytes Sent/sec | Microsoft Kernel Debug Network Adapter | | |
| 2019-08-22T15:33:06.917 | SVR01 | Network Adapter | Bytes Sent/sec | Teredo Tunneling Pseudo-Interface | | |
| 2019-08-22T15:33:06.917 | SVR01 | Network Adapter | Bytes Sent/sec | isatap.szcgi5dxtbourfnflgghmf25qg.bx.ii | | |
| 2019-08-22T15:33:06.917 | SVR01 | Processor | % Processor Time | _Total | | |
| 2019-08-22T15:33:06.917 | SVR01 | LogicalDisk | Disk Transfers/sec | C: | | |
| 2019-08-22T15:33:06.917 | SVR01 | LogicalDisk | Disk Transfers/sec | D: | | |
| 2019-08-22T15:33:06.917 | SVR01 | LogicalDisk | Disk Transfers/sec | _Total | | |
| 2019-08-22T15:33:06.917 | SVR01 | System | System Up Time | | | |
| 2019-08-22T15:33:06.917 | SVR01 | System | Processor Queue Length | | | |
| 2019-08-22T15:33:06.917 | SVR01 | LogicalDisk | % Free Space | C: | | |
| 2019-08-22T15:33:06.917 | SVR01 | LogicalDisk | % Free Space | D: | | |
| 2019-08-22T15:33:06.917 | SVR01 | LogicalDisk | % Free Space | _Total | | |

◀ ▶ Page 1 of 200 ▶ ▷ 50 items per page

45.2 Exercise 2: Monitor Websites with Azure Monitor Application Insights

With Azure Monitor Application Insights, you can easily monitor your website for availability, performance, and usage. You can also quickly identify and diagnose errors in your application without waiting for a user to report them. Application Insights provides both server-side monitoring as well as client/browser-side monitoring capabilities.

This exercise guides you through adding the open source Application Insights JavaScript SDK which allows you to understand the client/browser-side experience for visitors to your website.

45.2.1 Task 1: Enable Application Insights

Application Insights can gather telemetry data from any internet-connected application, running on-premises or in the cloud. Use the following steps to start viewing this data.

1. Select **Create a resource > IT & Management tools > Application Insights**.

A configuration box appears; use the following table to fill out the input fields.

| Settings | Value |
|----------------|-------------------------------|
| Name | Enter a Globally Unique Value |
| Resource Group | myResourceGroup |
| Location | East US |

2. Click **Review + Create** then click **Create**.

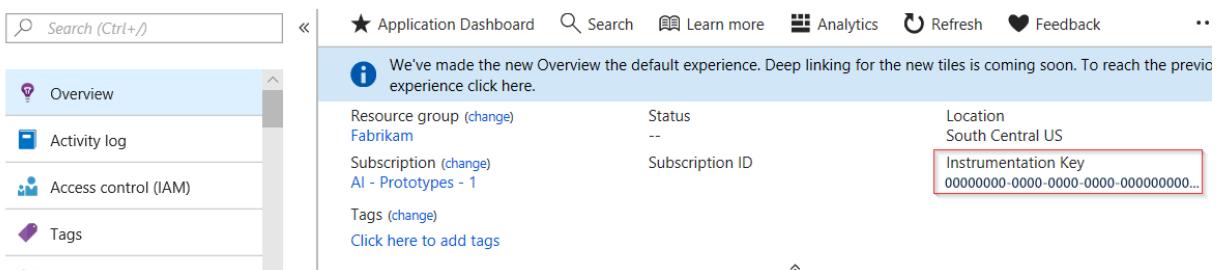
45.2.2 Task 2: Create an HTML file

1. On your local computer, create a file called `hello_world.html`. For this example the file will be placed on the root of the C: drive at `C:\hello_world.html`.
2. Copy the script below into `hello_world.html`:

```
<!DOCTYPE html>
<html>
<head>
<title>
Azure Monitor Application Insights
</title>
<script>
    var appInsights=window.appInsights||function(config)
    {
        function r(config){ t[config] = function(){ var i = arguments; t.queue.push(function(){ t[config].apply(this,i);}); };
        var t = { config:config },u=document,e=window,o='script',s=u.createElement(o),i,f;for(s.src=config;f(u.firstChild);)u.removeChild(f);
        instrumentationKey:'xxxxxxxx-xxxxxxx-xxxxxxx-xxxxxxxx' // REMOVE xxxx-xx... REPLACE WITH INSTRUMENTATION KEY
        );
        window.appInsights=appInsights;
        appInsights.trackPageView();
    </script>
</head>
<body>
<h1>Azure Monitor Application Insights Hello World!</h1>
<p>You can use the Application Insights JavaScript SDK to perform client/browser-side monitoring or server-side monitoring</p>
</body>
</html>
```

45.2.3 Task 3: Configure App Insights SDK

1. Navigate to the Applications Insights blade. Select **Overview** > **Essentials** > Copy your application's **Instrumentation Key**.



The screenshot shows the Azure Application Insights Overview page. On the left, there is a navigation sidebar with links for Search (Ctrl+/, Overview, Activity log, Access control (IAM), and Tags. The main content area has a header with Application Dashboard, Search, Learn more, Analytics, Refresh, and Feedback buttons. A message at the top says: "We've made the new Overview the default experience. Deep linking for the new tiles is coming soon. To reach the previous experience click here." Below this, there are sections for Resource group (Fabrikam), Status (--), Location (South Central US), Subscription (AI - Prototypes - 1), Subscription ID, and Tags (Click here to add tags). A red box highlights the "Instrumentation Key" field, which contains the value: 00000000-0000-0000-0000-000000000000.

2. Edit `hello_world.html` and add your instrumentation key and save the file.
3. Open `hello_world.html` in a local browser session. This will create a single pageview. You can refresh your browser to generate multiple test page views.

45.2.4 Task 4: Start monitoring in the Azure portal

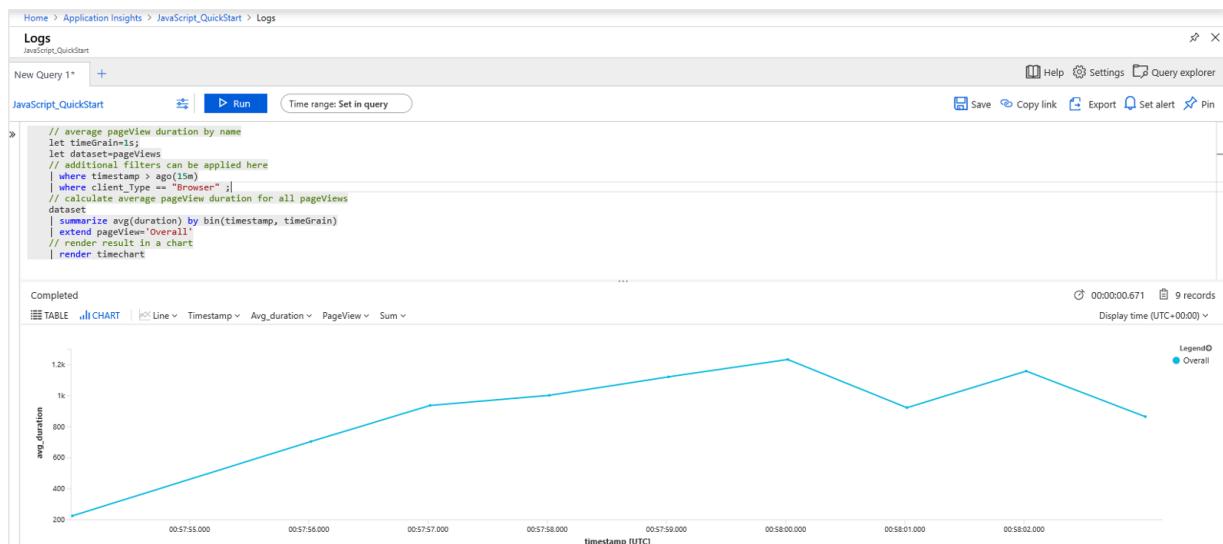
1. You can now reopen the Application Insights **Overview** page in the Azure portal, where you retrieved your instrumentation key, to view details about your currently running application. The four default charts on the overview page are scoped to server-side application data. Since we are instrumenting the client/browser-side interactions with the JavaScript SDK this particular view doesn't apply unless we also have a server-side SDK installed.
2. Click on **Logs (Analytics)**. This opens **Logs**, which provides a rich query language for analyzing all data collected by Application Insights. To view data related to the client-side browser requests run the following query then click **Run**:

```
// average pageView duration by name
let timeGrain=1s;
let dataset=pageViews
```

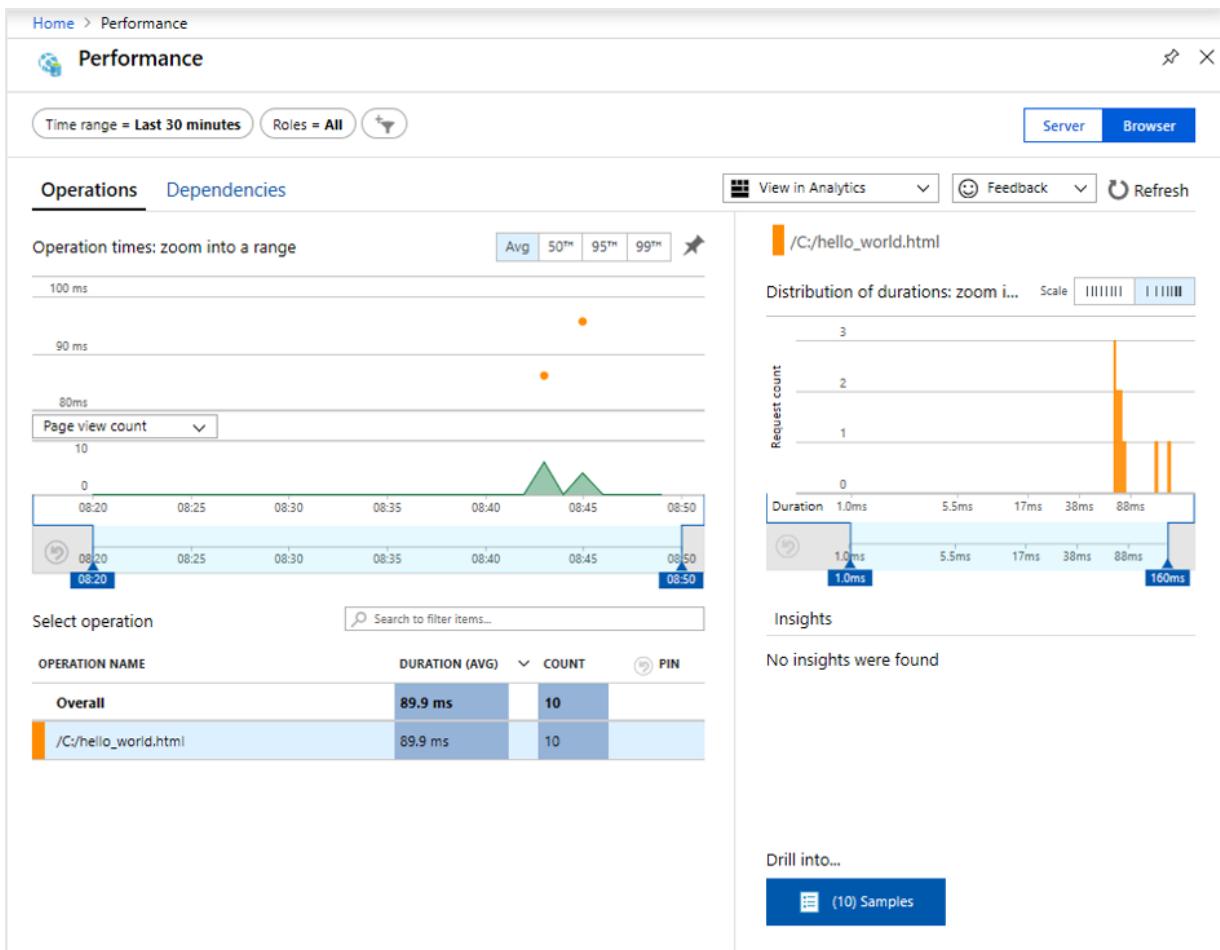
```

// additional filters can be applied here
| where timestamp > ago(15m)
| where client_Type == "Browser" ;
// calculate average pageView duration for all pageViews
dataset
| summarize avg(duration) by bin(timestamp, timeGrain)
| extend pageView='Overall'
// render result in a chart
| render timechart

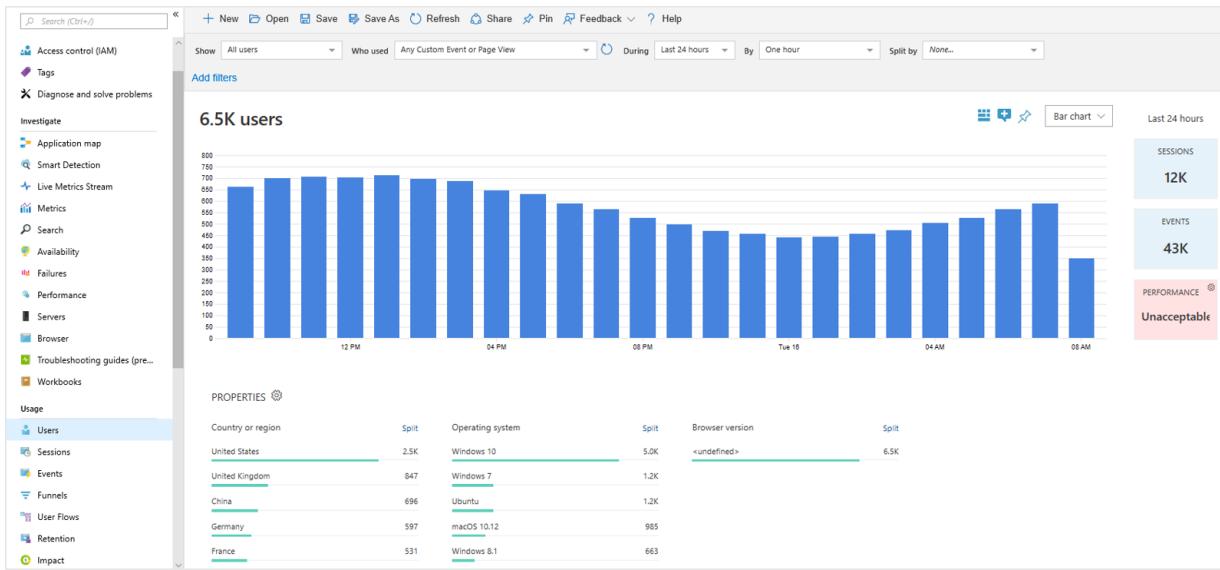
```



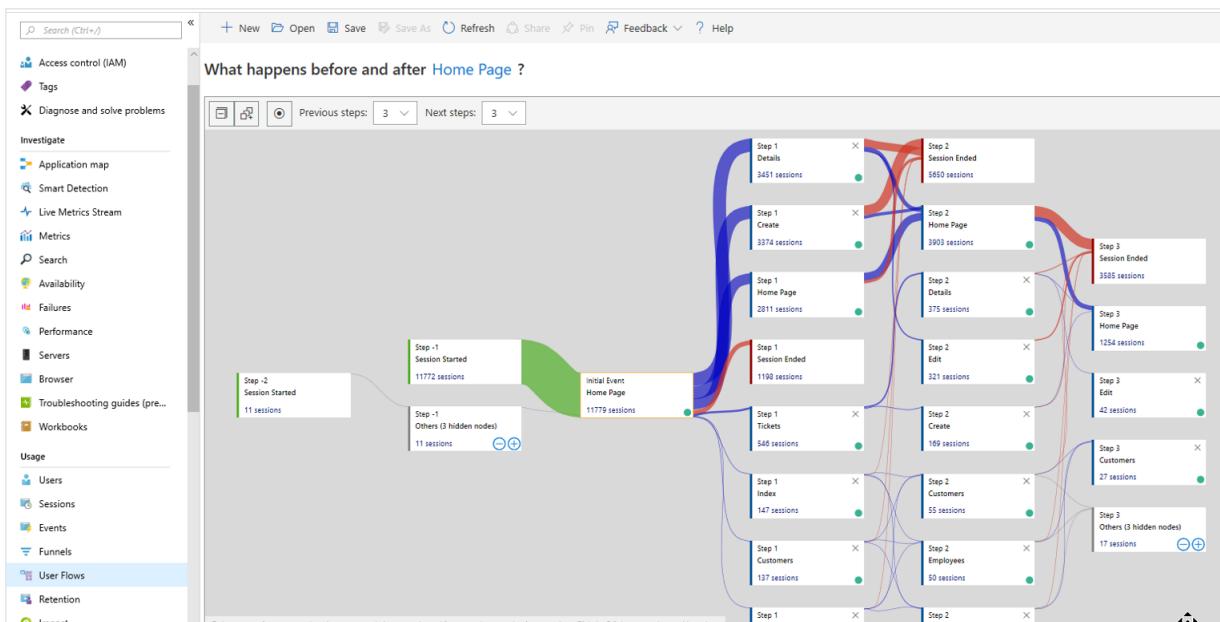
3. Go back to the **Overview** page. Click on **Performance** from under the **Investigate** header. Here you find metrics related to the performance of your website. There is also a corresponding view for analyzing failures and exceptions in your website. You can click **Samples** to drill into individual transaction details. From here, you can access the end-to-end transaction details. Change Local Time button from Last 24 hours to Last 30 Minutes. Change Server/Browser button to Browser.



