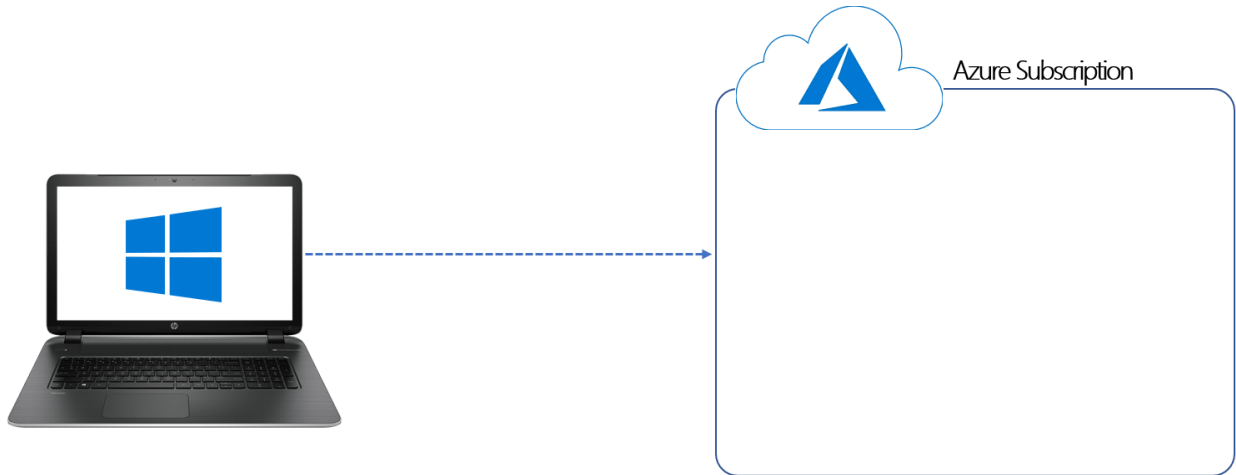


Chapter 1: Introduction to Azure Security

Responsibility	On-prem	IaaS	PaaS	SaaS
Data classification & accountability	Customer	Customer	Customer	Customer
Client & end-point protection	Customer	Customer	Customer	Customer
Identity & access management	Customer	Customer	Shared	Shared
Application-level controls	Customer	Customer	Shared	Cloud provider
Network controls	Customer	Shared	Cloud provider	Cloud provider
Host infrastructure	Customer	Shared	Cloud provider	Cloud provider
Physical security	Customer	Cloud provider	Cloud provider	Cloud provider

■ Customer ■ Cloud provider



1. Enter your email address

Sign in

No account? [Create one!](#)

[Can't access your account?](#)

Sign in with Windows Hello or a security key [?](#)


2. Click here



Next

Your profile



Country/Region 

United Kingdom 

Choose the location that matches your billing address. **You cannot change this selection later.** If your country is not listed, the offer is not available in your region.


[Learn More](#)

First name

David

Last name


Okeyode

Email address 

 packt-az500@outlook.com

Phone

 95

Company VatID 

Optional

Leave Empty

Next



Click to proceed

Your profile



Identity verification by phone



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

Country code

Phone number

Click here to proceed



Identity verification by card



We'll make a temporary authorization on this card, but **you won't be charged unless you upgrade.**

We accept the following cards:



Cardholder Name

Card number

Expires

<input type="text" value="MM"/>	<input type="text" value="YY"/>
---------------------------------	---------------------------------

CVV

[What is a CVV?](#)

Agreement



I agree to the [subscription agreement](#), [offer details](#), and [privacy statement](#).

I would like information, tips, and offers about Azure, including Azure Newsletter, Pricing updates, and other Microsoft products and services.

I would like Microsoft to share my information with select partners so I can receive relevant information about their products and services.

Sign up



Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Azure services



Create a resource



Subscriptions



Virtual machines



App Services



Storage accounts

Navigate



Subscriptions



Resource groups

Subscriptions

Default Directory


[+ Add](#)





View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have RBAC permissions, see [RBAC permissions for subscriptions](#). Showing subscriptions in Default Directory directory. Don't see a subscription? [Switch directories](#)

My role  Status 

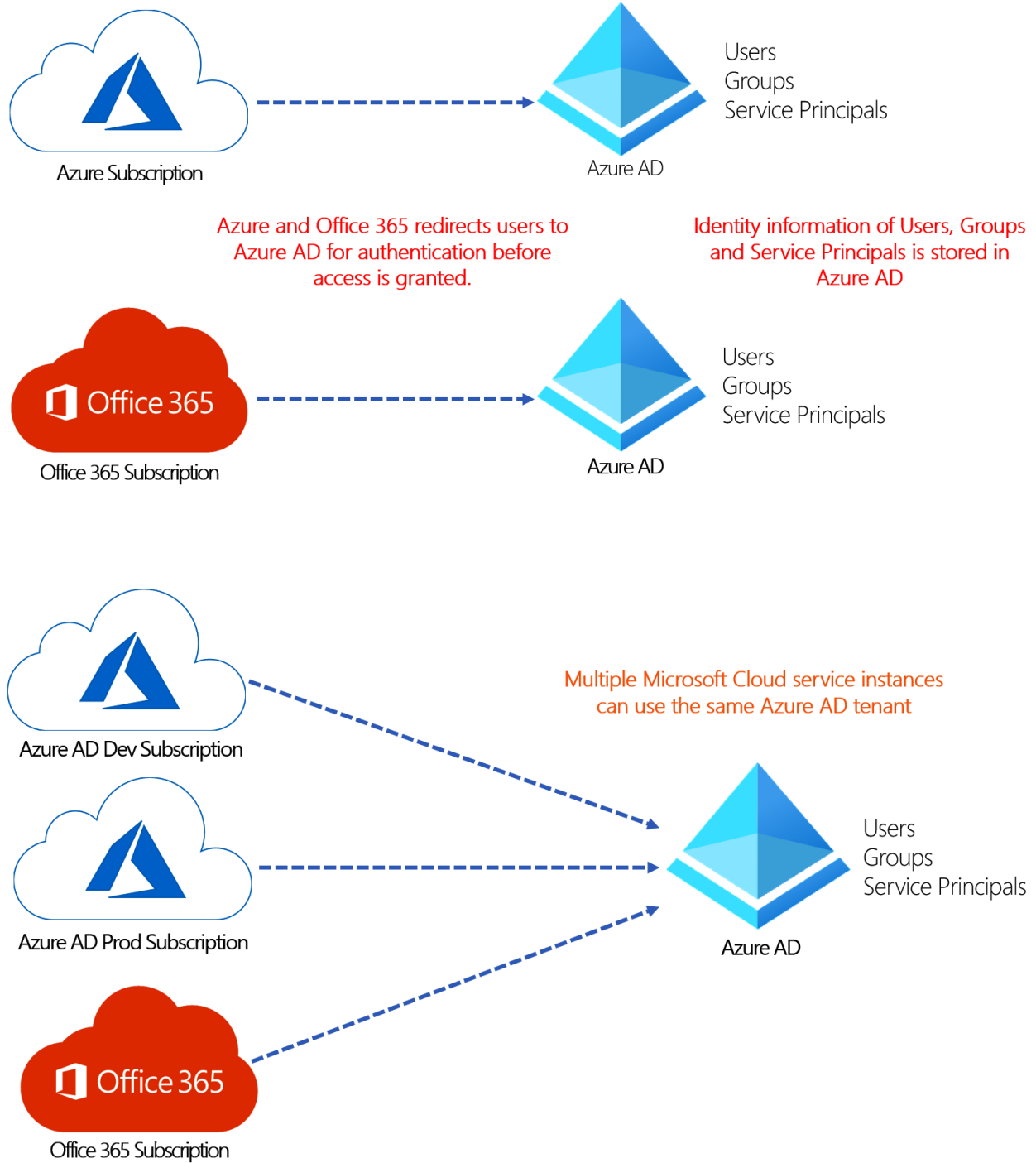
8 selected 3 selected

[Apply](#)

Showing 1 of 1 subscriptions Show only subscriptions selected in the [global subscriptions filter](#) 

Subscription name 	Subscription ID 	My role 
 Free Trial	5d5[REDACTED]	Account admin

Chapter 2: Understanding Azure AD



Microsoft Cloud
Services

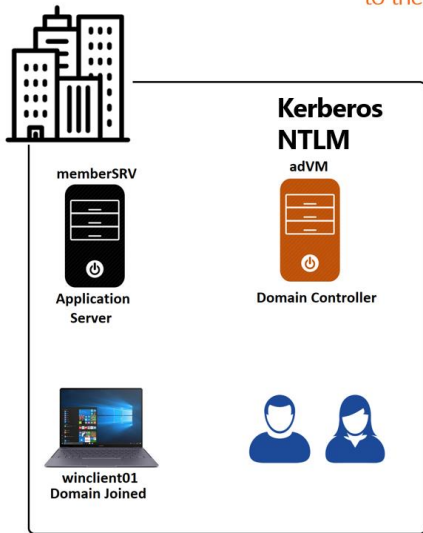
Cloud SaaS
apps



Azure Active
Directory

On-premises
apps

It is not practical to expose Kerberos ports to the Internet for authentication!