- To begin exploring the user behavior analytics tools, from the main Application Insights menu select **Users** under the **Usage** header. Since we are testing from a single machine, we will only see data for one user. For a live website, the distribution of users might look as follows:



- If we had instrumented a more complex website with multiple pages, another useful tool is **User Flows**. With **User Flows** you can track the pathway visitors takes through the various parts of your website.



6. Leave all resources. You will use these in a future lab.

Results: In this lab, you learned how to monitor resources with Azure Monitor.

46 Module 4: Lab 2 -Security Center

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Keeping your resources safe is a joint effort between your cloud provider, Azure, and you, the customer. You have to make sure your workloads are secure as you move to the cloud, and at the same time, when you move to IaaS (infrastructure as a service) there is more customer responsibility than there was in PaaS (platform as a service), and SaaS (software as a service). Azure Security Center provides you the tools needed to harden your network, secure your services and make sure you're on top of your security posture.

46.1 Exercise 1: Onboard your Azure subscription to Security Center Standard

Azure Security Center provides unified security management and threat protection across your hybrid cloud workloads. While the Free tier offers limited security for your Azure resources only, the Standard tier extends these capabilities to on-premises and other clouds. Security Center Standard helps you find and fix security vulnerabilities, apply access and application controls to block malicious activity, detect threats using analytics and intelligence, and respond quickly when under attack. You can try Security Center Standard at no cost. To learn more, see the pricing page.

In this Exercise, you upgrade to the Standard tier for added security and install the Microsoft Monitoring Agent on your virtual machines to monitor for security vulnerabilities and threats.

46.1.1 Task 1: Automate data collection

Security Center collects data from your Azure VMs and non-Azure computers to monitor for security vulnerabilities and threats. Data is collected using the Microsoft Monitoring Agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. By default, Security Center will create a new workspace for you.

When automatic provisioning is enabled, Security Center installs the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created. Automatic provisioning is strongly recommended.

To enable automatic provisioning of the Microsoft Monitoring Agent:

1. In the Azure Portal, select the **Security Center** from the Hub menu.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service links like Home, Dashboard, All services, and Favorites. Under Favorites, 'Security Center' is highlighted with a red box. The main content area is titled 'Azure services' and includes links for Create a resource, Resource groups, Security Center, Storage accounts, Azure Active Directory, All resources, Monitor, Azure Sentinel, Log Analytics workspaces, and More services. Below this is a 'Recent resources' table:

Name	Type	Last Viewed
[?] myResourceGroup	Resource group	5 h ago
[?] nijkrdbjbjnfdk	Storage account	2 wk ago
[?] AZ500LabDb (az500labserver222/AZ500LabDb)	SQL database	2 wk ago
[?] Mod4Lab1	Resource group	2 wk ago
[?] Azure Pass - Sponsorship	Subscription	2 wk ago

Below the table is a 'Navigate' section with links for Subscriptions, Resource groups, All resources, and Dashboard. The 'Tools' section contains links for Microsoft Learn, Azure Monitor, Security Center, and Cost Management.

2. On the **Getting started** blade click **Upgrade**.
3. Under the Security Center main menu, select **Pricing & settings**.
4. On the row of the subscription, click on the subscription on which you'd like to change the settings.
5. In the **Data Collection** tab, set **Auto provisioning** to **On**.
6. Exit the blade **without** saving.

Note: Ensure you do not click save otherwise the following exercises will not function as expected.

The screenshot shows the 'Settings - Data Collection' blade for a specific subscription. The 'Data Collection' tab is selected. It displays the 'Auto Provisioning' setting, which is currently set to 'On'. A note below explains that if a VM already has either SCOM or OMS agent installed locally, the MMA extension will still be installed and connected to the configured workspace.

With this new insight into your Azure VMs, Security Center can provide additional Recommendations related to system update status, OS security configurations, endpoint protection, as well as generate additional Security alerts.

46.2 Exercise 2: Onboard Windows computers to Azure Security Center

After you onboard your Azure subscriptions, you can enable Security Center for resources running outside of Azure, for example on-premises or in other clouds, by provisioning the Microsoft Monitoring Agent.

This exercise shows you how to install the Microsoft Monitoring Agent on a Windows computer.

46.2.1 Task 1: Add new Windows computer

1. In the Azure Portal, select **Security Center**. **Security Center - Overview** opens.

The screenshot shows the Azure Security Center - Overview page. On the left, there's a navigation menu with sections like Overview, Getting started, Pricing & settings, Policy & compliance, Resource security hygiene, Advanced cloud defense, and Threat protection. The main area has three main sections: Policy & compliance, Resource security hygiene, and Threat protection. Policy & compliance includes a secure score of 280 out of 410, regulatory compliance (ISO 27001, Azure CIS 1.1.0, PCI DSS 3.2.1), and subscription coverage. Resource security hygiene shows recommendations, resource health by severity (Compute & apps resources, Data & storage resources, Networking resources, Identity & access resources), and threat protection (Security alerts over time). Threat protection shows security alerts by severity (High, Medium, Low) and attacked resources.

2. Under the Security Center main menu, select **Getting started**.

3. Select the **Install Agents** tab.

The screenshot shows the Security Center - Getting started page. At the top, there's a header with a cloud icon and the title. Below it is a search bar and a navigation bar with tabs: Upgrade (selected), Install Agents (highlighted with a red box), and Get Started. The main content area is titled "Install agents automatically" and says "The Microsoft Monitoring Agent will be automatically installed on all the virtual machines in selected subscription." It shows a section for "Select subscriptions on which agents will be installed" with one managed resource selected. A blue button at the bottom says "Install agents".

4. Scroll down to the Install agents automatically section and click **Install agents**.

Install agents automatically

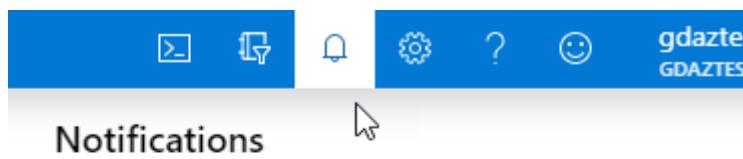
The Microsoft Monitoring Agent will be automatically installed on all the virtual machines in selected subscription.

^ Select subscriptions on which agents will be installed 1 Managed resources

<input checked="" type="checkbox"/> NAME	UNPROTECT...
<input checked="" type="checkbox"/> Azure Pass - Sponsorship	1

Install agents

5. Wait until the agent is install by monitoring the deployment.



6. Open the **Security Center** and click on **Compute & apps** then click on **VMs and Servers**.

Security Center | Compute & apps
Showing subscription 'CloudShare7'

Search (Ctrl+ /)

Add Servers

Overview

VMs and Servers

Resource type: All

Search resources

Name

Resources may take up to 24 hours to appear

POLICY & COMPLIANCE

- Coverage
- Secure Score
- Security policy
- Regulatory compliance

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- Networking
- IoT Hubs & resources
- Data & storage

7. Notice your Virtual Machine is now monitored.

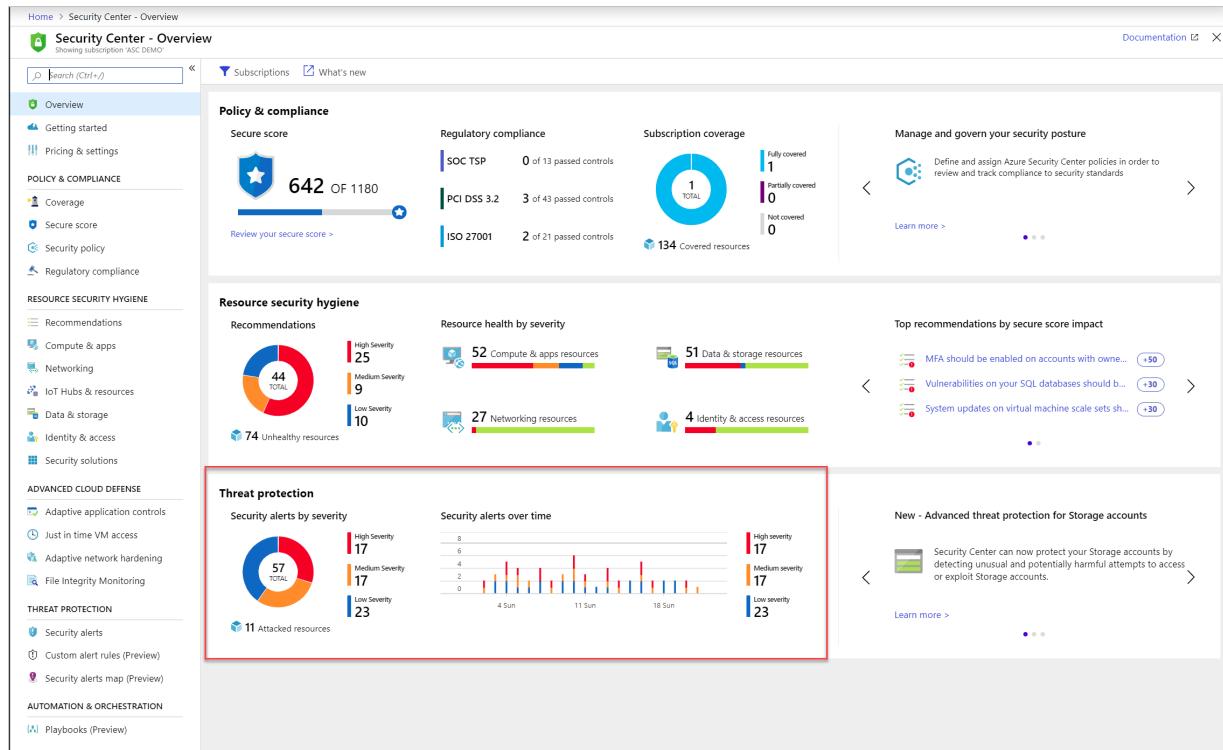
46.3 Exercise 3: Manage and respond to alerts in Azure Security Center

Security Center automatically collects, analyzes, and integrates log data from your Azure resources, the network, and connected partner solutions, like firewall and endpoint protection solutions, to detect real threats and reduce false positives. A list of prioritized security alerts is shown in Security Center along with the information you need to quickly investigate the problem and recommendations for how to remediate an attack.

46.3.1 Task 1: Manage your alerts

1. From the Security Center dashboard, see the **Threat protection** tile to view and overview of the alerts.

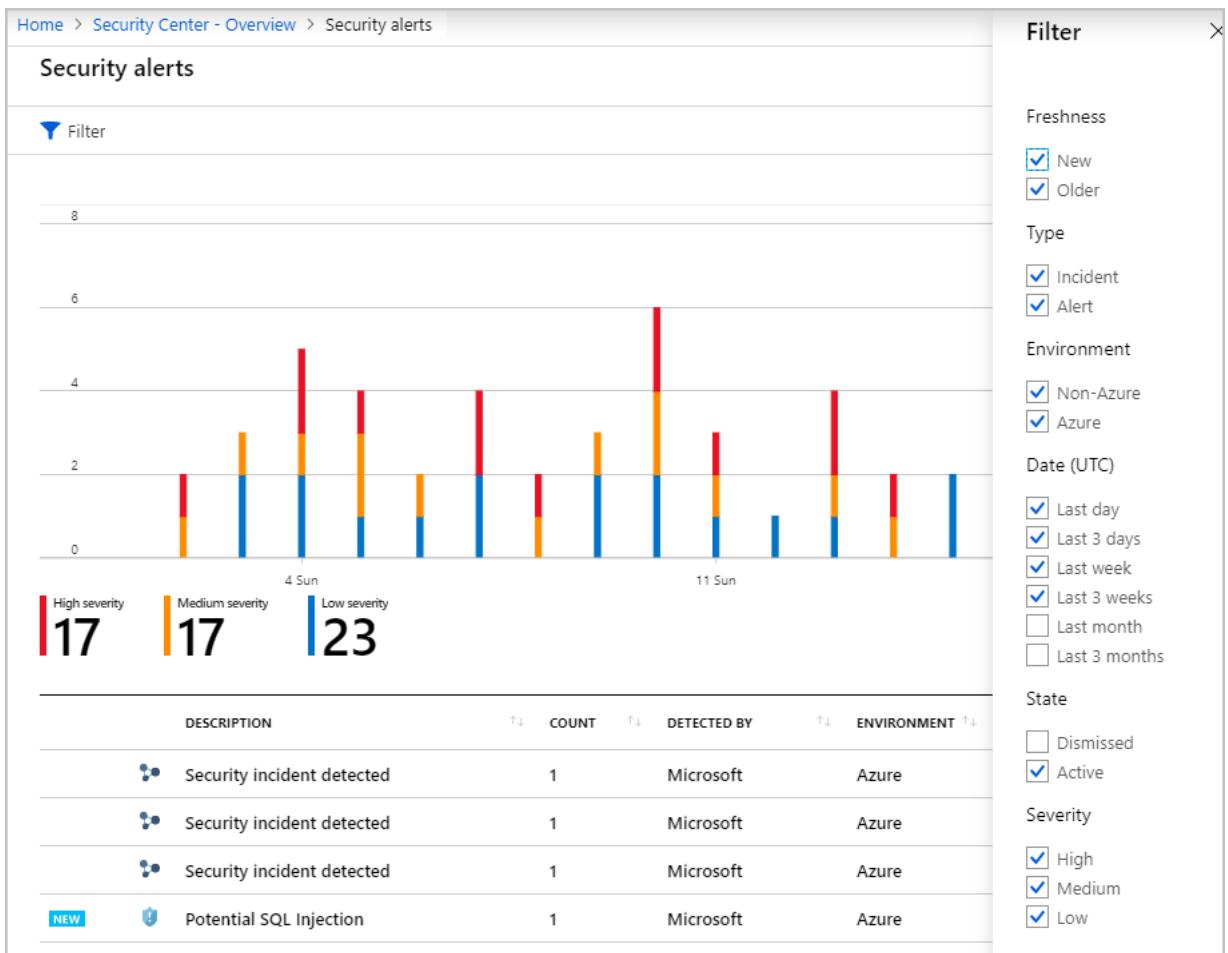
Note: If the tile displays **No security alerts**, you may have to wait some time for the evaluation to run.



2. To see more details about the alerts, click the tile. The screenshot below shows potential alerts you would see in the real world:



3. To filter the alerts shown, click **Filter**, and from the **Filter** blade that opens, select the filter options that you want to apply. The list updates according to the selected filter. Filtering can be very helpful. For example, you might want to address security alerts that occurred in the last 24 hours because you are investigating a potential breach in the system.



46.3.2 Task 2: Respond to recommendations

1. In the Azure Security Center click **Overview**.
2. From the Resource security hygiene list, in the **Resource health by severity** section select **Compute & apps resources**

The screenshot shows the Azure Security Center - Overview page. On the left, there's a navigation sidebar with links like Overview, Getting started, Pricing & settings, and sections for Policy & Compliance (Coverage, Secure score, Security policy, Regulatory compliance) and Resource Security Hygiene (Recommendations, Compute & apps, Networking, IoT Hubs & resources, Data & storage, Identity & access). The main content area has two main sections: 'Policy & compliance' and 'Resource security hygiene'. The 'Policy & compliance' section displays a secure score of 310 out of 440, regulatory compliance status for ISO 27001 (14 of 20 passed controls), Azure CIS 1.1.0 (12 of 16 passed controls), and PCI DSS 3.2.1 (31 of 39 passed controls). The 'Resource security hygiene' section shows recommendations (7 total, 6 High Severity, 1 Medium Severity, 0 Low Severity), unhealthy resources (2), and resource health by severity for Compute & apps resources (1) and Networking resources (0).

3. Review the recommendations.

This screenshot shows the 'Compute' recommendations page. It includes a navigation bar for Compute resources (Overview, VMs and Computers, VM scale sets, Cloud services, App services, Containers (Preview), Compute resources) and a search bar for recommendations. Below is a table of recommendations:

RECOMMENDATION	SECURE SCORE IMPACT	FAILED RESOURCES	SEVERITY
Just-In-Time network access control should be applied on virtual machines	+30	1 of 1 virtual machines	██████████
Vulnerability assessment solution should be installed on your virtual machines	+30	1 of 1 virtual machines	██████████
The rules for web applications on IaaS NSGs should be hardened	+20	1 of 1 virtual machines	██████████
Access should be restricted for permissive Network Security Groups with Internet-facing VMs	+20	1 of 1 virtual machines	██████████
Install endpoint protection solution on virtual machines	+15	1 of 1 virtual machines	██████████
Disk encryption should be applied on virtual machines	+10	1 of 1 virtual machines	██████████

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**

Results: You have now completed this lab and can move onto the next lab in the series

47 Module 4: Lab 3 - Event hub

Connect sending and receiving applications with Event Hubs so you can handle extremely high loads without losing data.

In this lab, you will:

- Create an Event Hub using the Azure portal
- Configure applications to send or receive messages through an Event Hub
- Evaluate Event Hub performance using the Azure portal

47.1 Exercise 1: Implementing Event Hub

47.1.1 Task 1: Enabling Event Hubs Namespace

1. Log into the Azure portal
2. In the search bar type **Event Hubs** and select **Event Hubs**
3. Click **+ Add** to add a new Event Hubs Namespace
 - Populate the fields with the following details:
 - **Name** : yourUniqueName
 - **Pricing Tier** : Standard
 - **Subscription**: yourSubscription
 - **Resource group**: Create New with name "EventHubRG"
 - **Location**: East US
 - **Throughput Units**: 2
4. Click Select **Review + Create** then select **Create**.

47.1.2 Task 2: Create a storage account for later user

Note: We also need to create a storage account and a blob store container to store events that will be sent to the Event Hubs later on

1. Search for **Storage Accounts** in the search bar and click on **Storage Accounts**
2. Click **Add**
3. Choose the Resource Group of **EventHubsRG** (Or the name of your resource group if you chose to use another)
4. Set the following options:
 - **Storage Account Name**: uniqueName (unique across all of azure)
 - **location**: east US
 - **Performance**: Standard
 - **Account Kind**: General purpose v2
 - **Replication**: Locally-redundant storage (LRS)
 - **Access tier**: Hot
5. Click **Review + Create** then click **Create**
6. Wait for the storage account to create.
7. Return to storage accounts
8. Select the storage account you created
9. In the overview pane click **Containers**
10. Click **+ Container**
11. For the name type **events**
12. Set the **Public Access Level** to **Container**
13. Click **Create**

47.1.3 Task 3: Create new event hub

1. Return to event Hubs click the name of your newly created Event Hub namespace
2. In the event hub namespace click **Event Hubs** underneath Entities in the selection pane
3. Click **+ Event Hub**
4. Enter the name of "events"
5. Click **On** underneath **Capture**

Note: This will turn on the dumping of events to the Blob store we created earlier

6. Click **Select Container**

7. Select the **Storage account** name you created earlier
8. Select the **Blob storage (Container)** name you created earlier
9. Click **Select**
10. Click **Create**

47.1.4 Task 4: Collect data to be able to send events into event hubs

1. Under event hubs namespace click **Shared access policies**
2. Click **RootManageSharedAccessKey**
3. Click the copy to clipboard icon next to Primary Key
4. Open notepad and paste it in there for later use
5. Copy the name of the Event Hubs namespace and the name of the Event Hub you created to the same notepad document

Note: You will need this primary key and other information for the scripts that will be run later to enter some data into the event hubs system

47.1.5 Task 5: Download the script files

We will now download the scripts that will be used to create some events to be sent into the Event Hub, this will simulate the Event Hub receiving data from an application in the environment that has been written to communicate with Event Hubs, or from other systems that communicate with Azure Event Hubs. The script files have been developed and published on the PowerShell gallery

1. Open **PowerShell as administrator** (right click on the PowerShell icon) and run the following command

```
install-script get-blobevents, send-blobevents
```

Note: If prompted confirm the installation. The script files have now been downloaded and are available for use in PowerShell

47.1.6 Task 6: Send some events to Event Hub

For this section you will need the primary key copied from the portal earlier

1. Open PowerShell
2. Run the following command

```
send-blobevents
```
3. This command will prompt you to enter the following data:
 - **primaryKey**: your primary key copied earlier in the lab
 - **eventhubnamespace**: the name of your namespace
 - **eventhub**: the name of your event hub
 - **numberOfEvents**: 10 (you can choose more, but they will take longer to send to the Event Hub)

If you receive a series of **401 Unauthorised errors** from the script check the clock on the machine you have executed the code, if using a virtual machine it should be set to UTC. If you have corrected the time you will need to restart the PowerShell shell and re-run the code.

Note: This will send a series of events to the Event Hub with randomised data

47.1.7 Task 7: Review the Events in EventHub and Blob Storage

1. Return to Event Hubs and your **Event hubs namespace**
2. Click **Event Hubs** and select your **Event Hub**
3. In the overview pane review the Event Hub graphs to see the data spikes on incoming messages
4. Search for and open **Storage Accounts**
5. Select your **event hubs Storage Account**

6. Click **Containers**

7. Open your **Blob containter** for events storage

Information: Here you can review the raw .avro events that have been created by the Event Hubs system, for more information about the .avro format used by Event Hubs see the following wiki article https://en.wikipedia.org/wiki/Apache_Avro

47.1.8 Task 8: Review the Events from a REST query to the Blob storage

1. Launch **PowerShell**

2. Run **get-blobevents** and enter the following when prompted:

- **blobName:** Name of the storage account
- **containterName:** Name of the Blob container where the events are stored

Note: You can see this information in your storage account. The script will make a REST query to the Blob storage to list out all the .avro event that are in the storage Blob

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click **R**

Results: You have now completed this lab and can move onto the next lab in the series

48 Module 4: Lab 4 - Azure Sentinel

Azure Sentinel is your bird's-eye view across the enterprise. Put the cloud and large-scale intelligence from decades of Microsoft security experience to work. Make your threat detection and response smarter and faster with artificial intelligence (AI)

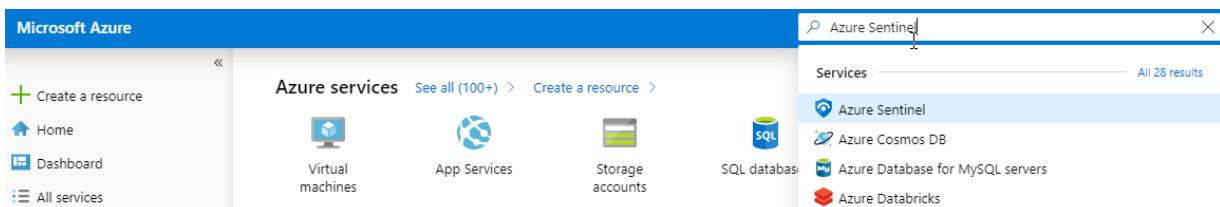
48.1 Exercise 1: On-board Azure Sentinel

To on-board Azure Sentinel, you first need to enable Azure Sentinel, and then connect your data sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft Threat Protection solutions, Microsoft 365 sources, including Office 365, Azure AD, Azure ATP, and Microsoft Cloud App Security, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use common event format, Syslog or REST-API to connect your data sources with Azure Sentinel.

After you connect your data sources, choose from a gallery of expertly created workbooks that surface insights based on your data. These workbooks can be easily customized to your needs.

48.1.1 Task 1: Enable Azure Sentinel

1. In the Azure portal, search for Azure Sentinel.



2. Click **+Add**.

3. Create a new workspace in a new resource group using the East US region if necessary.

Note: - Default workspaces created by Azure Security Center will not appear in the list; you can't install Azure Sentinel on them. - Azure Sentinel can run on workspaces in any GA region of Log Analytics except the China, Germany and Azure Government regions. Data generated by Azure Sentinel (such as incidents, bookmarks, and alert rules, which may contain some customer data sourced from these workspaces) is saved either in West Europe (for workspaces located in Europe) or East US (for all US-based workspaces, as well as any other region except Europe).

- To finish creating the workspace, click **Review and Create**, then click **Create**.
- Once the workspace has been created, click **Add Azure Sentinel**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons: Create a resource, Home, Dashboard, All services, FAVORITES (with Resource groups, All resources, Recent, App Services, SQL databases, Virtual machines (classic), Virtual machines, Cloud services (classic), Subscriptions, Storage accounts, and Azure Active Directory). The main area is titled "Choose a workspace to add to Azure Sentinel". It features a search bar labeled "Search workspaces", a button to "Create a new workspace", and a list of existing workspaces. One workspace, "Senintel East US 2", is listed with its icon and name. At the bottom right, a blue button labeled "Add Azure Sentinel" is highlighted with a red border.

48.1.2 Task 3: Connect data sources

Azure Sentinel creates connections to services and apps by connecting to the service and forwarding the events and logs to Azure Sentinel. For machines and virtual machines, you can install the Azure Sentinel agent that collects the logs and forwards them to Azure Sentinel. For Firewalls and proxies, Azure Sentinel utilizes a Linux Syslog server. The agent is installed collects the log files and forwards them to Azure Sentinel.

- In the Azure Portal select All resources and select the Log Analytics workspace you created in the previous task.
- On the menu, select **Data connectors**. This page lets you see the full list of connectors that Azure Sentinel provides and their status.

Azure Sentinel - Data connectors

Selected workspace: 'myWorkspaceDemo'

Search (Ctrl+ /)

Refresh

General

 Overview

 Logs

 News & guides

Threat management

 Incidents

 Workbooks

 Hunting

 Notebooks

Configuration

 Data connectors

 Analytics

 Playbooks

 Community

 Workspace settings

 25
Connectors

Search by na

STATUS ↑↓ C

	A	A
	A	N
	A	N
	A	N
	A	N

3. Select **Azure Activity** and click **Open connector page**.

4. Select **Configure Azure Activity logs**.



Prerequisites

To integrate with Azure Activity make sure you have:

- ✓ **Workspace:** read and write permissions are required.



Configuration

Select subscriptions to monitor

The Azure Activity log subscriptions you select will be monitored by Azure Sentinel.

[Configure Azure Activity logs >](#)

5. On the specific connector page, make sure you have fulfilled all the prerequisites and follow the instructions to connect the data to Azure Sentinel. It may take some time for the logs to start syncing with Azure Sentinel. After you connect, you see a summary of the data in the **Data received** graph, and connectivity status of the data types.
6. Select your Azure subscription then click **Connect**.

Results: You have now completed this lab.

49 Module 4: Lab 5 - Manage endpoint protection issues with Azure Security Center

Azure Security Center monitors the status of antimalware protection and reports this under the Endpoint protection issues blade. Security Center highlights issues, such as detected threats and insufficient protection, which can make your virtual machines (VMs) and computers vulnerable to antimalware threats. By using the information under **Endpoint protection issues**, you can identify a plan to address any issues identified.

Security Center reports the following endpoint protection issues:

- Endpoint protection not installed on Azure VMs - A supported antimalware solution is not installed on these Azure VMs.
- Endpoint protection not installed on non-Azure computers - A supported antimalware is not installed on these non-Azure computers.
- Endpoint protection health:

- Signature out of date - An antimalware solution is installed on these VMs and computers, but the solution does not have the latest antimalware signatures.
- No real time protection - An antimalware solution is installed on these VMs and computers, but it is not configured for real-time protection.
- Not reporting - An antimalware solution is installed but not reporting data.
- Unknown - An antimalware solution is installed but its status is unknown or reporting an unknown error.

49.1 Exercise 1: Implement the recommendation

Endpoint protection issues is presented as a recommendation in Security Center. If your environment is vulnerable to antimalware threats, this recommendation will be displayed under **Recommendations** and under **Compute**. To see the **Endpoint protection issues dashboard**, you need to follow the Compute workflow.

In this exercise, we will use **Compute**. We will look at how to install antimalware on Azure VMs and on non-Azure computers.

49.1.1 Task 1: Install antimalware on Azure VMs

1. Select **Compute & apps** under the Security Center main menu or **Overview**.

Security Center - Compute & apps
Showing subscription 'Azure Pass - Sponsorship'

RECOMMENDATION

- Just-In-Time network access control should be applied on virtual machines
- Vulnerability assessment solution should be installed on your virtual machines
- The rules for web applications on IaaS NSGs should be hardened
- Access should be restricted for permissive Network Security Groups with Internet-facing VMs
- Install endpoint protection solution on virtual machines
- Disk encryption should be applied on virtual machines

2. Under **Compute**, select **Install endpoint protection solution on virtual machines**. The **Endpoint protection issues dashboard** opens.

Overview	VMs and Computers	VM scale sets	Cloud services
<input type="text"/> Search recommendations			
RECOMMENDATION ↑ SECURE SCORE IMPACT ↓			
Just-In-Time network access control should be applied on virtual machines	+30		
Vulnerability assessment solution should be installed on your virtual machines	+30		
The rules for web applications on IaaS NSGs should be hardened	+20		
Access should be restricted for permissive Network Security Groups with Internet-facing VMs	+20		
Install endpoint protection solution on virtual machines	+15		
Disk encryption should be applied on virtual machines	+10		

3. On the **Endpoint Protection not installed on Azure VMs** blade click **Install on 1 VMs**.

Endpoint Protection not installed on Azure VMs

Filter **Install on 1 VMs**

VIRTUAL MACHINE

myVM

4. Under **Select Endpoint protection**, select the endpoint protection solution you want to use. In this example, select **Microsoft Antimalware**.

5. Additional information about the endpoint protection solution is displayed. Select **OK**.

Results: You have now completed this lab.

50 Module 4: Lab 6 - Security Playbook in Azure Sentinel

A security playbook is a collection of procedures that can be run from Azure Sentinel in response to an alert. A security playbook can help automate and orchestrate your response, and can be run manually or set to run automatically when specific alerts are triggered. Security playbooks in Azure Sentinel are based on Azure Logic Apps, which means that you get all the power, customizability, and built-in templates of Logic Apps. Each playbook is created for the specific subscription you choose, but when you look at the Playbooks page, you will see all the playbooks across any selected subscriptions.