Kerberos Ports

- UDP 88
- TCP 88
- TCP 2105
- TCP 544
- TCP 1 - 1023
- TCP 32000 - 65535



The screenshot shows the Azure portal interface. The browser address bar displays 'portal.azure.com/#home'. A red box highlights the menu icon (three horizontal lines) in the top left corner, with a red arrow pointing to it and the text '1. Click the portal menu icon'. Below the menu icon, a list of navigation options is shown: 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Azure Active Directory', and 'Resource groups'. A red box highlights 'Azure Active Directory', with a red arrow pointing to it and the text '2. Select Azure AD'. The main content area shows 'Azure services' with a 'Create a resource' button and 'Navigate' options.

Default Directory

Search your tenant

Tenant information

Your role
Global administrator [More info](#)

License
Azure AD Free ← **Our Azure AD license edition**

Tenant ID
7f3e6937-... ← **Unique ID of our Azure AD tenant**

Primary domain
davidpacktaz500outlook.onmicrosoft.com ← **Default domain name of our Azure AD tenant**

Azure AD Connect

Status
Not enabled

Last sync

Switch tenant Delete tenant +

Default Directory

Search your tenant

Tenant information

Your role
Global administrator [More info](#)

License
Azure AD Free

- Overview
- Getting started
- Preview hub
- Diagnose and solve problems
- Manage
 - Users**
 - Groups
 - External Identities

Users | All users (Preview)

Default Directory - Azure Active Directory

Navigation: + New user + New guest user Bulk operations Refresh Reset password Multi-Factor

This page includes previews available for your evaluation. View previews →

Search users Add filters

1 user found

Name	User principal name	User type
<input type="checkbox"/> DO David Okeyode	david-packt-az500_outlook.com#EXT#@davidpacktaz500outlo...	Member

Activity: Sign-ins, Audit logs, Bulk operation results

The single user is the account that we used to sign up for our Azure subscription

Default Directory | Custom domain names

Azure Active Directory

Navigation: + Add custom domain Refresh Troubleshoot Columns

Click to add a new custom domain

Search domains Add filters

Name
davidpacktaz500outlook.onmicrosoft.com

Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM)

Custom domain na... ✕

Default Directory

Custom domain name * ⓘ


azureblueteam.io ✓




Add domain

azureblueteam.io

Custom domain name

 Delete |  Got feedback?

 To use azureblueteam.io with your Azure AD, create a new TXT record with your domain name registrar using the info below.

Record type	<input checked="" type="radio"/> TXT <input type="radio"/> MX
Alias or host name	<input type="text" value="@"/> 
Destination or points to address	<input type="text" value="MS=ms98302515"/> 
TTL	<input type="text" value="3600"/> 

[Share these settings via email](#)

Verification will not succeed until you have configured your domain with your registrar as described above.



Make a note of this information as it will be needed for verification


[Verify](#)

Type *	Host *	TXT Value *
<input type="text" value="TXT"/> ▼	<input type="text" value="@"/>	<input type="text" value="MS=ms98302515"/>
TTL *	Seconds *	
<input type="text" value="Custom"/> ▼	<input type="text" value="3600"/>	
		<input checked="" type="button" value="Save"/> <input type="button" value="Cancel"/>

azureblueteam.io

Custom domain name

 Make primary  Delete

 Verification succeeded!

Type Custom

Status Verified

Federated No

To configure azureblueteam.io 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

Name	Status	Federated	Primary
azureblueteam.io	 Verified		
davidpacktaz500outlook.onmicrosoft.com	 Available		

Default Directory | Overview


Azure Active Directory


 App registrations

 Identity Governance


 Application proxy

 Licenses






 Azure AD Connect

 Custom domain names

 Mobility (MDM and MAM)

 Password reset


 Company branding

 Switch tenant  Delete tenant  Create a tenant  What's new |  Preview

Tenant information

Your role
Global administrator [More info](#)

License
Azure AD Free

Tenant ID
7f3e6... 

Primary domain
davidpacktaz500outlook.onmicrosoft.com

Azure AD Connect

Status
Not enabled

Last sync
Sync has never run



Licenses | All products

Default Directory - Azure Active Directory



Overview



Diagnose and solve problems

Manage



Licensed features



All products



Self-service sign up products

<<

+ Try / Buy

+

Assign



Bills



Columns



Name

No results.

Activate



Browse available plans and features

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.

∨ 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.

∧ 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

+ Try / Buy + Assign Bills | Columns | Got feedback?

<input type="checkbox"/>	Name	Total	Assigned	Available	Expiring soon
<input type="checkbox"/>	Azure Active Directory Premium P2	100	0	100	0

azureblueteam (Default Directory) | Overview

Azure Active Directory

- Overview
- Getting started
- Preview hub
- Diagnose and solve problems
- Manage
 - Users
 - Groups
 - External Identities
 - Roles and administrators
 - Administrative units
 - Enterprise applications
 - Devices
 - App registrations
 - Identity Governance

Switch tenant Delete tenant Create a tenant What's new Preview features

Azure Active Directory can help you enable remote work for your employees and partners. Learn more

azureblueteam (Default Directory)

Search your tenant

Tenant information

Your role
Global administrator [More info](#)

License
Azure AD Premium P2

Tenant ID
7f3e6[redacted]

Primary domain
azureblueteam.io

Azure AD Connect

Status
Not enabled

Last sync
Sync has never run

Other Account Sources

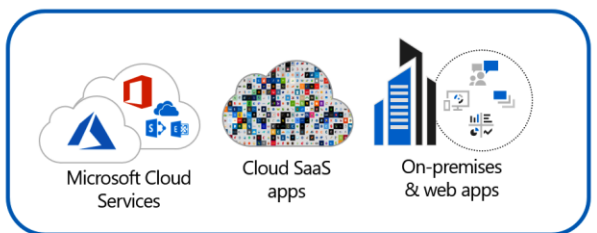
Microsoft Accounts



External Azure AD



On-Premises AD



Every user who needs access to services protected by Azure AD needs a user account



Internal Users

- Azure AD User
- On-Prem User
- MS User

External Users

- Microsoft User
- External Azure AD User

Microsoft account user invited

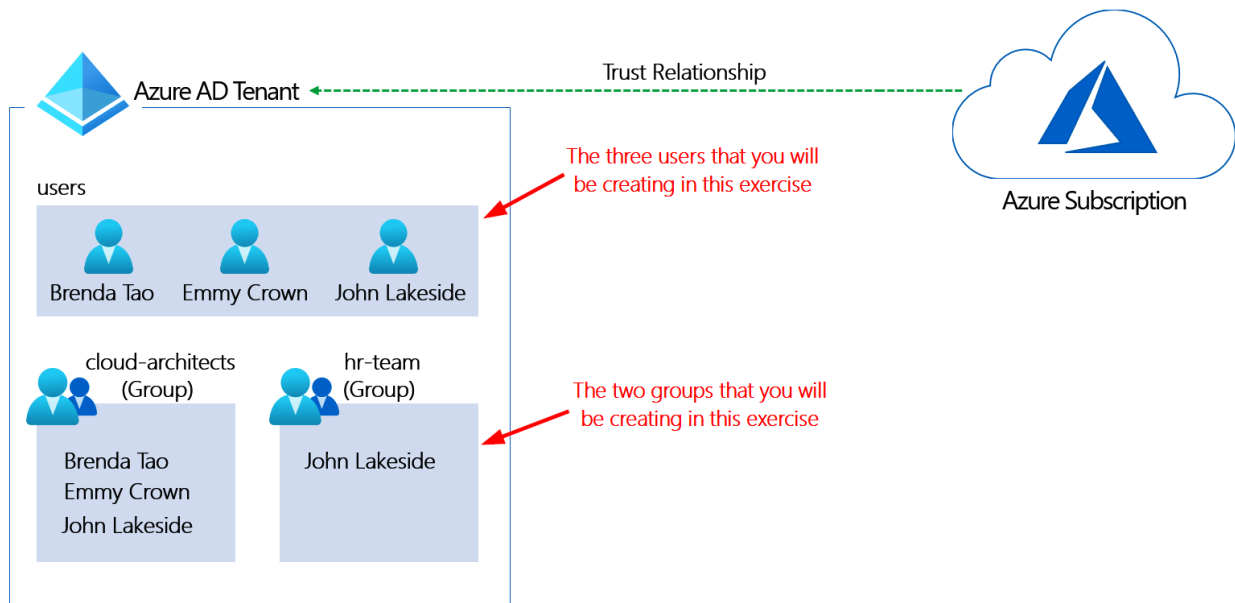
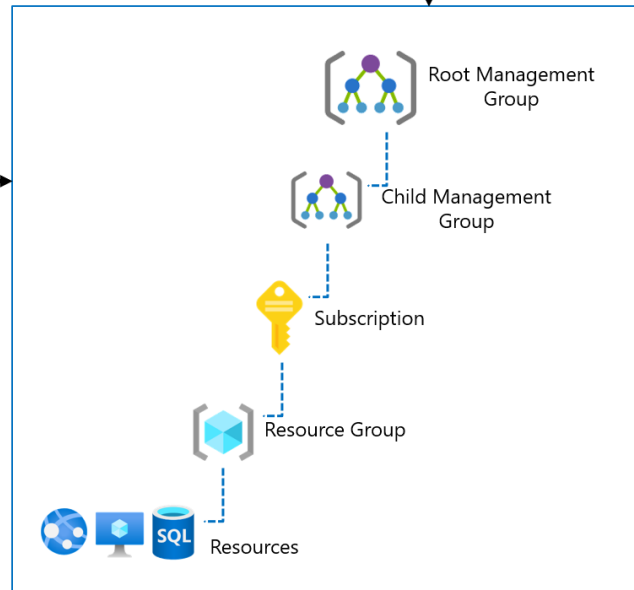
External Azure AD user invited