50.1 Exercise 1: Create and manage a Security Playbook in Azure.

50.1.1 Task 1: How to create a security playbook.

Follow these steps to create a new security playbook in Azure Sentinel:

1. Open **Azure Sentinel** dashboard.
2. Under **Configuration**, select **Playbooks**.

+ Add Playbook	Refresh	Last 24 hours	Enable	Disable	Delete	Logic Apps documentation																																																															
22 Security Playbooks		5 Total Runs		4 Succeeded Runs		0 Running Playbooks																																																															
1 Failed Runs																																																																					
<input type="text" value="Search playbooks"/> <table border="1"> <thead> <tr> <th>NAME</th><th>STATUS</th><th>RUNS</th><th>RUNNING</th><th>SUCCEEDED</th><th>FAILED</th><th>SUBSCRIPTION</th><th>LOCATION</th><th>TRIGGER KIND</th></tr> </thead> <tbody> <tr> <td>[A] ShaliniDemo</td><td>enabled</td><td>0</td><td>0</td><td>0</td><td>0</td><td>OMS Security Koby Koren</td><td>West US</td><td>Security Center</td></tr> <tr> <td>[A] AddRuleToNSG</td><td>enabled</td><td>0</td><td>0</td><td>0</td><td>0</td><td>OMS Security Koby Koren</td><td>East US</td><td>Security Center</td></tr> <tr> <td>[A] BlockIP_BlockUser_ServiceNow</td><td>enabled</td><td>0</td><td>0</td><td>0</td><td>0</td><td>OMS Security Koby Koren</td><td>East US</td><td>Security Center</td></tr> <tr> <td>[A] BlockIP_CheckPoint</td><td>enabled</td><td>0</td><td>0</td><td>0</td><td>0</td><td>OMS Security Koby Koren</td><td>East US</td><td>Security Center</td></tr> <tr> <td>[A] BlockIP_IsolateMachine_ServiceNow</td><td>enabled</td><td>0</td><td>0</td><td>0</td><td>0</td><td>OMS Security Koby Koren</td><td>East US</td><td>Security Center</td></tr> <tr> <td>[A] BlockIP_Paloalto</td><td>enabled</td><td>3</td><td>0</td><td>2</td><td>1</td><td>OMS Security Koby Koren</td><td>East US</td><td>Security Center</td></tr> </tbody> </table>							NAME	STATUS	RUNS	RUNNING	SUCCEEDED	FAILED	SUBSCRIPTION	LOCATION	TRIGGER KIND	[A] ShaliniDemo	enabled	0	0	0	0	OMS Security Koby Koren	West US	Security Center	[A] AddRuleToNSG	enabled	0	0	0	0	OMS Security Koby Koren	East US	Security Center	[A] BlockIP_BlockUser_ServiceNow	enabled	0	0	0	0	OMS Security Koby Koren	East US	Security Center	[A] BlockIP_CheckPoint	enabled	0	0	0	0	OMS Security Koby Koren	East US	Security Center	[A] BlockIP_IsolateMachine_ServiceNow	enabled	0	0	0	0	OMS Security Koby Koren	East US	Security Center	[A] BlockIP_Paloalto	enabled	3	0	2	1	OMS Security Koby Koren	East US	Security Center
NAME	STATUS	RUNS	RUNNING	SUCCEEDED	FAILED	SUBSCRIPTION	LOCATION	TRIGGER KIND																																																													
[A] ShaliniDemo	enabled	0	0	0	0	OMS Security Koby Koren	West US	Security Center																																																													
[A] AddRuleToNSG	enabled	0	0	0	0	OMS Security Koby Koren	East US	Security Center																																																													
[A] BlockIP_BlockUser_ServiceNow	enabled	0	0	0	0	OMS Security Koby Koren	East US	Security Center																																																													
[A] BlockIP_CheckPoint	enabled	0	0	0	0	OMS Security Koby Koren	East US	Security Center																																																													
[A] BlockIP_IsolateMachine_ServiceNow	enabled	0	0	0	0	OMS Security Koby Koren	East US	Security Center																																																													
[A] BlockIP_Paloalto	enabled	3	0	2	1	OMS Security Koby Koren	East US	Security Center																																																													

3. In the Azure Sentinel - Playbooks page, click **+ Add Playbook** button.

Azure Sentinel | Playbooks
Selected workspace: 'Senintell'

[+ Add Playbook](#) [Refresh](#) [Last 24 hours](#)

General

- [Overview](#)
- [Logs](#)
- [News & guides](#)

Threat management

- [Incidents](#)
- [Workbooks](#)
- [Hunting](#)
- [Notebooks](#)

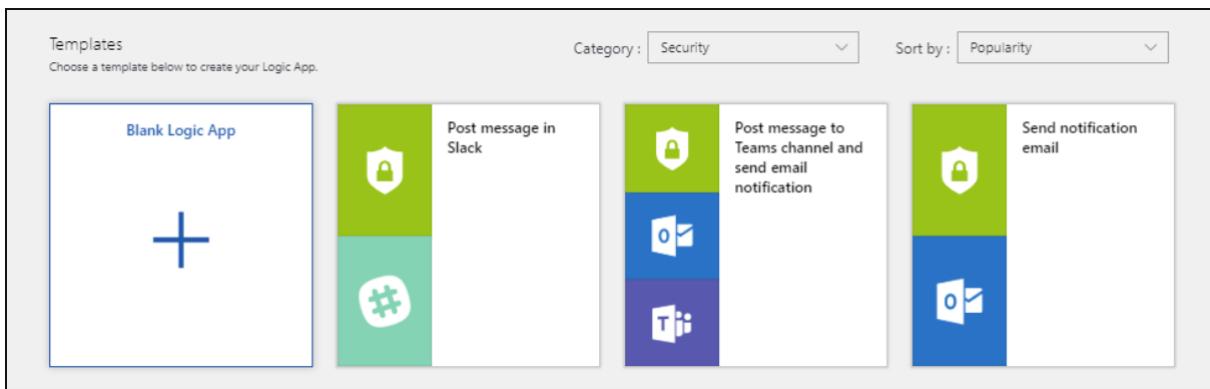
Configuration

- [Data connectors](#)
- [Analytics](#)
- Playbooks** (highlighted with a red box)
- [Community](#)
- [Settings](#)

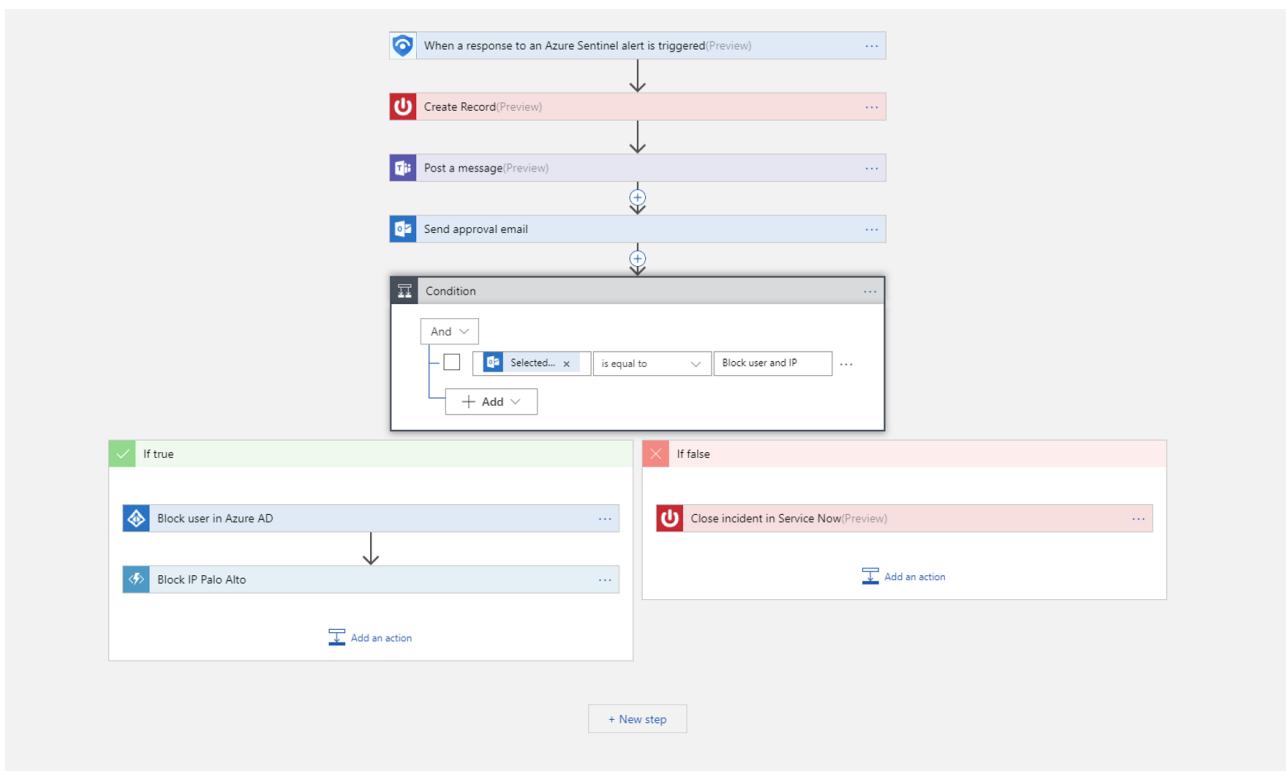
0 Security playbooks
0 Total runs

Name	Status
[A] ShaliniDemo	enabled
[A] AddRuleToNSG	enabled
[A] BlockIP_BlockUser_ServiceNow	enabled
[A] BlockIP_CheckPoint	enabled
[A] BlockIP_IsolateMachine_ServiceNow	enabled
[A] BlockIP_Paloalto	enabled

- In the **Create Logic app** page, type the requested information to create your new logic app, and click **Review + create** then click **Create**.
- Once created click **Go to resource**.
- In the **Logic App Designer** select the template you want to use. If you select a template that necessitates credentials, you will have to provide them. Alternatively, you can create a new blank playbook from scratch. Select **Blank Logic App**.



7. You are taken to the Logic App Designer where you can either build new or edit the template.
8. If you are creating a blank playbook, in the **Search all connectors and triggers** field, type **Azure Sentinel**, and select **When a response to an Azure Sentinel alert is triggered**.
- Note:** You may be required to re-authenticate. If so, click **Sign in** and authenticate with your Azure credentials.
9. Click **Save** and return to the Azure Sentinel blade. After it is created, the new playbook appears in the **Playbooks** list. If it doesn't appear, click **Refresh**.
10. Use the **Get entities** functions, which enable you to get the relevant entities from inside the **Entities** list, such as accounts, IP addresses and hosts. This will enable you to run actions on specific entities.
11. Now you can define what happens when you trigger the playbook. You can add an action, logical condition, switch case conditions, or loops.



50.1.2 Task 2: How to run a security playbook

You can run a playbook on demand.

To run a playbook on-demand:

1. In the **Incidents** page, select an incident and click on **View full details**.
2. In the **Alerts** tab, click on the alert you want to run the playbook on, and scroll all the way to the right and click **View playbooks** and select a playbook to **run** from the list of available playbooks on the subscription.

50.2 Exercise 2: Automate threat responses

SIEM/SOC teams can be inundated with security alerts on a regular basis. The volume of alerts generated is so huge, that available security admins are overwhelmed. This results all too often in situations where many alerts can't be investigated, leaving the organization vulnerable to attacks that go unnoticed.

Many, if not most, of these alerts conform to recurring patterns that can be addressed by specific and defined remediation actions. Azure Sentinel already enables you to define your remediation in playbooks. It is also possible to set real-time automation as part of your playbook definition to enable you to fully automate a defined response to particular security alerts. Using real-time automation, response teams can significantly reduce their workload by fully automating the routine responses to recurring types of alerts, allowing you to concentrate more on unique alerts, analyzing patterns, threat hunting, and more.

50.2.1 Task 1: Automate Responses

1. Select the alert for which you want to automate the response.
2. In the **Edit alert rule** page, under **Real-time automation**, choose the **Triggered playbook** you want to run when this alert rule is matched.
3. Select **Save**.

The screenshot shows the 'Edit alert rule' configuration page. The 'Realtime automation' section is highlighted, displaying the following settings:

- Triggered playbooks:** BlockIP_BlockUser_ServiceNow
- Suppression status:** On (button is blue)

At the bottom right of the form is a blue 'Save' button.

Results: In this lab, you learned how to use playbooks in Azure Sentinel.

51 Module 4: Lab 7 - Secure score in Azure Security Center

With so many services offering security benefits, it's often hard to know what steps to take first to secure and harden your workload. The Azure secure score reviews your security recommendations and prioritizes them for you, so you know which recommendations to perform first. This helps you find the most serious security vulnerabilities so you can prioritize investigation. Secure score is a tool that helps you assess your workload security posture.

Secure score calculation

Security Center mimics the work of a security analyst, reviewing your security recommendations, and applying advanced algorithms to determine how crucial each recommendation is. Azure Security center constantly reviews your active recommendations and calculates your secure score based on them, the score of a recommendation is derived from its severity and security best practices that will affect your workload security the most.

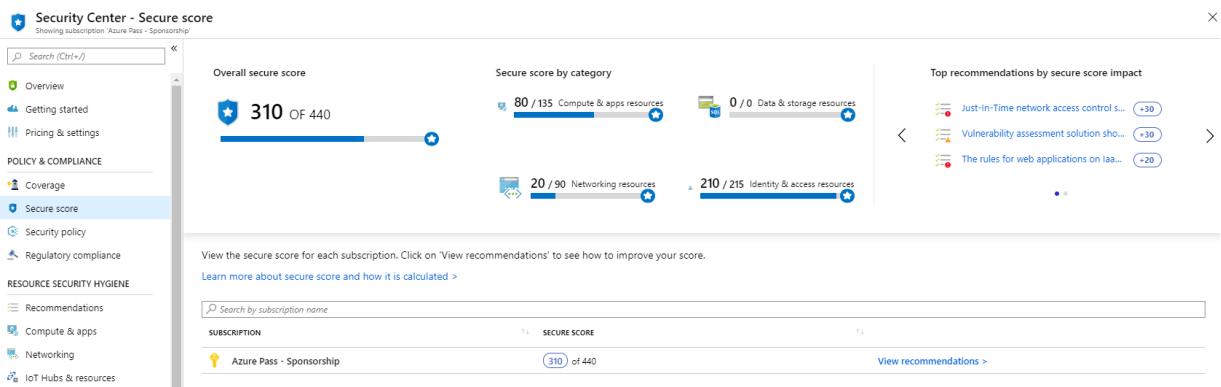
Security Center also provides you with an **Overall secure score**.

Overall secure score is an accumulation of all your recommendation scores. You can view your overall secure score across your subscriptions or management groups, depending on what you select. The score will vary based on subscription selected and the active recommendations on these subscriptions.

51.1 Exercise 1: Improve your secure score in Azure Security Center.

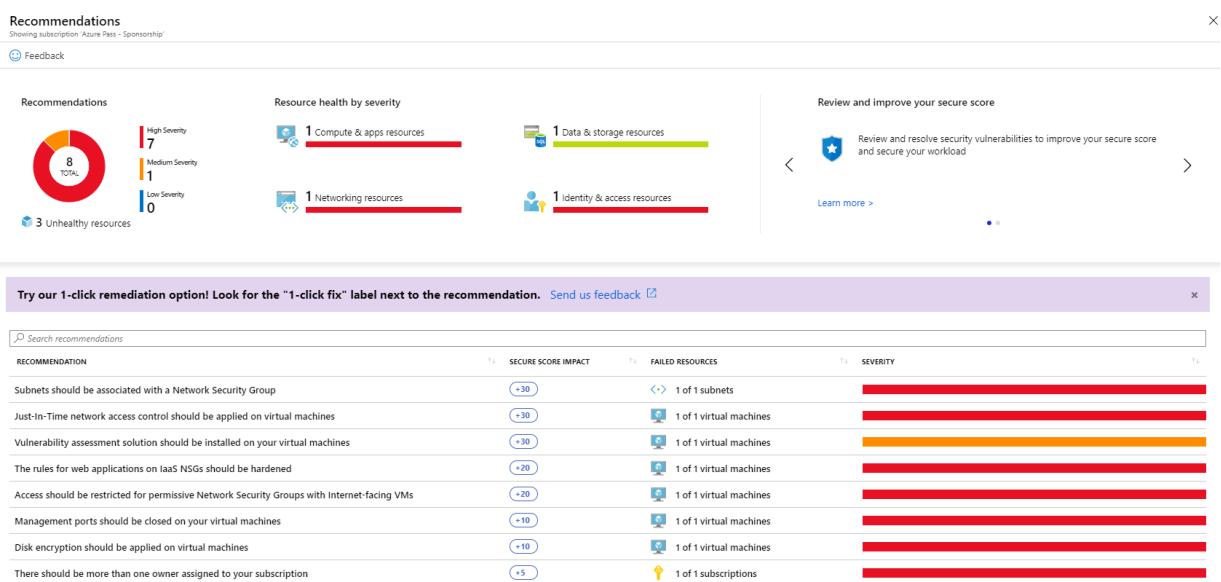
51.1.1 Task 1: View the secure score in the Azure Portal.