On-premises AD user synchronized

Azure AD roles are used to grant access to Azure AD. Example roles are:
Global Administrator, User Administrator



Azure RBAC roles are used to grant access to Azure resources. Example roles are:
Owner; Contributor and Reader



- Overview
- Getting started
- Preview hub
- Diagnose and solve problems
- Manage
 - Users**
 - Groups
 - External Identities

1. Click on "Users"

Users | All users (Preview)

azureblueteam (Default Directory) - Azure Active Directory

- All users (Preview)
- Deleted users (Preview)
- Password reset
- User settings
- Diagnose and solve problems
- Activity
 - Sign-ins
 - Audit logs

+ New user + New guest user Bulk operations Refresh

2. Click to create a new user

This page includes previews available for your evaluation. View previews →

Search users Add filters

1 user found

Name	User principal name	User type
<input type="checkbox"/> DO David Okeyode	david-packt-az500_outloo...	Member

New user

azureblueteam (Default Directory)

Got feedback?

Create user

Create a new user in your organization. This user will have a user name like `alice@azureblueteam.io`.

[I want to create users in bulk](#)

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.

[I want to invite guest users in bulk](#)

Help me decide

Identity

User name * ⓘ

brenda @ azureblueteam.io

The domain name I need isn't shown here

Name * ⓘ

Brenda Tao ✓

First name

Brenda ✓

Last name

Tao ✓

Settings

Block sign in

Yes **No**

Ensure it is set to "No"

Usage location

United Kingdom

Job info

Job title

Cloud Solutions Architect

Department

IT

Company name

Azure Blue Team

Manager

No manager selected

Create

Search users

Add filters

4 users found

	Name	↑↓	User principal name	↑↓	User type	Directory synced
<input type="checkbox"/>	DO David Okeyode		david-packt-az500_outloo...		Member	No
<input type="checkbox"/>	BT Brenda Tao		brenda@azureblueteam.io		Member	No
<input type="checkbox"/>	EC Emmy Crown		emmy@azureblueteam.io		Member	No
<input type="checkbox"/>	JL John Lakeside		john@azureblueteam.io		Member	No

- Overview
- Getting started
- Preview hub
- Diagnose and solve problems

Manage

- Users
- Groups**
- External Identities

- All groups
- Deleted groups
- Diagnose and solve problems


Settings

- General
- Expiration
- Naming policy

Activity

Click to create a new group

[+ New group](#) [Download groups](#)

 This page includes previews available

Name

No groups found

New Group

Group type * ⓘ

Security

Group name * ⓘ

cloud-architects

Group description ⓘ

A Group for Cloud Architects

Azure AD roles can be assigned to the group (Preview) ⓘ

Yes No

Membership type * ⓘ

Assigned

Owners

1 owner selected

Add "Brenda Tao" as an owner

Members

2 members selected

Add "Brenda Tao" and "Emmy Crown" as members

Create

Dynamic membership rules



4
Save | Discard | Got feedback?

Configure Rules | Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

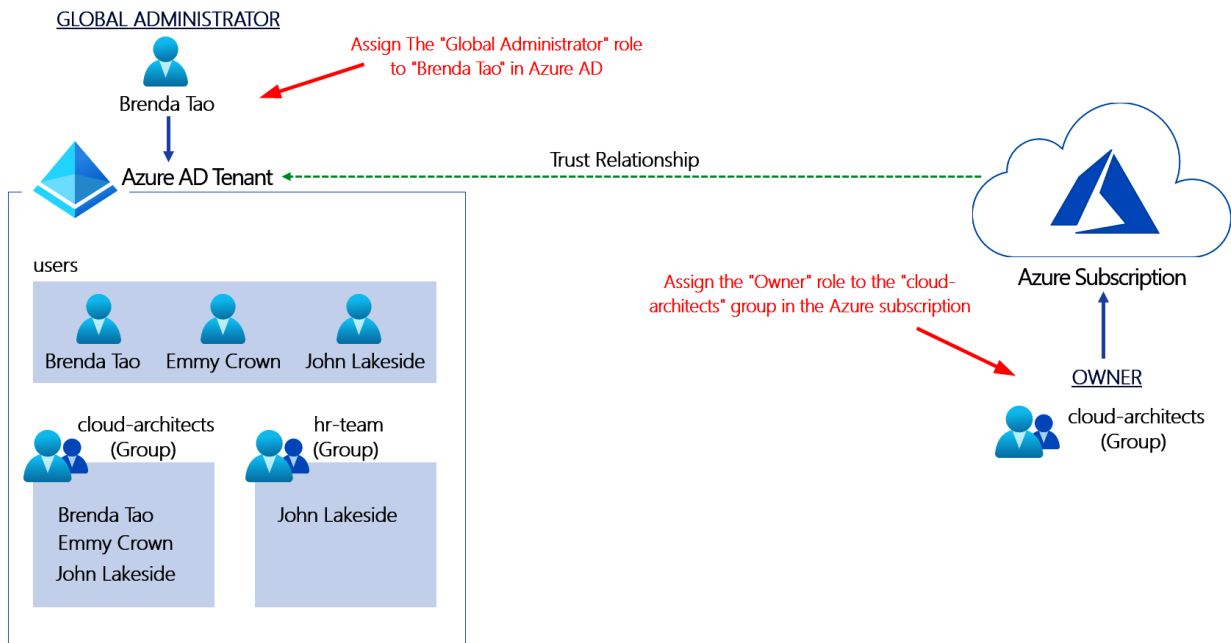
And/Or	Property 1	Operator 2	Value 3	
▼	department	Equals	HR	🗑️

+ Add expression | + Get custom extension properties ⓘ

Rule syntax [Edit](#)

```
(user.department -eq "HR")
```

Name	Object Id	Group Type	Membership Type	Email	Source
<input type="checkbox"/> HR hr-team	b2f74e1f-fcee-4794-965d-eb3a...	Security	Dynamic		Cloud
<input type="checkbox"/> CL cloud-architects	3ed92323-3235-4102-8a6c-260...	Security	Assigned		Cloud



azureblueteam (Default Directory) | Roles and administrators

- Overview
- Getting started
- Preview hub
- Diagnose and solve problems
- Manage**
 - Users
 - Groups
 - External Identities
 - Roles and administrators**
 - Administrative units

[+ New custom role](#)
[Delete custom role](#)
[Refresh](#)
[Preview features](#)
[Got feedback?](#)

Get just-in-time access to a role when you need it using PIM. [Learn more about PIM](#) →

<input type="checkbox"/>	Exchange administrator	Can manage all aspects of the Exchange product.
<input type="checkbox"/>	External ID user flow administrator	Can create and manage all aspects of user flows.
<input type="checkbox"/>	External ID user flow attribute administrator	Can create and manage the attribute schema available to a
<input type="checkbox"/>	External Identity Provider administrator	Can configure identity providers for use in direct federati
<input checked="" type="checkbox"/>	Global administrator	Can manage all aspects of Azure AD and Microsoft service
<input type="checkbox"/>	Global reader	Can read everything that a global administrator can, but n
<input type="checkbox"/>	Groups administrator	Can manage all aspects of groups and group settings like r
<input type="checkbox"/>	Guest inviter	Can invite guest users independent of the 'members can in
<input type="checkbox"/>	Helpdesk administrator	Can reset passwords for non-administrators and Helpdesk

Home > azureblueteam (Default Directory) > Global administrator

Global administrator | Assignments

[Diagnose and solve problems](#)

[+ Add assignments](#)
[Remove assignments](#)
[Download](#)

You can also assign built-in roles to groups now. [Learn More](#)

Name	UserName
<input type="checkbox"/> David Okeyode	david-packt-

Add assignments

Only groups eligible for role assignment are displayed. [Learn more](#)

Search

BT Brenda Tao
brenda@azureblueteam.io
Selected 2

DO David Okeyode
david-packt-az500@outlook.com

Selected items

BT Brenda Tao
brenda@azureblueteam.io [Remove](#)

[Add](#) 3

Name	UserName	Type	Scope
<input type="checkbox"/> Brenda Tao	brenda@azureblueteam.io	User	Directory
<input type="checkbox"/> David Okeyode	david-packt-az500@outlook.com	User	Directory

Azure services

Icons for Azure services: Create a resource, Azure Active Directory, Subscriptions (highlighted with a red arrow), Virtual machines, App Services, Storage accounts.

Navigate

Navigate icons: Subscriptions (highlighted with a red arrow), Resource groups, All resources.

Subscriptions

azureblueteam (Default Directory)

+ Add

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which Showing subscriptions in azureblueteam (Default Directory) directory. Don't see a subscription? [Switch directories](#)

My role Status
8 selected 3 selected

Apply

Showing 1 of 1 subscriptions Show only subscriptions selected in the [global subscriptions filter](#)

Search

Subscription name	Subscription ID	My role
Free Trial	5d58	Account admin

Search (Ctrl+/)

+ Add | Download role assignments | Edit columns | Refresh | Remove | Got feedback?

- Overview
- Activity log
- Access control (IAM)**
- Tags
- Diagnose and solve problems
- Security
- Events
- Cost Management
 - Cost analysis
 - Cost alerts
 - Budgets

Check access | Role assignments | Roles | Deny assignments | Classic administrators

My access
View my level of access to this resource.
[View my access](#)

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find

Grant access to this resource

Grant access to resources by assigning a role.

Click to add a role assignment to the subscription

[Add role assignments](#) [Learn more](#)

View access to this resource

View the role assignments that grant access to this and other resources.

Add role assignment



Role ⓘ

1

Owner ⓘ

Assign access to ⓘ

User, group, or service principal

Select ⓘ

Search by name or email address



Brenda Tao
brenda@azureblueteam.io



David Okeyode
david-packt-az500_outlook.com#EXT#@davidpa...



Emmy Crown
emmy@azureblueteam.io

Selected members:



cloud-architects

2

Remove

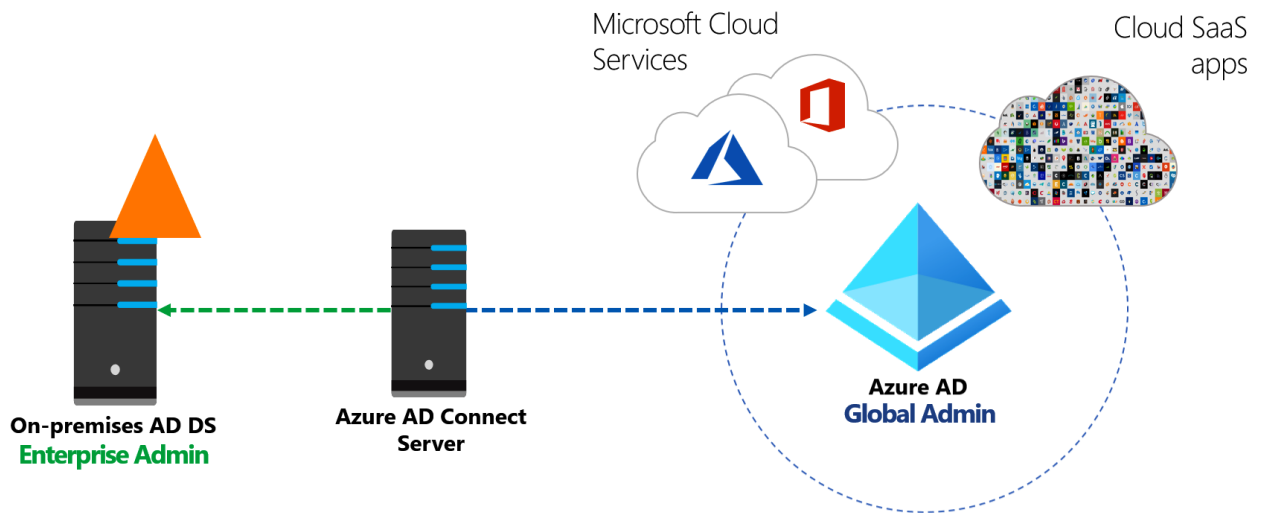
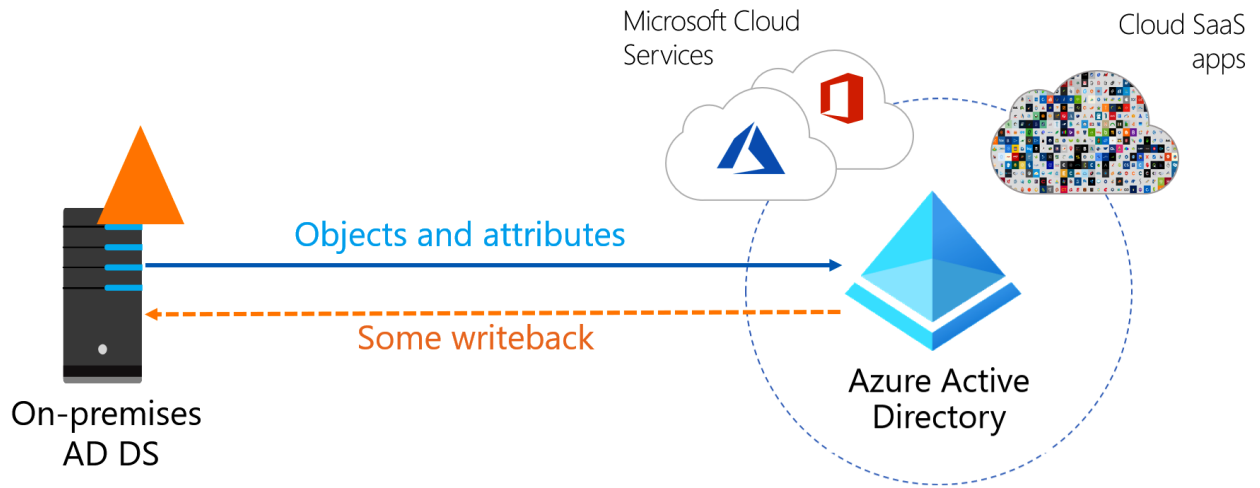
3

Save

Discard

Name	Type	Membership
London-Group	Security	Dynamic user membership type that contains all London users
Chicago-Group	Security	Dynamic user membership type that contains all Chicago users

Chapter 3: Azure AD Hybrid Identity



Create a new Windows VM and create a new AD Forest, Domain and DC

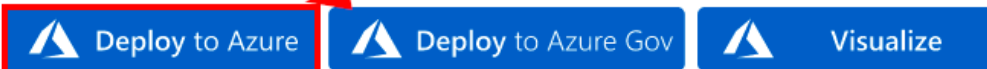
Azure Public Test Date 2020.12.10 Azure Public Test Result **pass**

Azure US Gov Test Date 2020.12.09 Azure US Gov Test Result **pass**

Best Practice Check **fail** CredScan Check Not Tested

This template will deploy a new VM (along with a new VNet and Load Balancer) and will configure it as a Domain Controller and create a new forest and domain.