1. In the Azure dashboard, click **Security Center** and then click **Secure score**.
2. At the top you can see Secure score highlights:
 - The **Overall secure score** represents the score per policies, per selected subscription
 - **Secure score by category** shows you which resources need the most attention
 - **Top recommendations by secure score impact** provides you with a list of the recommendations that will improve your secure score the most if you implement them.



Note: The sum of the secure score of each subscription does not equal the overall secure score. The secure score is a calculation based on the ratio between your healthy resources and your total resources per recommendation, not a sum of secure scores across your subscriptions.

3. Click **View recommendations** to see the recommendations for that subscription that you can remediate to improve your secure score.
4. In the list of recommendations, you can see that for each recommendation there is a column that represents the **Secure score impact**. This number represents how much your overall secure score will improve if you follow the recommendations. For example, in the screen below, if you **Remediate vulnerabilities in container security configurations**, your secure score will increase by 35 points.



51.1.2 Task 2: View the individual secure scores.

In addition, to view individual secure scores, you can find these within the individual recommendation blade.

The **Recommendation secure score** is a calculation based on the ratio between your healthy resources and your total resources. If the number of healthy resources is equal to the total number of resources, you get the maximum secure score of the recommendation of 50. To try to get your secure score closer to the max score, fix the unhealthy resources by following the recommendations.

The **Recommendation impact** lets you know how much your secure score improves if you apply the recommendation steps. For example, if your secure score is 42 and the **Recommendation impact** is +3, performing the steps outlined in the recommendation improve your score to become 45.

1. Click any of the recommendations in the Secure Score blade.

The recommendation shows which threats your workload is exposed to if the remediation steps are not taken.

The screenshot shows the Azure Security Center Secure Score blade. A specific recommendation is highlighted:

Description: Subnets should be associated with a Network Security Group. Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet. When an NSG is associated with a subnet, the ACL rules apply to all the VM instances and integrated services in that subnet, but don't apply to internal traffic inside the subnet. To secure resources in the same subnet from one another, enable NSG directly on the resources as well.

General Information:

- Recommendation score: 0/30
- Recommendation Impact: +30 (highlighted)
- User Impact: High
- Implementation effort: Moderate

Threats:

- Malicious insider
- Data spillage
- Data exfiltration

Remediation steps:

To enable Network Security Groups on your subnets:

1. Select a subnet to enable NSG on.
2. Click the 'Network security group' section.
3. Follow the steps and select an existing network security group to attach to this specific subnet.

Affected resources:

- Unhealthy resources (1)
- Healthy resources (0)
- Unscanned resources (0)

Was this recommendation useful? Yes No

Results: In this lab, you learned how to improve your secure score in Azure Security Center

52 Module 4: Lab 8 - Create security baselines

Azure doesn't monitor security or respond to security incidents within the customer's area of responsibility. Azure does provide many tools (such as Azure Security Center, Azure Sentinel) that are used for this purpose. There is also an effort to help make every service as secure as possible by default. That is, every service comes with a baseline that is already designed to help provide security for most common-use cases. However, because Azure cannot predict how a service will be used, you should always review these security controls to evaluate whether they adequately mitigate risks.

This lab will guide you through a security baseline for Azure services. Each unit will provide a checklist of things to verify about the services you are using in your architecture.

In this lab, you will:

- Learn Azure platform security baselines and how they were created
- Create and validate a security baseline for the most commonly used Azure services

52.1 Exercise 1: Create an Identity & Access Management (IAM) baseline

Identity management is key to granting access and to the security enhancement of corporate assets. To secure and control your cloud-based assets you must manage identity and access for your Azure administrators, application developers, and application users.

IAM recommendations

Here are the recommendations for identity and access management. Included with each recommendation are the basic steps to follow in the Azure portal.

52.1.1 Task 1: Restrict access to the Azure AD administration portal

All non-Administrators should not have access due to the sensitive data and the rules of least privilege.

1. Sign in to the Azure portal.

2. On the left, select **Azure Active Directory > Users**.
3. Go to **User settings**.
4. Ensure that Restrict access to Azure AD administration portal is set to Yes. Setting this value to Yes restricts all non-administrators from accessing any Azure AD data in the administration portal, but does not restrict such access using PowerShell or another client such as Visual Studio.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons. Under 'Azure Active Directory', the 'User settings' option is selected and highlighted with a red box. The main content area shows sections like 'Enterprise applications', 'App registrations', 'Administration portal' (which has a red box around it), 'External users', and 'User feature previews'. At the top right, there are 'Save' and 'Discard' buttons.

5. Click **Save**.

52.1.2 Task 2: Enable Azure Multi-Factor Authentication (MFA)

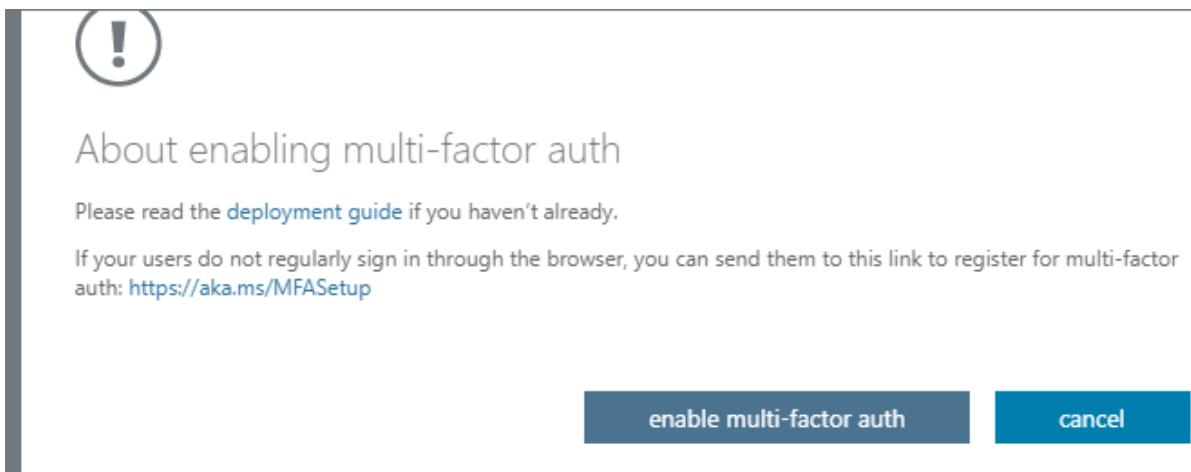
Enable it for privileged and non-privileged users.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Users**.
3. Click **+ New User**.
4. On the New user blade, enter the following details and click Create:
 - **Username:** Abbi
 - **Name:** Abbi Skinner
 - **First name:** Abbi
 - **Last Name:** Skinner
 - **Roles:** Select Global Admin

5. On the left, select **Azure Active Directory > Users > All users**.
6. Select Multi-Factor Authentication. This will open a new window.
7. Select Abbi Skinner and click **Enable**

The screenshot shows the 'Users - All users' page in the Azure portal. The 'All users' option is selected in the left navigation. At the top right, there are buttons for 'New user', 'New guest user', 'Reset password', 'Delete user', and 'Multi-Factor Authentication' (which is highlighted with a red box). Below the buttons, there are search and filter fields. The main table lists users with columns for NAME, USER NAME, and USER TYPE.

8. Select **enable multi-factor auth** then click **Close**.



9. Abbi is now enabled for MFA.

52.1.3 Task 3: Block remembering MFA on trusted devices

Remember Multi-Factor Authentication feature for devices and browsers that are trusted by the user is a free feature for all Multi-Factor Authentication users. Users can bypass subsequent verifications for a specified number of days, after they've successfully signed-in to a device by using Multi-Factor Authentication. If an account or device is compromised, remembering Multi-Factor Authentication for trusted devices can negatively affect security.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Users > All users**.
3. Select Multi-Factor Authentication.
4. Select **Abi Skinner**, then click **Manage users settings**.
5. Ensure that **Restore multi-factor authentication on all remembered devices** is Selected then click **Save**.

A screenshot of the "Manage user settings" dialog for the user "Abi Skinner". The dialog title is "Manage user settings". There are three checkboxes listed:

- Require selected users to provide contact methods again
- Delete all existing app passwords generated by the selected users
- Restore multi-factor authentication on all remembered devices

52.1.4 Task 4: About guests

In this task you will ensure that no guest users exist, or alternatively if the business requires guest users, ensure to limit their permissions.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Users > All users**.
3. Select the Show drop down and select **Guest users only**.
4. Verify that there are no guest users listed (**USER TYPE=Guest**).

52.1.5 Task 5: Password options

With dual identification set, an attacker would require compromising both the identity forms before they could maliciously reset a user's password.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Users**.
3. Select **Password reset**.
4. Go to Authentication methods.
5. Set the Number of methods required to reset to 2.
6. Select two methods and click **Save**.

52.1.6 Task 6: Establish an interval for reconfirming user authentication methods

If authentication reconfirmation is set to disabled, register users will never be prompted to re-confirm their authentication information.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Users**.
3. Go to **Password reset**.
4. Go to **Registration**.
5. Ensure that Number of days before users are asked to re-confirm their authentication information is not set to 0. The default is 180 days.

52.1.7 Task 7: Disable Members invitations

Restricting invitations through administrators only ensures that only authorized accounts have access Azure resources.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Users**.
3. Go to **User settings**.
4. Go to External users, click **Manage external collaboration settings**.

5. Ensure that Members can invite is set to **No**.

External collaboration settings

Save Discard

Guest users permissions are limited

Yes No

Admins and users in the guest inviter role can invite

Yes No

Members can invite

Yes No

Guests can invite

Yes No

Enable Email One-Time Passcode for guests (Preview)

[Learn more](#)

Yes No

52.1.8 Task 8: Users to create and manage security groups

When this feature is enabled, all users in AAD are allowed to create new security groups. Security Group creation should be restricted to administrators.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Groups**.
3. Go to **General** under the settings section.
4. Ensure that Users can create security groups is set to **No**.

Groups - General
gdaztest12outlookcom (Default Directory) - Azure Active Directory

Save Discard

Self Service Group Management

Owners can manage group membership requests in the Access Panel Yes No

Restrict access to Groups in the Access Panel Yes No

Security Groups

Users can create security groups in Azure portals Yes No

Owners who can assign members as group owners in Azure portals All Selected None

52.1.9 Task 9: Self-service group management enabled

Until your business requires this delegation to various users, it is a best practice to disable this feature.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Groups**

3. Go to **General** under the settings section.
4. Ensure that Self-service group management enabled is set to **No**.

Groups - General
Default Directory - Azure Active Directory

Save Discard

Self Service Group Management

Owners can manage group membership requests in the Access Panel Yes

Restrict access to Groups in the Access Panel Yes

52.1.10 Task 10: Application options - Allow users to register apps

Require administrators to register custom applications.

1. Sign in to the Azure portal.
2. On the left, select **Azure Active Directory > Users**
3. Go to User settings.
4. Ensure that User can register applications is set to **No** then click **Save**.

Users - User settings
gdaztest12outlookcom (Default Directory) - Azure Active Directory

Save Discard

Enterprise applications
[Manage how end users launch and view their applications](#)

App registrations
Users can register applications

52.2 Exercise 2: Create an Azure Security Center baseline

Azure Security Center (ASC) provides unified security management and advanced threat protection for workloads running in Azure, on-premises, and in other clouds. The following are Security Center recommendations that, if followed, will set various security policies on an Azure subscription.

These policies define the set of controls that are recommended for your resources with an Azure subscription.

52.2.1 Task 1: Enable System Updates

Azure Security Center monitors daily Windows and Linux virtual machines (VMs) and computers for missing operating system updates. Security Center retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS), depending on which service is configured on a Windows computer. Security Center also checks for the latest updates in Linux systems. If your VM or computer is missing a system update, Security Center will recommend that you apply system updates.

1. Sign in to the Azure portal.
2. Select **Security Policy** on the **Security Center** main menu.

3. The **Policy Management** screen is displayed.
4. Choose your subscription from the displayed list.
5. Select **View effective policy**.
6. Check that **System updates should be installed on your machines** is one of the policies.
7. Click the Enable Monitoring in Azure Security Center link (This may also be displayed as ASC Default with a GUID).

Security policy
Azure Pass - Sponsorship

i Security policies are displayed with their effect as defined through Azure Policy. Learn more →

The selected subscription has 1 security policy assignments. The overall effective policies in Security Center are displayed below.

In order to configure a specific policy assignment, choose one of the assignments below:

ASC Default (subscription: 9de00928-aed4-4dd6-8e8b-3f5551dc33fc)

The following security policies are assessed and displayed in Security Center:

8. In this example, the ASC agent has not been deployed to a VM or physical machine so the message AuditIfNotExists is displayed. AuditIfNotExists enables auditing on resources that match the if condition. If the resource is not deployed, NotExists is displayed.

[Preview]: Enable Monitoring in Azure Security Center
Edit Initiative Assignment

Duplicate assignment Create Remediation Task

* Endpoint protection solution should be installed on virtual machine scale sets ⓘ
AuditIfNotExists

* Vulnerabilities in security configuration on your virtual machine scale sets should be remediated ⓘ
AuditIfNotExists

* System updates should be installed on your machines ⓘ
AuditIfNotExists
AuditIfNotExists
Disabled

If enabled, Audit is displayed. If deployed but disabled, Disabled is displayed.

Encryption should be enabled on Automation account variables ⓘ

Audit

All authorization rules except RootManageSharedAccessKey should be removed from Event Hub namespace ⓘ

Disabled

52.2.2 Task 2: Enable Security Configurations

Azure Security Center monitors security configurations by applying a set of over 150 recommended rules for hardening the OS, including rules related to firewalls, auditing, password policies, and more. If a machine is found to have a vulnerable configuration, Security Center generates a security recommendation.

1. Sign in to the Azure portal.
2. On the Hub menu select **Security Center**.
3. Select **Security Policy** then select your **Subscription**.
4. Click **View effective policy**.
5. The Policy Management screen is displayed.
6. Check that **Vulnerabilities in security configuration on your virtual machine scale sets should be remediated** is one of the policies.

Security policy

Pay-As-You-Go

 Security policies are displayed with their effect as defined through Azure Policy. Learn more →

The selected subscription has 1 security policy assignments. The overall effective policies in Security Center are displayed below.

In order to configure a specific policy assignment, choose one of the assignments below:

 [Preview]: Enable Monitoring in Azure Security Center

The following security policies are assessed and displayed in Security Center:

^ Compute And Apps (30 out of 33 policies enabled)

Monitor missing Endpoint Protection in Azure Security Center 

 AuditIfNotExists

System updates should be installed on your machines 

 AuditIfNotExists

Vulnerabilities in security configuration on your machines should be remediated 

 AuditIfNotExists

Vulnerabilities in security configuration on your virtual machine scale sets should be remediated 

Audit whether there are any missing system security updates and critical updates that should be installed to ensure that your Windows and Linux virtual machine scale sets are secure.

Endpoint protection solution should be installed on virtual machines 

System updates on virtual machine scale sets should be installed 

 AuditIfNotExists

Disk encryption should be applied on virtual machines 

 AuditIfNotExists

Note: All of the following policies that have a (*) in their title are listed in the Security policies blade as described above

- **Enable Endpoint Protection** - *Endpoint protection is recommended for all virtual machines.*
- **Enable Disk Encryption** - *Azure Security Center recommends that you apply disk encryption if you have Windows or Linux VM disks that are not encrypted using Azure Disk Encryption. Disk Encryption lets you encrypt your Windows and Linux IaaS VM disks. Encryption is recommended for both the OS and data volumes on your VM.*
- **Enable Network Security Groups** *Azure Security Center recommends that you enable a network security group (NSG) if one is not already enabled. NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your VM instances in a Virtual Network. NSGs can be associated with either subnets or individual VM instances within that subnet. When an NSG is associated with a subnet, the ACL rules apply to all the VM instances in that subnet. In addition, traffic to an individual VM can be restricted further by associating an NSG directly to that VM.*
- **Enable Web Application Firewall** - *Azure Security Center may recommend that you add a web application firewall (WAF) from a Microsoft partner to secure your web applications.*
- **Enable Vulnerability Assessment** - *The vulnerability assessment in Azure Security Center is part of the Security Center virtual machine (VM) recommendations. If Security Center doesn't find a vulnerability assessment solution installed on your VM, it recommends that you install one. A partner agent, after being deployed, starts reporting vulnerability data to the partner's management platform. In turn, the partner's management platform provides vulnerability and health monitoring data back to Security Center.*
- **Enable Storage Encryption** - *When this setting is enabled, any new data in Azure Blobs and Files will be encrypted.*
- **Enable JIT Network Access** - *Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.*
- **Enable Adaptive Application Controls** - *Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence. This capability greatly simplifies the process of configuring and maintaining application whitelisting policies.*
- **Enable SQL Auditing & Threat Detection** - *Azure Security Center will recommend that you turn on auditing and threat detection for all databases on your Azure SQL servers if auditing is not already enabled. Auditing and threat detection can help you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.*
- **Enable SQL Encryption** - *Azure Security Center will recommend that you enable Transparent*

Data Encryption (TDE) on SQL databases if TDE is not already enabled. TDE protects your data and helps you meet compliance requirements by encrypting your database, associated backups, and transaction log files at rest, without requiring changes to your application.

- **Set Security Contact Email and Phone Number** - Azure Security Center will recommend that you provide security contact details for your Azure subscription if you haven't already. This information will be used by Microsoft to contact you if the Microsoft Security Response Center (MSRC) discovers that your customer data has been accessed by an unlawful or unauthorized party. MSRC performs select security monitoring of the Azure network and infrastructure and receives threat intelligence and abuse complaints from third parties.

7. Select **Cost Management + Billing**.

Note: The following steps will not work with an Azure Pass subscription but remains in this lab in order to identify the steps required in a Real World scenario.

8. The Contact info screen is displayed.

9. Enter or validate the contact information displayed.

The screenshot shows the Azure portal interface with the following details:

- Left sidebar:** A vertical menu with icons and text for: Create a resource, Home, Dashboard, All services, FAVORITES (All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing).
- Top navigation bar:** Home > Cost Management + Billing - Contact info
- Page title:** Cost Management + Billing - Contact info
- Page content:**
 - Waypoint Ventures LLC
 - Search (Ctrl+ /)
 - Contact info** (highlighted in blue)
 - Overview
 - Cost Management
 - Management groups
 - Diagnose and solve problems
 - Billing**
 - Subscriptions
 - Invoices
 - Billing address
 - Payment methods
 - Support + troubleshooting**
 - New support request

52.2.3 Task 3: Enable Send me emails about alerts

Azure Security Center will recommend that you provide security contact details for your Azure subscription if you haven't already.

1. On the Hub menu select **Security Center**.
2. Select **Pricing & settings**.
3. The Pricing & settings screen is displayed.
4. Click on your Subscription.
5. Click **Email notifications**.
6. Select **Save**.

The screenshot shows the 'Email notifications' settings page in the Azure Security Center. The left sidebar lists 'Settings' with options: 'Pricing tier', 'Threat detection', 'Data Collection', and 'Email notifications' (which is selected and highlighted in blue). The main area has a heading 'Enter contact information for the administrator who should be notified when Azure Security Center detects compromised resources.' Below this are fields for 'Email address' (containing 'One or more e-mail addresses, separated by a comma') and 'Phone number'. Under 'Email notification settings', there are two toggle switches: 'Send email notification for high severity alerts' (set to 'On') and 'Also send email notification to subscription owners' (set to 'On'). A note below states: 'An email notification is sent once a day for each high severity alert when it is first detected. All email notifications are sent from a US-based service regardless of the geographical location of the affected resources.' A 'Learn more >' link is also present.

52.2.4 Task 4: Enable Send email also to subscription owners

Azure Security Center will recommend that you provide security contact details for your Azure subscription if you haven't already.

1. Using the above Email notifications form, additional emails can be added separated by commas.
2. Click **Save**.

52.3 Exercise 3: Create an Azure storage accounts baseline

An Azure storage account provides a unique namespace to store and access your Azure Storage data objects. Storage Accounts also need to be secured.

52.3.1 Task 1: Require security-enhanced transfers

Another step you should take to ensure the security of your Azure Storage data is to encrypt the data between the client and Azure Storage. The first recommendation is to always use the HTTPS protocol, which ensures secure communication over the public Internet. You can enforce the use of HTTPS when calling the REST APIs to access objects in storage accounts by enabling Secure transfer required for the storage account. Connections using HTTP will be refused once this is enabled.

1. Go to **Storage Accounts** under **All services**.
2. Select the storage account.
3. Under **Settings**, select **Configuration**.
4. Ensure **Secure Transfer required** is set to **Enabled**.

The screenshot shows the Azure Storage Account configuration page for a specific account. The left sidebar lists various management options. Under the 'Settings' section, 'Configuration' is currently selected. In the main configuration area, several parameters are set: 'Secure transfer required' is enabled, which is highlighted with a red rectangular box. The 'Access tier (default)' is set to 'Hot'. The 'Replication' type is 'Locally-redundant storage (LRS)'. There is no 'Identity-based Directory Service for Azure File Authentication' configured. Under 'Data Lake Storage Gen2', 'Hierarchical namespace' is enabled.

52.3.2 Task 2: Enable binary large object (blob) encryption

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data. Unstructured data is data that does not adhere to a particular data model or definition, such as text or binary data. Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.

1. Go to Storage Accounts under Azure services.
2. Select the storage account.
3. Under **Settings**, select **Encryption**.
4. Azure Storage encryption is enabled by default and cannot be disabled.

The screenshot shows the Azure Storage account settings for a storage account named 'bhhjghjghhk'. The left sidebar lists various settings like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Data transfer, Events, Storage Explorer (preview), and Settings (Access keys, Geo-replication, CORS, Configuration). The 'Encryption' section is currently selected. On the right, there's a 'Save' and 'Discard' button, followed by a note about data encryption at rest. It states that by default, data is encrypted using Microsoft Managed Keys. A note also says that after enabling Service Encryption, only new data will be encrypted. Below this is a link to 'Learn More about Azure Storage Encryption'. The 'Encryption type' section contains two options: 'Microsoft Managed Keys' (selected) and 'Customer Managed Keys', both enclosed in a red box.

52.3.3 Task 3: Periodically regenerate access keys

When you create a storage account, Azure generates two 512-bit storage access keys, which are used for authentication when the storage account is accessed. Rotating these keys periodically ensures that any inadvertent access or exposure to these keys could be undermined.

1. Go to **Storage Accounts** under Azure services.
2. Select the storage account.
3. For the storage account, go to **Activity log**.
4. Under Timespan drop-down, select **Custom** and choose Start Time and End Time so it creates a 90 day range.
5. Click **Apply**.

52.3.4 Task 4: Require Shared Access Signature (SAS) tokens to expire within an hour

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but to whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you can grant them access to a resource for a specified period of time, with a specified set of permissions.

Currently verification of a SAS token expiry times cannot be accomplished. Until Microsoft makes token expiry time as a setting rather than a token creation parameter, this recommendation would require a manual verification.

1. Go to **Storage Accounts**.
2. Select the existing account.
3. For the storage account, go to **Shared Access signature**.
4. Set the Start and expiry date/time.
5. Set Allowed protocols to HTTPS only.

Both SAS features are shown below.

52.3.5 Task 5: Require only private access to blob containers

You can enable anonymous, public read access to a container and its blobs in Azure Blob storage. By doing so, you can grant read-only access to these resources without sharing your account key, and without requiring a shared access signature (SAS). By default, a container and any blobs within it may be accessed only by a user that has been given appropriate permissions. To grant anonymous users read access to a container and its blobs, you can set the container public access level. When you grant public access to a container, then anonymous users can read blobs within a publicly accessible container without authorizing the request.

1. Go to **Storage Accounts**.
2. For the storage account, select **Containers** under **Blob Service**.
3. Click **+ Container**.
4. Give the container the name **az500** and click **OK**.
5. Ensure that Public access level to **Private**.

52.4 Exercise 4: Create an Azure SQL Database baseline

Azure SQL Server is a cloud-based relational database server that supports many of the same features as Microsoft SQL Server. It provides an easy transition from an on-premises database into a cloud-based one with built-in diagnostics, redundancy, security and scalability. This exercise looks at the security recommendations to set Azure SQL Server policies.

52.4.1 Task 1: Enable auditing

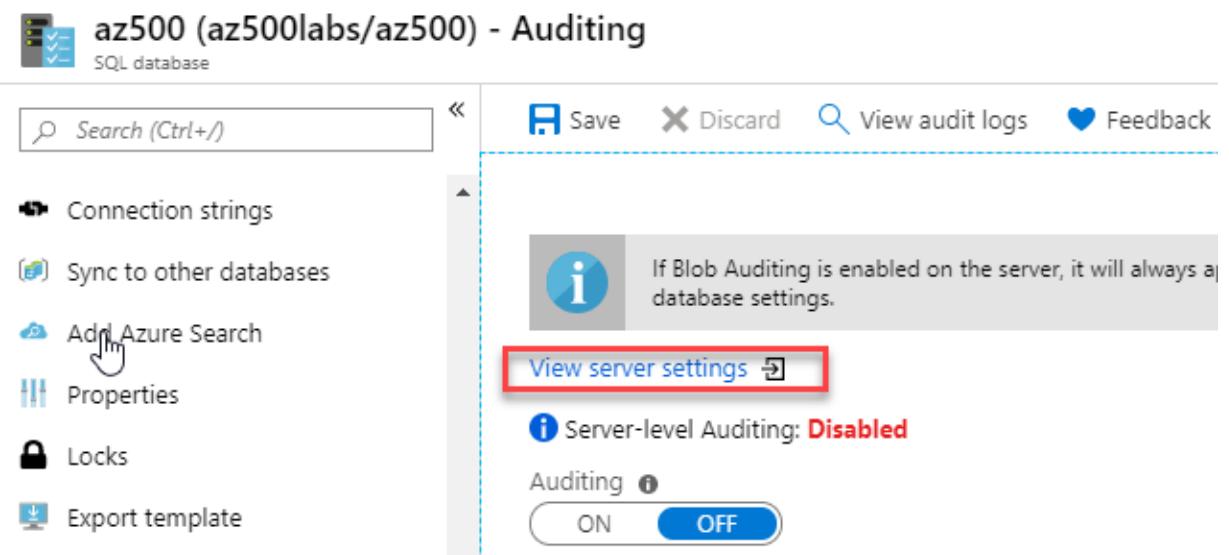
Auditing for Azure SQL Database and SQL Data Warehouse tracks database events and writes them to an audit log in your Azure storage account, OMS workspace or Event Hubs. Auditing also:

- Helps you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.
- Enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance.

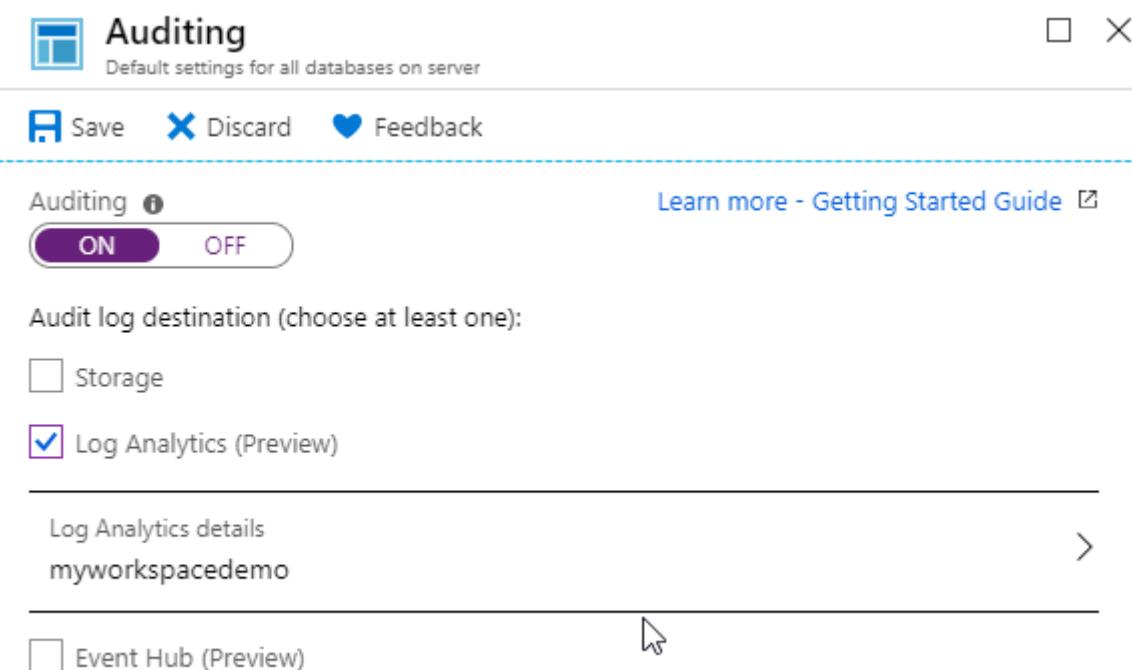
1. In the Azure Portal go to **SQL databases**.
2. Click **+ Add**.
3. Create the database with the following settings then click **Review + create** and click **Create**:

- **Resource Group:** Select myResourceGroup
- **Database name:** az500
- **Server:** Create new
 - **Server Name:** Give the server a unique name
 - **Server admin login:** localadmin
 - **Password:** Pa55w.rd1234
 - **Location:** EastUS

4. Once the deployment is complete, click **Go to resource**.
5. Select **Auditing**, under the **Security** section.
6. Click **View server settings**.



7. Select **On** and check the box next to **Log Analytics**.
8. Select your Log Analytics workspace created in earlier labs and then click **Save**.



9. Exit the Auditing blade.
10. Ensure that Auditing is set to **On** and check the box next to **Log Analytics**.
11. Select your Log Analytics workspace created in earlier labs and then click **Save**.

52.4.2 Task 2: Enable a threat detection service

Threat detection for single and pooled databases detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases. Threat detection can identify Potential SQL injection, Access from unusual location or data center, Access from unfamiliar principal or potentially harmful application, and Brute force SQL credentials. Threat detection is part of the advanced data security (ADS) offering, which is a unified package for advanced SQL security capabilities. Threat detection can be accessed and managed via the central SQL ADS portal.

1. In the Azure portal go to **SQL databases**.

2. Under **Security**, then navigate to **Advanced Data Security**.
3. Click **Settings**.
4. Select **Enable Advanced Data Security on the server** and click **Yes** then click **Save**.