Click the button below to deploy



Sign in

to continue to Microsoft Azure

david-packt-az500@outlook.com

No account? [Create one!](#)

[Can't access your account?](#)

[Sign in with Windows Hello or a security key](#) 

Next

Create an Azure VM with a new AD Forest



Azure quickstart template

Deployment scope

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

Subscription * ⓘ	<input type="text" value="AzureBlueTeam-PROD"/>
Resource group * ⓘ	<input type="text" value="(New) onpremises-rg"/>

[Create new](#)

Parameters

Region * ⓘ	<input type="text" value="UK South"/>
Admin Username * ⓘ	<input type="text" value="onpremadmin"/>
Admin Password * ⓘ	<input type="password" value="••••••••"/>
Domain Name * ⓘ	<input type="text" value="az500lab.com"/>
Dns Prefix * ⓘ	<input type="text" value="az500lab-27120"/>
Vm Size ⓘ	<input type="text" value="Standard_D2s_v3"/>
_artifacts Location ⓘ	<input type="text" value="[deployment().properties.templateLink.uri]"/>


Review + create

< Previous

Next : Review + create >

Create an Azure VM with a new AD Forest

Azure quickstart template

✓ Validation Passed 

Admin Password	*****
Domain Name	az500lab.com
Dns Prefix	az500lab-27120
Vm Size	Standard_D2s_v3
_artifacts Location	[deployment().properties.templateLink.uri]
_artifacts Location Sas Token	-
Location	[resourceGroup().location]
Virtual Machine Name	adVM
Virtual Network Name	adVNET
Virtual Network Address Range	10.0.0.0/16
Load Balancer Front End IP Name	LBFE


Create

< Previous


Next

[Download a template for automation](#)

 Delete  Cancel  Redeploy  Refresh

 We'd love your feedback! →

✓ Your deployment is complete

 Deployment name: Microsoft.Template-20201227014328
Subscription: [AzureBlueTeam-PROD](#)
Resource group: [onpremises-rg](#)

Start time: 12/27/2020, 1:43:29 AM
Correlation ID: cc01b6b3-b7af-4ed1-a0f2-06573e353488









∨ Deployment details ([Download](#))

∧ Next steps

Go to resource group

Filter by name... Type == all X Location == all X + Add filter

Showing 1 to 8 of 8 records. Show hidden types ⓘ

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/>  adAvailabilitySet	Availability set	UK South
<input type="checkbox"/>  adLoadBalancer	Load balancer	UK South
<input type="checkbox"/>  adNic	Network interface	UK South
<input type="checkbox"/>  adPublicIP	Public IP address	UK South
<input type="checkbox"/>  adVM	Virtual machine	UK South
<input type="checkbox"/>  adVM_DataDisk	Disk	UK South
<input type="checkbox"/>  adVM_OSDisk	Disk	UK South
<input type="checkbox"/>  adVNET	Virtual network	UK South

adVM Virtual machine

Search (Ctrl+/) << Connect Start Restart Stop Capture Delete Refresh Open in mobile

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks

Essentials

Resource group [\(change\)](#) onpremises-rg

Status Running

Location UK South

Subscription [\(change\)](#) AzureBlueTeam-PROD

Subscription ID 18b55860-f311-4e0b-b4ab-bf283288b6aa

Tags [\(change\)](#) [Click here to add tags](#)

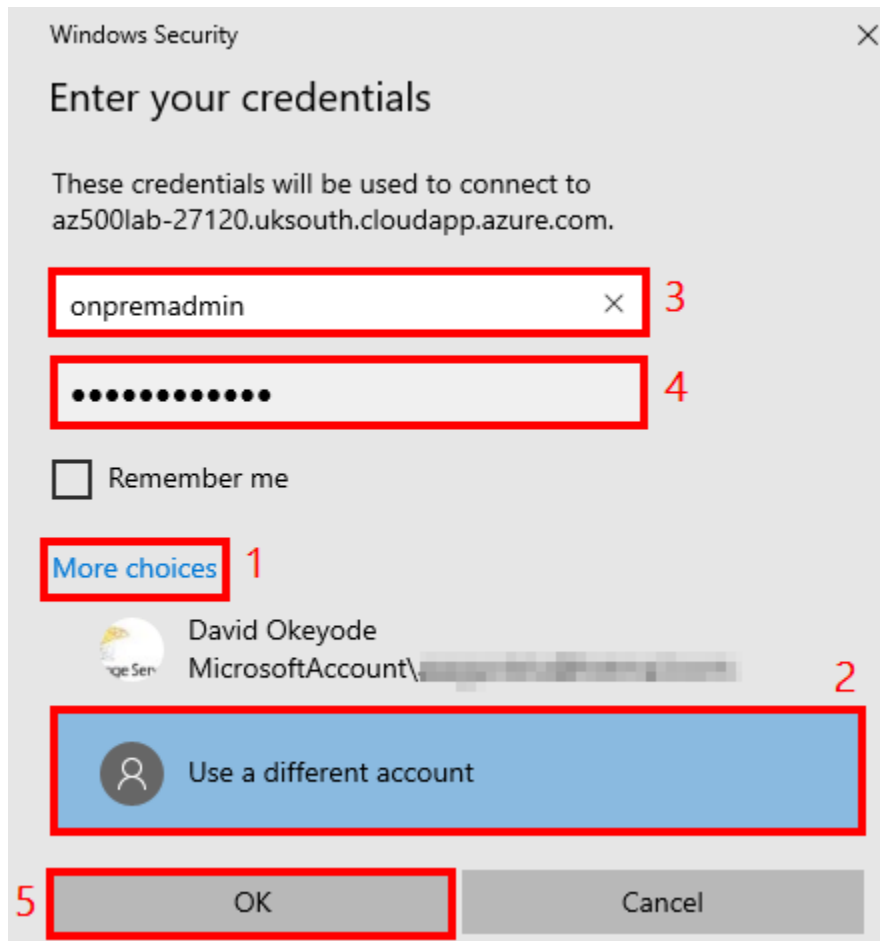
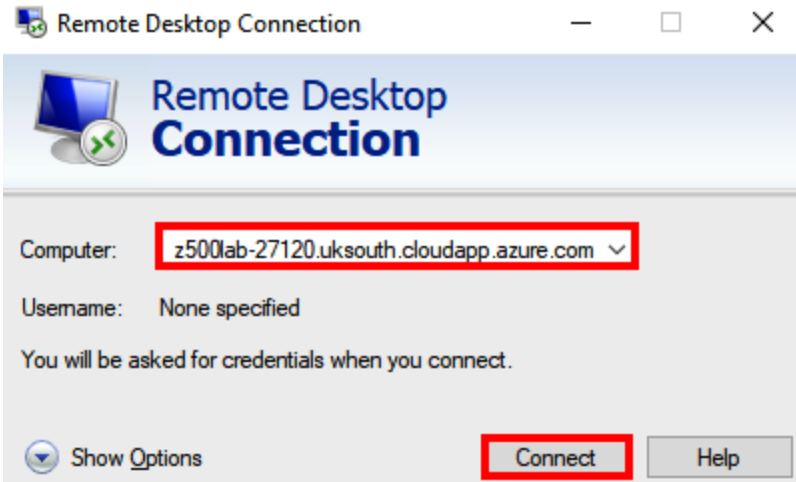
Operating system Windows (Windows Server 2016 Datacenter)

Size Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address 51.140.40.74

Virtual network/subnet adVNET/adSubnet

DNS name **az500lab-27120.uksouth.cloudapp.azure.com**



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
adVM.az500lab.com

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

! The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

Don't ask me again for connections to this computer

View certificate... Yes No

Server Manager Dashboard

WELCOME TO SERVER MANAGER

1 Configure this local server

QUICK START

- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

WHAT'S NEW

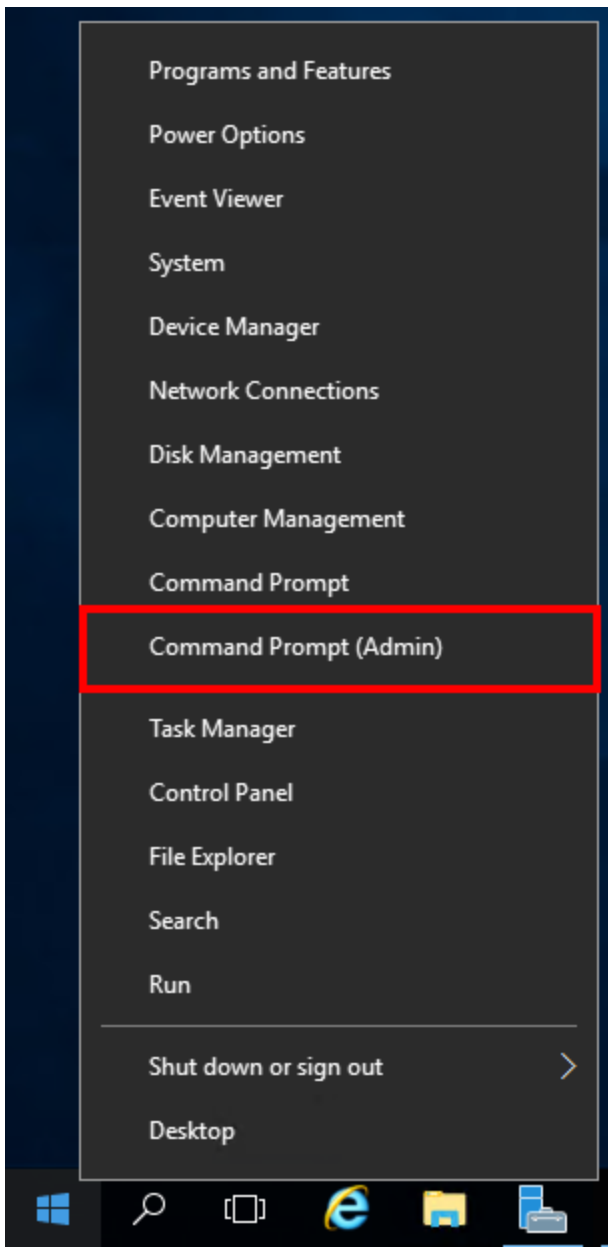
LEARN MORE

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

AD DS	DNS	File and Storage Services	Local Server	All Servers
1	1	1	1	1
Manageability	Manageability	Manageability	Manageability	Manageability
Events	Events	Events	Events	Events
Services	Services	Services	2 Services	2 Services
Performance	Performance	Performance	Performance	Performance
BPA results	BPA results	BPA results	BPA results	BPA results
			12/27/2020 2:29 PM	12/27/2020 2:29 PM