52.4.3 Task 3: Enable all threat detection types

Advanced data security (ADS) provides a set of advanced SQL security capabilities, including data discovery & classification, vulnerability assessment, and Advanced Threat Protection (ATP).

Advanced Threat Protection is part of the advanced data security (ADS) offering, which is part of the defense in depth SQL security strategy. Advanced Threat Protection can be accessed and managed via the central SQL ADS portal.

1. In the Azure portal go to **SQL databases**.
2. Under **Security**, then navigate to **Advanced Data Security**.
3. Click **Settings**.
4. Ensure that **Send alerts** is set as appropriate.

ADVANCED THREAT PROTECTION SETTINGS

Send alerts to i

Also send email notification to admins and subscription owners i

Advanced Threat Protection types >
 All

52.5 Exercise 5: Create a logging and monitoring baseline

Logging and monitoring are a critical requirement when trying to identify, detect, and mitigate security threats. Having a proper logging policy can ensure you can determine when a security violation has occurred, but also potentially identify the culprit responsible. Azure Activity logs provide data about both external access to a resources and diagnostic logs, which provide information about the operation of that specific resource.

52.5.1 Task 1: Ensure that a log profile exists

The Azure Activity Log provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events. The Activity Log was previously known as Audit Logs or Operational Logs, since the Administrative category reports control-plane events for your subscriptions. There is a single Activity Log for each Azure subscription. It provides data about the operations on a resource from the outside. Diagnostic Logs are emitted by a resource and provide information about the operation of that resource. You must enable diagnostic settings for each resource.

1. In the Azure Portal go to **Monitor**, then select **Activity log**.
2. Click **Diagnostic settings**.

Activity log						
Edit columns		Refresh	Diagnostics settings	Download as CSV	Logs	Pin current filters
Management Group : None		Subscription : Contoso IT - demo	Timespan : Last 6 hours	Event severity : All	Add Filter	
First 12 items.						
Operation name	Status	Time	Time stamp	Subscription	Event initiated by	
> Validate Deployment	Succeeded	2 min ago	Tue Oct 29 ...	Contoso IT - demo	5cd1303a9a9848d5956e2...	
> 'deployIfNotExists' Policy action.	Succeeded	3 min ago	Tue Oct 29 ...	Contoso IT - demo	Microsoft Azure Policy Ins...	
> Write GuestConfigurationAssignments	Started	4 min ago	Tue Oct 29 ...	Contoso IT - demo	MicrosoftGuestConfigurat...	
> Write GuestConfigurationAssignments	Succeeded	5 min ago	Tue Oct 29 ...	Contoso IT - demo	MicrosoftGuestConfigurat...	

3. Click the purple banner for the legacy experience.

Name	Storage account	Event hub	Log analytic	Edit setting
No diagnostic settings defined				

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

4. Configure the following settings then click **Save**.

- **Region:** EastUS
- **Select:** Export to Storage Account
- **Storage Account:** Select your storage account and click OK
- **Retention:** 90 days

5. Select **Save**.

Export activity log (PREVIEW)

Save Discard Reset

Archive your activity log to a storage account or stream them to an Azure event hub. Diagnostic data is billed at normal storage rates.

* Subscription i
Azure Pass - Sponsorship

* Regions i
East US

Export to a storage account

Storage account i
csb9de00928aed4x4dd6x8e8 >

Retention (days) i
90

Export to an event hub

52.5.2 Task 2: Change activity log retention is set to 365 days or more

Setting the Retention (days) to 0 retains the data forever.

1. Follow the steps listed above. Adjust the Retention days slider bar.

52.5.3 Task 3: Create an activity log alert for "Creating, updating, or deleting a Network Security Group"

By default, no monitoring alerts are created when NSGs are created/updated/deleted. Changing or deleting a security group can allow internal resources to be accessed from improper sources, or for unexpected outbound network traffic.

1. In to the Azure portal go to **Monitor**, then select **Alerts**.
2. Select **+ New alert rule**.
3. In the **Resource** section click **Select**.
4. Select your subscription and click **Done**.
5. In the **Condition** section click **Add**.
6. Search for **Create or Update Network Security Group** and select it.
7. On the Configure signal logic blade, in the Event initiated by enter **any** and click **Done**.

Alert logic

Event Level All

Status All

Event initiated by any

Condition preview

Whenever the Administrative Activity Log "Create or Update Network Security Group (Microsoft.Network/networkSecurityGroups)" has "any" level, with "any" status and event is initiated by "any"

 Set at least one filter criteria to create an alert

Done

8. In the **Actions** section click **Create action group**.
9. On the Add action group blade enter the following details:
 - **Action group name:** NSG Alert
 - **Short name:** NSGAlert
 - **Action Name:** NSG Alert
 - **Action type:** Email/SMS/Push/Voice
10. On the **Email/SMS/Push/Voice** blade check the email box and enter your email address and click **OK**.

Email/SMS/Push/Voice

Add or edit an Email/SMS/Push/Voice action

Email

* Email

SMS (Carrier charges may apply)

* Country code

* Phone number

Azure app Push Notifications

* Azure account email

Voice

* Country code

* Phone number

Enable the common alert schema. [Learn more](#)

Yes

No

OK

11. On the Add action group blade click **OK**.

Add action group

Action group name	NSG Alert
Short name	NSGAlert
Subscription	Azure Pass - Sponsorship
Resource group	Default-ActivityLogAlerts (to be created)

Actions

ACTION NAME	ACTION TYPE	STATUS	DETAILS	ACTIONS
NSG Alert	Email/SMS/Push/Voice	✓	Edit details	X
Unique name for the action	Select an action type	✓		

[Privacy Statement](#)
[Pricing](#)

12. On the Create rule blade, in the **Alert Details** section enter the following details:

- Alert rule name:** NSG Alert
- Save to resource group:** myResourceGroup

ALERT DETAILS

* Alert rule name ✓

Description
Specify alert description here...

* Save alert to resource group ▼

Enable rule upon creation
 Yes No

 It can take up to 5 minutes for an Activity log alert rule to become active.

13. Click **Create alert rule**

52.6 Exercise 6: Create a Networking baseline

Azure networking services maximize flexibility, availability, resiliency, security, and integrity by design. Network connectivity is possible between resources located in Azure, between on-premises and Azure-hosted resources, and to and from the Internet and Azure.

52.6.1 Task 1: Restrict RDP and SSH access from the Internet

It's possible to reach Azure virtual machines by using Remote Desktop Protocol (RDP) and the Secure Shell (SSH) protocol. These protocols enable the management VMs from remote locations and are standard in datacenter computing.

The potential security problem with using these protocols over the Internet is that attackers can use brute force techniques to gain access to Azure virtual machines. After the attackers gain access, they can use your VM as a launch point for compromising other machines on your virtual network or even attack networked devices outside Azure.

It's recommended that you disable direct RDP and SSH access to your Azure VMs from the Internet. After direct RDP and SSH access from the Internet is disabled, you have other options that you can use to access these VMs for remote management:

- Point-to-site VPN
- Site-to-site VPN
- Azure ExpressRoute
- Azure Bastion Host

1. In the Azure portal click **Virtual machines**.
2. Select **myVM**.
3. open the **Networking** blade.
4. Select the rule which allows RDP (Port 3389) then click **Delete**.

The screenshot shows the Azure portal interface for managing network security groups. On the left, the 'Networking' section of the 'myVM' virtual machine settings is visible. In the center, the 'myNetworkSecurityGroup3389' rule is selected, indicated by a red box around its row in the table. The rule details pane on the right shows the configuration: Source Any, Destination Any, Destination port ranges 3389, Protocol TCP, Action Allow, and Priority 1001.

52.6.2 Task 2: Restrict SQL Server access from the Internet

Firewall systems help prevent unauthorized access to computer resources. If a firewall is turned on but not correctly configured, attempts to connect to SQL Server might be blocked.

To access an instance of the SQL Server through a firewall, you must configure the firewall on the computer that is running SQL Server. Allowing ingress for the IP range 0.0.0.0/0 (Start IP of 0.0.0.0 and End IP of 0.0.0.0) allows open access to any/all traffic potentially making the SQL Database vulnerable to attacks. Ensure that no SQL Databases allow ingress from the Internet.

1. In the Azure portal go to **SQL servers** and select your SQL Server.
2. Click on **Firewalls and virtual networks**.

The screenshot shows the 'az500labs' blade in the Azure portal under the 'Firewalls and virtual networks' section. It displays two main summary messages: one for client IP access (connections from specified IPs) and one for VNET/Subnet access (connections from the VNET/Subnet). Below these are sections for 'Allow Azure services and resources to access this server' (set to ON) and 'Client IP address' (37.122.198.25). A table for 'Client IP' rules is shown with one entry: 'No firewall rules configured.' Below this is another table for 'Virtual networks' rules, also showing 'No vnet rules for this server.'

3. Ensure that the firewall rules exist, and no rule has a Start IP of 0.0.0.0 and End IP of 0.0.0.0 or other combinations which allows access to wider public IP ranges.
4. Close the blade.

52.6.3 Task 3: Configure the NSG flow logs

When you create or update a virtual network in your subscription, Network Watcher will be enabled automatically in your Virtual Network's region. There is no impact to your resources or associated charge for automatically enabling Network Watcher.

Network security group (NSG) flow logs are a feature of Network Watcher that allows you to view information about ingress and egress IP traffic through an NSG. Flow logs are written in JSON format, and show outbound and inbound flows on a per rule basis, the network interface (NIC) the flow applies to, 5-tuple information about the flow (Source/destination IP, source/destination port, and protocol), if the traffic was allowed or denied, and

in Version 2, throughput information (Bytes and Packets). Logs can be used to check for anomalies and give insight into suspected breaches.

1. In the Azure portal select **All services**.
2. Select **Networking**.
3. Select **Network Watcher**.
4. Select **NSG flow logs** under Logs.
5. Select **On**.
6. Select a storage account and click **Save**.

52.6.4 Task 4: Enable Network Watcher

Network security group (NSG) flow logs are a feature of Network Watcher that allows you to view information about ingress and egress IP traffic through an NSG.

1. In the Azure portal select All services. In the Filter box, enter **Network Watcher**. When Network Watcher appears in the results, select it.
2. Select Regions, to expand it, and then select the elipsis (...) button on a region which is not enabled.
3. Select **Enable Network Watcher**.

The screenshot shows the Azure Network Watcher interface. On the left, there's a sidebar with 'Overview', 'Monitoring' (Topology, Connection monitor, Network Performance Monitor), and 'Network diagnostic tools' (IP flow verify, Next hop, Effective security rules). The main area is titled 'Subscriptions: Azure Pass - Sponsorship'. It lists 'Azure Pass - Sponsorship' with three regions: West US (Enabled), East US (Enabled), and North Europe (Disabled). A red box highlights the 'Enable network watcher' button next to the North Europe row.

NAME	REGION	STATUS
Azure Pass - Sponsorship	▼ 30 regions	Partially enabled
	West US	Enabled
	East US	Enabled
	North Europe	Disabled

52.7 Exercise 7: Create an Azure VM baseline

Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements. Azure Policy meets this need by evaluating your resources for non-compliance with assigned policies. For example, you can have a policy to allow only a certain SKU size of virtual machines in your environment. Once this policy is implemented, new and existing resources are evaluated for compliance. With the right type of policy, existing resources can be brought into compliance.

Azure networking security recommendations

Here are the security recommendations you should follow to set Virtual Machine (VM) policies on your Azure subscription. Included with each recommendation are the basic steps to follow in the Azure portal. You should perform these steps on your own subscription with your own resources to validate the security for each. Keep in mind that Level 2 options might restrict some features or activity, so carefully consider which security options you decide to enforce.

52.7.1 Task 1: Ensure that OS disk are encrypted

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks of Azure virtual machines (VMs). It is also integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets, and ensures that all data on the VM disks are encrypted at rest while in Azure storage. Azure Disk Encryption for Windows and Linux VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

If you use Azure Security Center (recommended), you're alerted if you have VMs that aren't encrypted.

1. In the Azure portal search for **KeyVault**.
2. Select **Key Vault** and click **Create**.

3. Enter the following details:

- **Resource Group:** myResourceGroup
- **Key vault name:** *Enter something unique*
- **Region:** EastUS

Create key vault

Basics Access policy Virtual network Tags Review + create

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance. [Learn more](#)

Project details

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

* Subscription	Azure Pass - Sponsorship
* Resource group	myResourceGroup
	Create new

Instance details

* Key vault name <small>i</small>	AZ-500-Vault
* Region	East US
* Pricing tier <small>i</small>	Standard

4. Select the **Access policy** tab and select **Azure Disk Encryption** for volume encryption.

Basics **Access policy** Virtual network Tags Review + create

Enable Access to:

- Azure Virtual Machines for deployment i
- Azure Resource Manager for template deployment i
- Azure Disk Encryption for volume encryption i

5. Click **Review + create** then click **Create**.

6. Wait for the deployment to complete before continuing.

7. In the Azure portal select **Virtual machines**.

8. Select **myVM** virtual machine.

9. Under the **Settings** section select **Disks**.

10. Notice the disk is not encrypted.

OS disk		NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOST CACHING
		myVM_OsDisk_1_f45935987ebe40c180df679a80b7ed1b	127 GiB	Premium SSD	Not enabled	Read/write

11. Click **Encryption**.

The screenshot shows the 'Disks' blade for a virtual machine named 'myVM'. On the right, there's a toolbar with 'Edit', 'Refresh', 'Encryption' (which is highlighted with a red box), and 'Swap OS Disk'. Below the toolbar, there are two informational cards: one about managed disks being encrypted at rest and another about Ultra Disk compatibility.

12. Select **OS & data disks** to be encrypted.

13. Click **Select a key vault and key for encryption** and select your vault and click **Select**.

14. Click **Save** and click **Yes** to confirm.

52.7.2 Task 2: Ensure only approved extensions are installed

Azure virtual machine (VM) extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs. For example, if a virtual machine requires software installation, anti-virus protection, or to run a script inside of it, a VM extension can be used. Azure VM extensions can be run with the Azure CLI, PowerShell, Azure Resource Manager templates, and the Azure portal. Extensions can be bundled with a new VM deployment, or run against any existing system.

1. In the Azure portal select **Virtual machines**.
2. Select **myVM** and then in the **Settings** section click **Extensions**.
3. Ensure that the listed extensions are approved for use.

The screenshot shows the 'Extensions' blade for the 'myVM' virtual machine. On the left, there's a sidebar with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems'. Below that is a 'Settings' section with 'Networking', 'Disks', 'Size', 'Security', and 'Extensions' (which is highlighted with a blue box). The main area shows a table of installed extensions:

NAME	TYPE	VERSION
IaaSAntimalware	Microsoft.Azure.Security.IaaSAntimalware	1.*
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Monitoring.MicrosoftMonitor...	1.*

Results: You have now completed this lab.

53 Module 4: Lab 9 - JIT

Scenario

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Brute force attacks commonly target management ports as a means to gain access to a VM. If successful, an attacker can take control over the VM and establish a foothold into your environment.

One way to reduce exposure to a brute force attack is to limit the amount of time that a port is open. Management ports don't need to be open at all times. They only need to be open while you're connected to the VM, for example to perform management or maintenance tasks. When just-in-time is enabled, Security Center uses network security group (NSG) and Azure Firewall rules, which restrict access to management ports so they cannot be targeted by attackers.