Windows taskbar: 2:29 PM, 12/27/2020



Administrator: Command Prompt - powershell

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32> powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\windows\system32> █
```

```
PS C:\windows\system32> New-Item -Path "c:\\" -Name "packtaz500" -ItemType "directory"

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          12/27/2020   4:08 PM         packtaz500

PS C:\windows\system32> Set-Location -Path "c:\packtaz500"
PS C:\packtaz500> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/davidokoyode/azure-offensive/master/packtaz500testusers.ps1" -OutFile "packtaz500testusers.ps1"
PS C:\packtaz500> .\packtaz500testusers.ps1
Input Password: *****
PS C:\packtaz500> █
```

Enter a password for the test users when prompted

```
PS C:\packtaz500>
PS C:\packtaz500> dsa.msc
PS C:\packtaz500>
```

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [adVM.az500lab.com]

- Saved Queries
- az500lab.com 1
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Keys
 - LostAndFound
 - Managed Service Accounts
 - OrgUsers 2
 - Finance 2
 - IT
 - Program Data

Name	Type
Davy Flury	User
FinanceUsers	Security Group - Global
Jack Robinson	User
Kerri Ondrich	User
LanieCominotti	User
Octavius Mohun	User

Search resources, services, and docs (G+)

- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Azure Active Directory
- Resource groups

Azure Active Directory

Virtual machines

Azure Cosmos DB

More services

- Overview
- Getting started
- Preview hub
- Diagnose and solve problems
- Manage**
- Users**
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices

- All users (Preview)
- Deleted users (Preview)
- Password reset
- User settings
- Diagnose and solve problems
- Activity
- Sign-ins
- Audit logs
- Bulk operation results
- Troubleshooting + Support
- New support request

+ New user + New guest user Bulk operations

This page includes previews available for your evaluation. View


Search users Add filters

4 users found

	Name	User principal n...	User type
<input type="checkbox"/>	Brenda Tao	brenda@azurebluete...	Member
<input type="checkbox"/>	David Okeyode	david-packt-az500_o...	Member
<input type="checkbox"/>	Emmy Crown	emmy@azurebluete...	Member
<input type="checkbox"/>	John Lakeside	john@azurebluetea...	Member

New user

azureblueteam (Default Directory)

 Got feedback?

User name * ⓘ

syncadmin ✓

@ azureblueteam.io ▾



The domain name I need isn't shown here

Name * ⓘ

syncadmin ✓

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password * ⓘ

●●●●●●●●●● ✓

Groups and roles

Groups

0 groups selected

Roles

Global administrator

Create





syncadmin@azureblueteam.io

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Sign in

Application Install - Security Warning



Do you want to install this application?



Name:

[IdFix](#)

From (Hover over the string below to see the full domain):

raw.githubusercontent.com

Publisher:

[Microsoft Corporation](#)

Install

Don't Install



While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not install this software. [More Information...](#)

Open File - Security Warning



Do you want to run this file?



Name: ...ae1245bd53d87 0002.0003 1a851a1c9a84870e\ldFix.exe

Publisher: Microsoft Corporation

Type: Application

From: C:\Users\onpremadmin\AppData\Local\Apps\2.0\ZW...

Run

Cancel

Always ask before opening this file



While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust.

[What's the risk?](#)

ldFix Privacy Statement



This privacy statement applies to ldFix only. It does not apply to any other Microsoft Office 365 server or other applications by Microsoft Corporation. ldFix is intended for IT Administrators. If you are an end-user, Microsoft recommends that you end this program and contact your IT Administrator for assistance. ldFix collects data from your corporate network and can optionally store data that may contain personal data in a Comma Separated Value (.csv) or LDAP Data Interchange Format (.ldf) file located on the computer where the program was run. Microsoft recommends that you remove this file when you have completed your use of the program. ldFix does not send any collected data back to Microsoft or it's partners.

OK

ldFix version 2.3.0.0

Office 365

Query

Cancel

Accept

Apply

Export

Import

Undo

DISTINGUISHEDNAME	OBJECTCLASS	ATTRIBUTE	ERROR	VALUE	UPDATE	ACTION
CN=DefaultAccount,CN=Users,DC=az500lab,DC=com	user	displayName	Blank		DefaultAccount	
CN=Keri Ondrich,OU=Finance,OU=OrgUsers,DC=az500lab,DC=com	user	userPrincipalName	Character	kem%:@az500lab.com	kem@az500lab.com	EDIT
CN=onpremadmin,CN=Users,DC=az500lab,DC=com	user	displayName	Blank		onpremadmin	

1

3

2

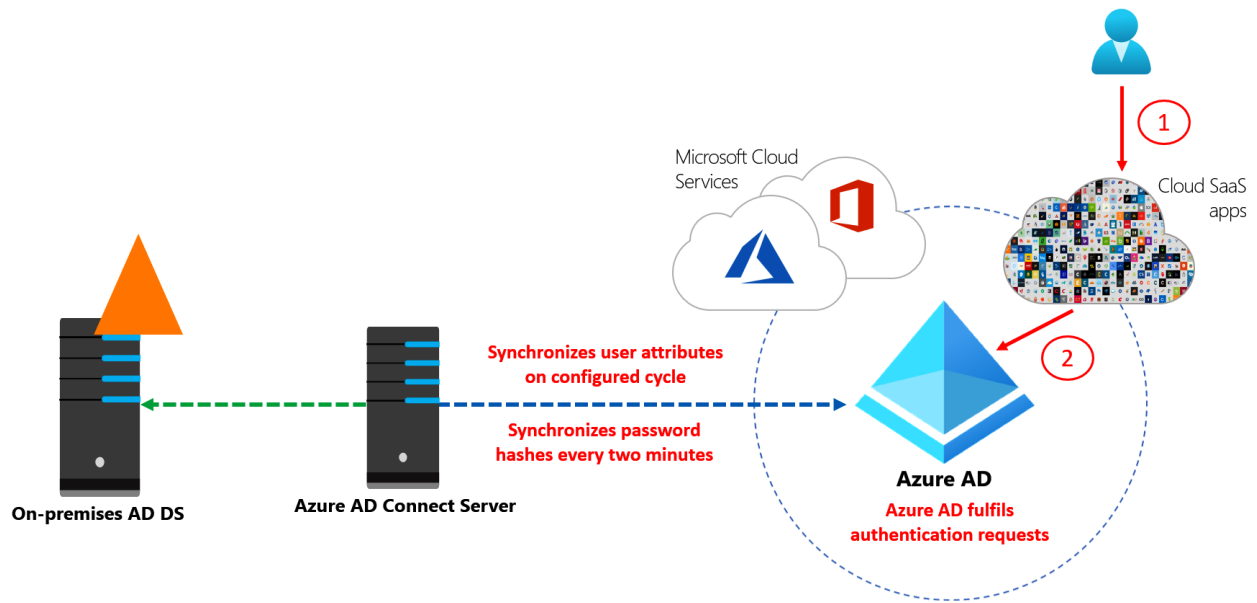
Apply Pending

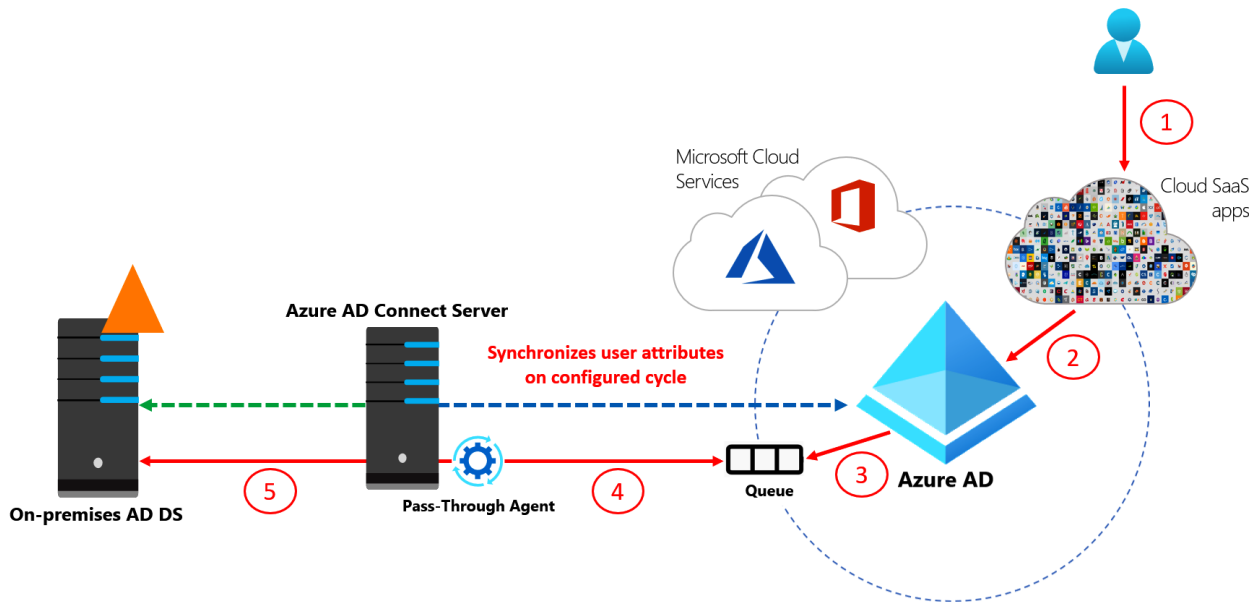
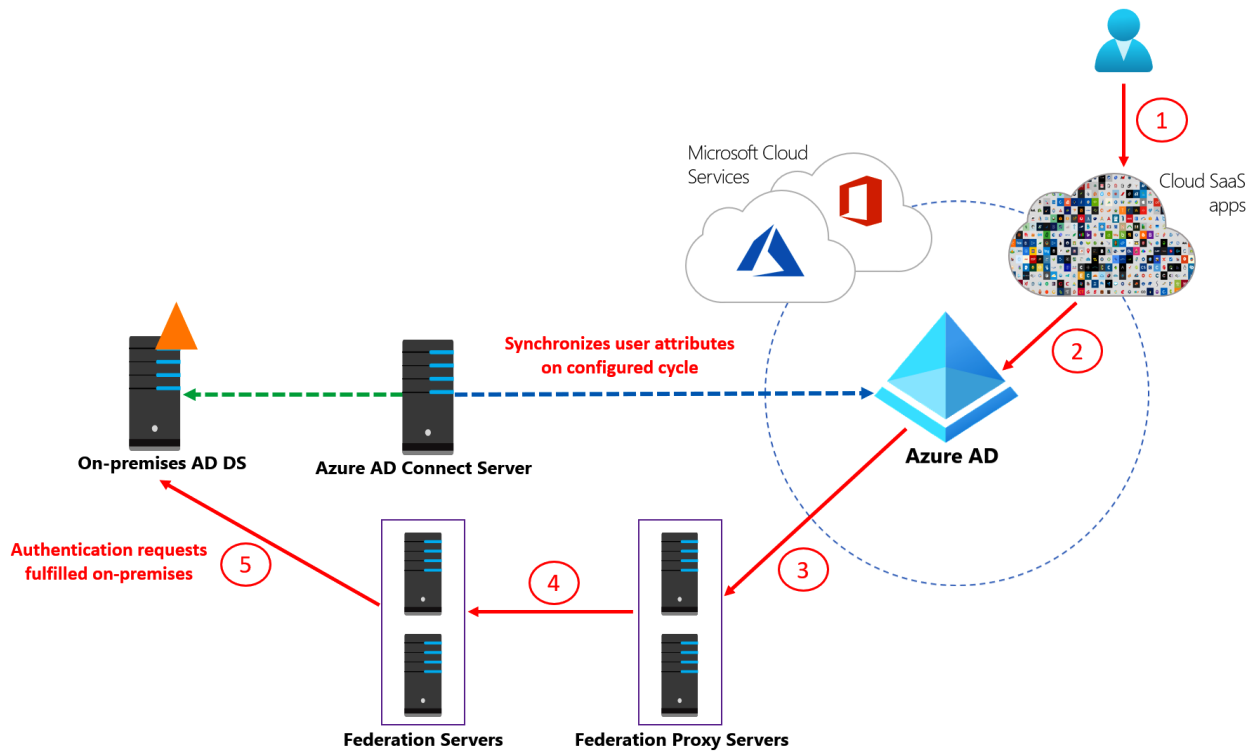


Are you sure you wish to Apply the update values for all transactions with an action? NOTE: The user assumes all risk for inspecting each row marked with Action for suitability and accuracy.

Yes

No





Welcome

Express Settings

Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of AZ500LAB
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

[Learn more about express settings](#)

Select Customize to choose advanced deployment options or import settings from an existing server.

Custom Settings
Option

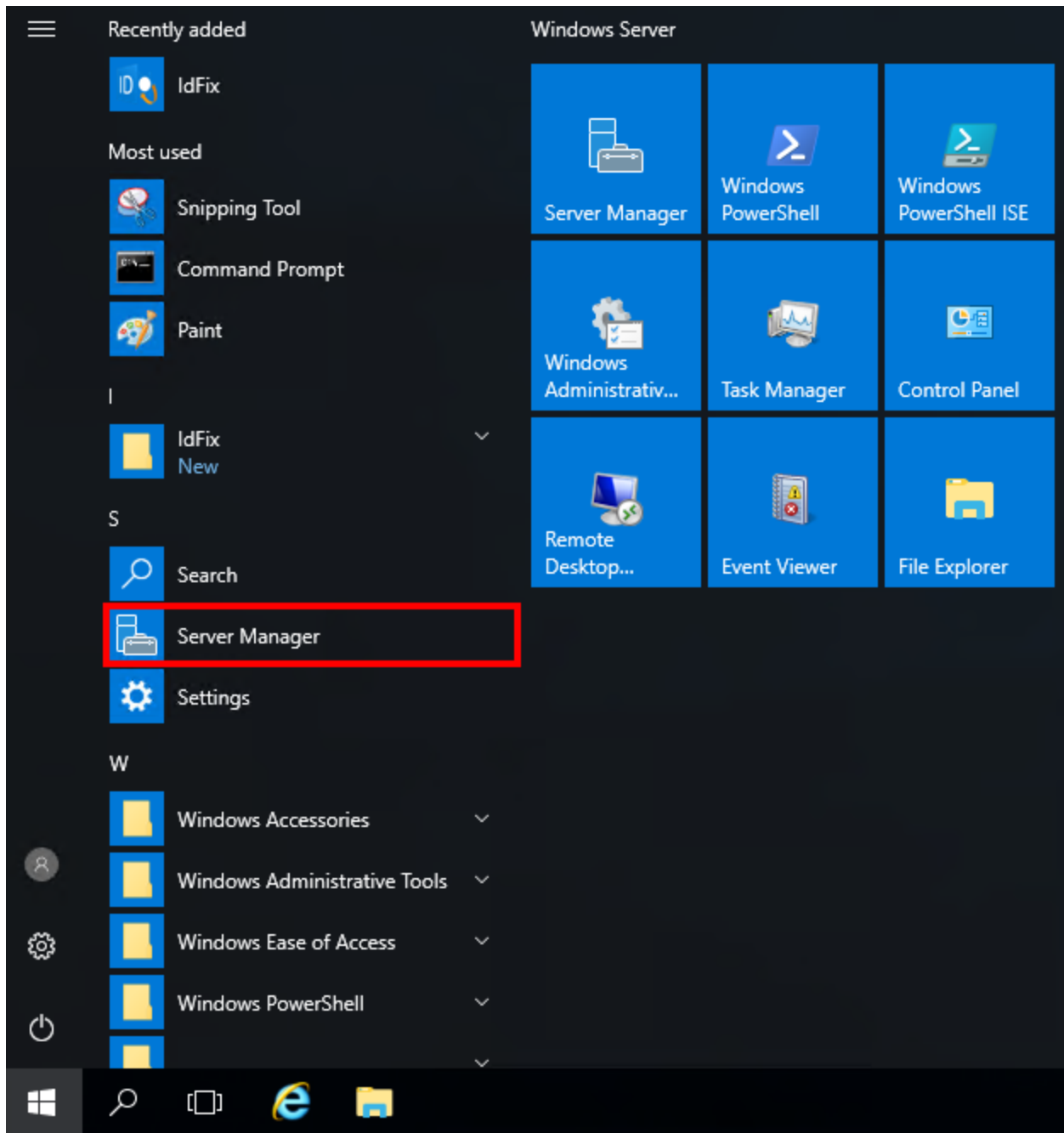


Customize

Express Settings
Option



Use express settings



Server Manager

Server Manager ▶ Local Server

Dashboard

Local Server

All Servers

AD DS

DNS

File and Storage Services ▶

PROPERTIES
For adVM

TASKS ▼

Computer name	adVM	Last installed updates	Yesterday at 2:29 PM
Domain	az500lab.com	Windows Update	Install updates automatically using Windows Update
		Last checked for updates	Yesterday at 2:27 PM
Windows Firewall	Domain: On	Windows Defender	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Universal Time
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00376-40000-00000-AA947 (activated)
Operating system version	Microsoft Windows Server 2016 Datacenter	Processors	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	8 GB
		Total disk space	162.38 GB

Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

On (Recommended)

Off 1

Users:

On (Recommended)


Off 2

[More about Internet Explorer Enhanced Security Configuration](#)


3



Microsoft Azure Active Directory Connect


Important! Selecting a language below will dynamically change the complete page content to that language.



Language: **English** 

Download

Do you want to run or save **AzureADConnect.msi** (96.5 MB) from **download.microsoft.com**? 

 This type of file could harm your computer. 

Run Save  Cancel

 Microsoft Azure Active Directory Connect 

Welcome
Express Settings

Welcome to Azure AD Connect


Run this installation tool on the server where the synchronization service component will be installed.


Azure Active Directory Connect integrates your on-premises and online directories.

This installation tool will:

- Guide you in selecting a solution (for example, password hash synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Enable application telemetry and component health data by default. You can change what data is shared with Microsoft by updating your [privacy settings](#).

[Learn more about hybrid identity](#)

 I agree to the [license terms](#) and [privacy notice](#).



Continue

Microsoft Azure Active Directory Connect

Welcome
Express Settings


Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of AZ500LAB
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

[Learn more about express settings](#)

Select Customize to choose advanced deployment options or import settings from an existing server.

 **Customize** Use express settings

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In

Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. [?](#)

- Specify a custom installation location
- Use an existing SQL Server
- Use an existing service account
- Specify custom sync groups
- Import synchronization settings (Preview) [Learn more](#)

Previous **Install**

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure

User sign-in

Select the Sign On method. ?

- Password Hash Synchronization ?
- Pass-through authentication ?
- Federation with AD FS ?
- Federation with PingFederate ?
- Do not configure ?

Select this option to enable single sign-on for your corporate desktop users:

Enable single sign-on ?

Previous Next

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure

Connect to Azure AD

Enter your Azure AD global administrator credentials. ?

USERNAME
syncadmin@azureblueteam.io 1

PASSWORD
..... 2

3

Previous Next

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features

Connect your directories

Enter connection information for your on-premises directories or forests. ?

DIRECTORY TYPE
Active Directory

FOREST ?
az500lab.com

Add Directory

No directories are currently configured.

AD forest account

AD forest account

An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. [Learn more](#) about managing account permissions.

The first option is recommended and requires you to enter Enterprise Admin credentials.

Select account option.

Create new AD account **1**

Use existing AD account

ENTERPRISE ADMIN USERNAME
AZ500LAB\onpremadmin **2**

PASSWORD
..... **3**

OK **4** Cancel

Microsoft Azure Active Directory Connect

Welcome

- Express Settings
- Required Components
- User Sign-In
- Connect to Azure AD
- Sync
- Connect Directories**
- Azure AD sign-in
- Domain/OU Filtering
- Identifying users
- Filtering
- Optional Features
- Configure

Connect your directories

Enter connection information for your on-premises directories or forests. ?

DIRECTORY TYPE
Active Directory

FOREST ?
 Add Directory

CONFIGURED DIRECTORIES

az500lab.com (Active Directory) ✓	Remove
-----------------------------------	--------

Previous Next

Microsoft Azure Active Directory Connect

Welcome

- Express Settings
- Required Components
- User Sign-In
- Connect to Azure AD
- Sync
- Connect Directories
- Azure AD sign-in**
- Domain/OU Filtering
- Identifying users
- Filtering
- Optional Features
- Configure

Azure AD sign-in configuration

To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain. ?