53.1 Exercise 1: Manage virtual machine access using just-in-time

There are three ways to configure a JIT policy on a VM:

- Configure JIT access in Azure Security Center
- Configure JIT access in an Azure VM blade
- Configure a JIT policy on a VM programmatically

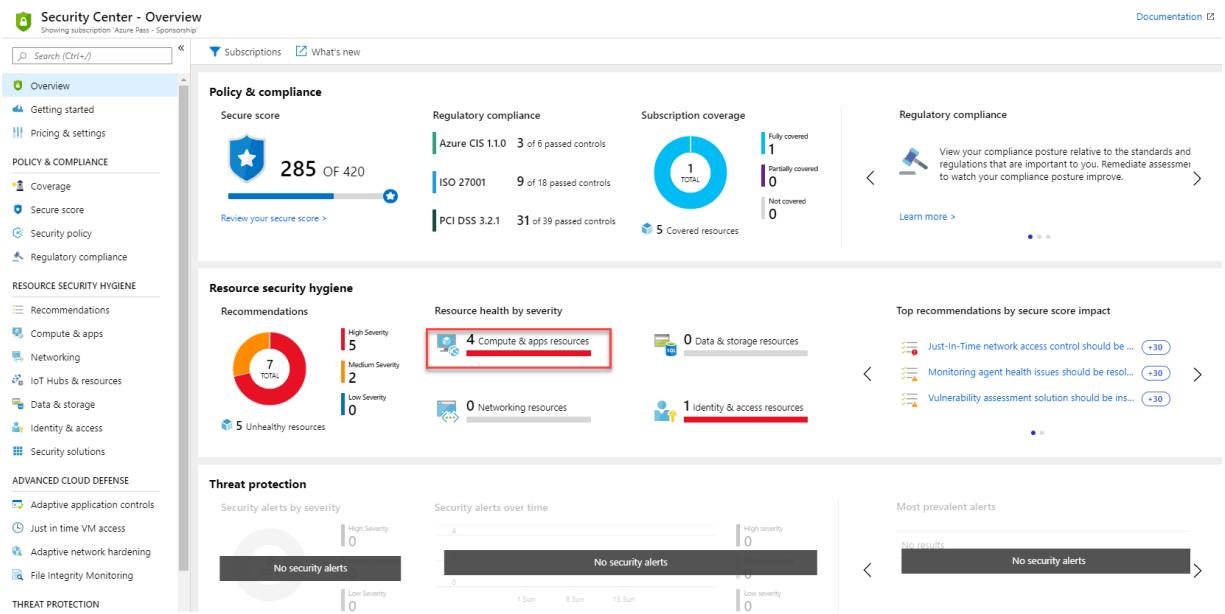
53.1.1 Task 1: Configure JIT access on a VM in Azure Security Center

1. In the Azure Portal open the **Security Center** and then click **Getting Started**.
2. Click **Install agents**.

The screenshot shows the Azure Security Center - Getting started page. On the left, there's a sidebar with links to Home, Dashboard, All services, Favorites, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, and Help + support. The main content area has a heading 'Security Center detected virtual machines without the data collection agent installed!' in bold. Below it, a message says: 'Protect your virtual machines now by installing the Security Center data collection agent on each VM. To receive security alerts and recommendations, the agent must be installed.' There's a 'Learn more >' link. Under 'Install agents automatically', it says: 'The Microsoft Monitoring Agent will be automatically installed on all the virtual machines in selected subscription.' A section titled 'Select subscriptions on which agents will be installed' shows '2 Managed resources'. Two checkboxes are shown: 'NAME' (selected) and 'Azure Pass - Sponsorship' (selected). At the bottom, there's a large blue 'Install agents' button with a red border, and a 'Remind me later' link.

Note: You may have to wait upto 5 minutes for the agents to deploy.

2. In the left pane, select **Overview**.
3. Select **Compute & app resources**.



- On the Compute blade, note the recommendations.
- Select the **Just-In-Time network access control should be applied on virtual machines**.

Compute

Add Computers

Overview **VMs and Computers** **VM scale sets**

RECOMMENDATION

Just-In-Time network access control should be applied on virtual machines (highlighted)

Vulnerability assessment solution should be installed on your virtual machines

Monitoring agent health issues should be resolved on your machines

Install endpoint protection solution on virtual machines

Access should be restricted for permissive Network Security Groups with Internet-facing VMs

Disk encryption should be applied on virtual machines

- Select all 4 virtual machines and click **Enable JIT on 4 VMs**.

Apply a just in time VM access control

□ >

Filter Enable JIT on 4 VMs

VIRTUAL MA...	RESOURC...	SUBSCRIPTI...	STATE	SEVERITY	...
<input checked="" type="checkbox"/> myVM1	MYRESOURC...	Azure Pass - ...	Open	! High	...
<input checked="" type="checkbox"/> myVM2	MYRESOURC...	Azure Pass - ...	Open	! High	...
<input checked="" type="checkbox"/> Srv-Jump	TEST-FW-RG	Azure Pass - ...	Open	! High	...
<input checked="" type="checkbox"/> Srv-Work	TEST-FW-RG	Azure Pass - ...	Open	! High	...

7. On the **JIT VM access configuration** blade click **Save**.

- This blade displays the default ports recommended by Azure Security Center:
 - 22 - SSH
 - 3389 - RDP
 - 5985 - WinRM
 - 5986 - WinRM

JIT VM access configuration

□ >

myVM1, myVM2, Srv-Work, Srv-Jump

Add Save Discard

Configure the ports for which the just in time VM access will be applicable

PORT	PROT...	ALLOWED SOUR...	IP RANGE	TIME RANGE (H...	...
22 (Recommended)	Any	Per request	N/A	3 hours	...
3389 (Recommended)	Any	Per request	N/A	3 hours	...
5985 (Recommended)	Any	Per request	N/A	3 hours	...
5986 (Recommended)	Any	Per request	N/A	3 hours	...

1. Close all the blade and on the Security Center blade click **Just in time VM access**.

The screenshot shows the Azure Security Center interface for 'Just in time VM access'. The left sidebar has sections like 'POLICY & COMPLIANCE' (Coverage, Secure score, Security policy, Regulatory compliance), 'RESOURCE SECURITY HYGIENE' (Recommendations, Compute & apps, Networking, IoT Hubs & resources, Data & storage, Identity & access, Security solutions), 'ADVANCED CLOUD DEFENSE' (Adaptive application controls, Just in time VM access, Adaptive network hardening, File Integrity Monitoring), 'THREAT PROTECTION' (Security alerts, Security alerts map (Preview)), and 'AUTOMATION & ORCHESTRATION' (Playbooks (Preview)). The 'Just in time VM access' link is highlighted with a red box. The main content area shows 'Virtual machines' with tabs for 'Configured' (selected), 'Recommended', and 'No recommendation'. It lists 4 VMs: myVM1, myVM2, Srv-Jump, and Srv-Work, all with 0 Requests. A search bar at the top says 'Search (Ctrl+ /)'.

VIRTUAL MACHINE	APPROVED
myVM1	0 Requests
myVM2	0 Requests
Srv-Jump	0 Requests
Srv-Work	0 Requests

The **Just-in-time VM access** window opens.

Just-in-time VM access provides information on the state of your VMs:

- **Configured** - VMs that have been configured to support just-in-time VM access. The data presented is for the last week and includes for each VM the number of approved requests, last access date and time, and last user.
- **Recommended** - VMs that can support just-in-time VM access but haven't been configured to. We recommend that you enable just-in-time VM access control for these VMs.
- **No recommendation** - Reasons that can cause a VM not to be recommended are:
 - Missing NSG - The just-in-time solution requires an NSG to be in place.
 - Classic VM - Security Center just-in-time VM access currently supports only VMs deployed through Azure Resource Manager. A classic deployment is not supported by the just-in-time solution.
 - Other - A VM is in this category if the just-in-time solution is turned off in the security policy of the subscription or the resource group, or if the VM is missing a public IP and doesn't have

an NSG in place.

Note: When JIT VM Access is enabled for a VM, Azure Security Center creates "deny all inbound traffic" rules for the selected ports in the network security groups associated and Azure Firewall with it. If other rules had been created for the selected ports, then the existing rules take priority over the new "deny all inbound traffic" rules. If there are no existing rules on the selected ports, then the new "deny all inbound traffic" rules take top priority in the Network Security Groups and Azure Firewall.

53.1.2 Task 2: Request JIT access via ASC

To request access to a VM via ASC:

1. Under **Just in time VM access**, select the **Configured** tab.
2. Under **Virtual Machine**, select one of the VMs that you want to request access for. This puts a checkmark next to the VM.
 - The icon in the **Connection Details** column indicates whether JIT is enabled on the NSG or FW. If it's enabled on both, only the Firewall icon appears.
 - The **Connection Details** column provides the information required to connect the VM, and its open ports.

The screenshot shows the Azure Security Center interface for 'Just in time VM access'. On the left, there's a navigation sidebar with sections like 'POLICY & COMPLIANCE' (Coverage, Secure score, Security policy, Regulatory compliance), 'RESOURCE SECURITY HYGIENE' (Recommendations, Compute & apps, Networking, IoT Hubs & resources, Data & storage, Identity & access, Security solutions), and 'ADVANCED CLOUD DEFENSE' (Adaptive application controls). The 'Just in time VM access' section is highlighted. The main area has a heading 'Virtual machines' with tabs for 'Configured', 'Recommended', and 'No recommendation'. It says '4 VMs' and shows a table with columns: VIRTUAL MACHINE, APPROVED, LAST ACCESS, and CONNECTION DETAILS. The first row for 'myVM1' has a checked checkbox in the VIRTUAL MACHINE column, indicating it's configured. Other rows for 'myVM2', 'Srv-Jump', and 'Srv-Work' have unchecked checkboxes. A 'Request access' button is visible at the top right of the table area.

3. Click **Request access**. The **Request access** window opens.

The screenshot shows the 'Request access' window for 'myVM1'. It asks to 'Please select the ports that you would like to open per virtual machine.' Below is a table with columns: PORT, TOGGLE, ALLOWED SOURCE IP, IP RANGE, and TIME RANGE (HOURS). The table lists four ports: 22, 3389, 5985, and 5986. Each row has an 'On' or 'Off' toggle switch, a 'My IP' button, an 'IP Range' input field set to 'No range', and a 'TIME RANGE (HOURS)' slider set to 3. The 'PORT' column has a dropdown arrow pointing to 'myVM1'.

PORT	TOGGLE	ALLOWED SOURCE IP	IP RANGE	TIME RANGE (HOURS)			
22	On	Off	My IP	IP Range	No range	<input type="range" value="3"/>	3
3389	On	Off	My IP	IP Range	No range	<input type="range" value="3"/>	3
5985	On	Off	My IP	IP Range	No range	<input type="range" value="3"/>	3
5986	On	Off	My IP	IP Range	No range	<input type="range" value="3"/>	3

4. Under **Request access**, for each VM, configure the ports that you want to open and the source IP addresses that the port is opened on and the time window for which the port will be open. It will only be possible to request access to the ports that are configured in the just-in-time policy. Each port has a maximum allowed time derived from the just-in-time policy.

5. Click **Open ports**.

Note: If a user who is requesting access is behind a proxy, the option **My IP** may not work. You may need to define the full IP address range of the organization.

53.1.3 Task 3: Edit a JIT access policy via ASC

You can change a VM's existing just-in-time policy by adding and configuring a new port to protect for that VM, or by changing any other setting related to an already protected port.

To edit an existing just-in-time policy of a VM:

1. In the **Configured** tab, under **VMs**, select a VM to which to add a port by clicking on the three dots within the row for that VM.
2. Select **Edit**.
3. Under **JIT VM access configuration**, you can either edit the existing settings of an already protected port or add a new custom port.

VIRTUAL MACHINE	APPROVED	LAST ACCESS	CONNECTION DETAILS	LAST USER
myVM1	0 Requests	N/A	shield -	N/A
myVM2	0 Requests	N/A	shield -	N/A
Srv-Jump	0 Requests	N/A	shield -	N/A
Srv-Work	0 Requests	N/A	shield -	N/A

53.1.4 Task 4: Audit JIT access activity in ASC

You can gain insights into VM activities using log search. To view logs:

1. Under **Just-in-time VM access**, select the **Configured** tab.
2. Under **VMs**, select a VM to view information about by clicking on the three dots within the row for that VM and select **Activity Log** in the menu. The **Activity log** opens.

VIRTUAL MACHINE	APPROVED	LAST ACCESS	CONNECTION DETAILS	LAST USER
myVM1	0 Requests	N/A	shield -	N/A
myVM2	0 Requests	N/A	shield -	N/A
Srv-Jump	0 Requests	N/A	shield -	N/A
Srv-Work	0 Requests	N/A	shield -	N/A

Activity log provides a filtered view of previous operations for that VM along with time, date, and subscription.

You can download the log information by selecting **Click here to download all the items as CSV**.

Modify the filters and click **Apply** to create a search and log.

53.1.5 Task 5: Configure JIT access on a VM via the Azure VM blade

To make it easy to roll out just-in-time access across your VMs, you can set a VM to allow only just-in-time access directly from within the VM.

1. In the Azure portal, select **Virtual machines**.
2. Click on the virtual machine you want to limit to just-in-time access.
3. In the menu, click **Configuration**.

4. Under **Just-in-time-access** click **Enable just-in-time policy**.

This enables just-in-time access for the VM using the following settings:

- Windows servers:
 - RDP port 3389
 - Three hours of maximum allowed access
 - Allowed source IP addresses is set to Any
- Linux servers:
 - SSH port 22
 - Three hours of maximum allowed access
 - Allowed source IP addresses is set to Any

If a VM already has just-in-time enabled, when you go to its configuration page you will be able to see that just-in-time is enabled and you can use the link to open the policy in Azure Security Center to view and change the settings.

The screenshot shows the Azure portal's 'Virtual machines' blade. A specific VM named 'vm-contoso-us' is selected and highlighted with a red box. On the right, the 'vm-contoso-us - Configuration' pane is open. Within this pane, the 'Just-in-time access' section is highlighted with a red box, containing a callout bubble with the text 'To improve security, enable a just-in-time access policy.' and a blue 'Enable just-in-time policy' button. Below this, the 'Azure hybrid benefit' section is shown with a 'No' and 'Yes' button. At the bottom of the configuration pane, the 'Configuration' section is also highlighted with a red box. The left sidebar lists other VMs: vm-usa, vm-europe, vm-contoso1, vm-contoso2, vmcontoso-3, vm-contoso4, vm-london, vm-marketing, vm-hr, vm-uni, vm-contoso-hr, and vm-contoso.

53.1.6 Task 5: Request JIT access to a VM via the Azure VM blade

In the Azure portal, when you try to connect to a VM, Azure checks to see if you have a just-in-time access policy configured on that VM.

- If you do have a JIT policy configured on the VM, you can click **Request access** to enable you to have access in accordance with the JIT policy set for the VM.

Connect to virtual machine

X

vm1



This VM has a just-in-time access policy. Select "Request access" before connecting.

RDP

SSH

You need to request access to connect to your virtual machine. Select an IP address, optionally change the port number, and select "Request access". [Learn more](#)

o

* IP address

Public IP address (52.161.18.9)



* Port number

3389

Request access

[Download RDP file anyway](#)

Having trouble connecting to this VM?

- [Diagnose and solve problems](#)
- [Troubleshoot connection](#)
- [Serial console](#)

The access is requested with the following default parameters:

- **source IP:** 'Any' (*) (cannot be changed)
- **time range:** Three hours (cannot be changed)
- **port number:** RDP port 3389 for Windows / port 22 for Linux (can be changed)

Note: After a request is approved for a VM protected by Azure Firewall, Security Center provides the user with the proper connection details (the port mapping from the DNAT table) to use to connect to the VM.

- If you do not have JIT configured on a VM, you will be prompted to configure a JIT policy it.

Connect to virtual machine

X

vm1



This VM has a just-in-time access policy. Select "Request access" before connecting.

RDP

SSH

You need to request access to connect to your virtual machine. Select an IP address, optionally change the port number, and select "Request access". [Learn more](#)

o

* IP address

Public IP address (52.161.18.9)



* Port number

3389

Request access

[Download RDP file anyway](#)

Having trouble connecting to this VM?

- [Diagnose and solve problems](#)
- [Troubleshoot connection](#)
- [Serial console](#)

WARNING: Prior to continuing you should remove all resources used for this lab. To do this in the **Azure Portal** click [Remove](#).

Results: You have now completed this lab.