Active Directory UPN Suffix	Azure AD Domain
az500lab.com	Not Added ?

Select the on-premises attribute to use as the Azure AD username

USER PRINCIPAL NAME ?
userPrincipalName

Continue without matching all UPN suffixes to verified domains

Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. [Learn more](#)

Previous Next

- Welcome
- Express Settings
- Required Components
- User Sign-In
- Connect to Azure AD
- Sync
 - Connect Directories
 - Azure AD sign-in
 - Domain/OU Filtering**
 - Identifying users
 - Filtering
 - Optional Features
- Configure

Domain and OU filtering

Directory: az500lab.com

Refresh Domains ?

- Sync all domains and OUs
- Sync selected domains and OUs

- az500lab.com
 - BuiltIn
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Infrastructure
 - LostAndFound
 - Managed Service Accounts
 - OrgUsers
 - Finance
 - IT
 - Program Data
 - System
 - Users

Previous

Next

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure

Optional features

Select enhanced functionality if required by your organization.

- Exchange hybrid deployment ?
- Exchange Mail Public Folders ?
- Azure AD app and attribute filtering ?
- Password hash synchronization ?
- Password writeback ?
- Group writeback ?
- Device writeback ?
- Directory extension attribute sync ?

[Learn more](#) about optional features.

Previous **Next**

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure

Ready to configure

Once you click Install, we will do the following:

- Configure synchronization services on this computer
- Configure Source Anchor Attribute
- Configure davidpacktaz500outlook.onmicrosoft.com - AAD Connector
- Configure az500lab.com Connector
- Enable Password hash synchronization
- Enable Password writeback
- Enable Azure AD Export Deletion Threshold (500)

- Start the synchronization process when configuration completes.
- Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

Previous **Install**

- Welcome
- Express Settings
- Required Components
- User Sign-In
- Connect to Azure AD
- Sync
 - Connect Directories
 - Azure AD sign-in
 - Domain/OU Filtering
 - Identifying users
 - Filtering
 - Optional Features
- Configure

Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. [Learn more](#)

The Active Directory Recycle Bin is not enabled for your forest (az500lab.com) and is strongly recommended. [Learn more](#)

Azure Active Directory is configured to use AD attribute `mS-DS-ConsistencyGuid` as the source anchor attribute. [Learn more](#)

Previous

Exit

Home > azureblueteam (Default Directory) >

azurebluetea... x
Azure Active Directory

Users | All users (Preview)

azureblueteam (Default Directory) - Azure Active Directory

- Overview
- Getting started
- Preview hub
- Diagnose and solve problems
- Manage
 - Users
 - Groups
 - External Identities
 - Roles and administrators
 - Administrative units
 - Enterprise applications
 - Devices
 - App registrations
 - Identity Governance
 - Application proxy
 - Licenses
 - Azure AD Connect
 - Custom domain names
 - Mobility (MDM and MAM)
 - Password reset
 - Company branding

+ New user + New guest user Bulk operations Refresh Reset password Multi-Factor Authentication Delete user

This page includes previews available for your evaluation. View previews →

Search users Add filters

16 users found

	Name	User principal name	User type	Directory synced
<input type="checkbox"/>	BT Brenda Tao	brenda@azureblueteam.io	Member	No
<input type="checkbox"/>	DO David Okeyode	david-packt-az500_outlook.com#EX...	Member	No
<input type="checkbox"/>	DF Davy Flury	davy@davidpacktaz500outlook.on...	Member	Yes
<input type="checkbox"/>	EC Emmy Crown	emmy@azureblueteam.io	Member	No
<input type="checkbox"/>	JR Jack Robinson	jack@davidpacktaz500outlook.onmi...	Member	Yes
<input type="checkbox"/>	JP Jefferson Pinchen	jefferson@davidpacktaz500outlook...	Member	Yes
<input type="checkbox"/>	JL John Lakeside	john@azureblueteam.io	Member	No
<input type="checkbox"/>	JL Jonah Lerohan	jonah@davidpacktaz500outlook.on...	Member	Yes
<input type="checkbox"/>	KA Kendrick Axtonne	kendrick@davidpacktaz500outlook...	Member	Yes
<input type="checkbox"/>	KO Kerri Ondrich	kerri@davidpacktaz500outlook.onm...	Member	Yes
<input type="checkbox"/>	KM Kofi Mensah	kofi@davidpacktaz500outlook.onmi...	Member	Yes
<input type="checkbox"/>	LC Lanie Cominotti	lanie@davidpacktaz500outlook.on...	Member	Yes
<input type="checkbox"/>	NO Nat Ortner	nat@davidpacktaz500outlook.onmi...	Member	Yes
<input type="checkbox"/>	OM Octavius Mohun	octavius@davidpacktaz500outlook...	Member	Yes
<input type="checkbox"/>	OD On-Premises Directory Synch...	Sync_adVM_1b0f3fa993f2@davidpa...	Member	Yes
<input type="checkbox"/>	SY syncadmin	syncadmin@azureblueteam.io	Member	No

Password reset | Authentication methods

Test Cloud - Azure Active Directory



Save



Discard

Diagnose and solve problems

Manage

Properties

1

Authentication methods

Registration

Notifications

Customization

On-premises integration

Administrator Policy

Activity

Audit logs

Number of methods required to reset ⓘ

1

2

Methods available to users

Mobile app notification

2

Mobile app code

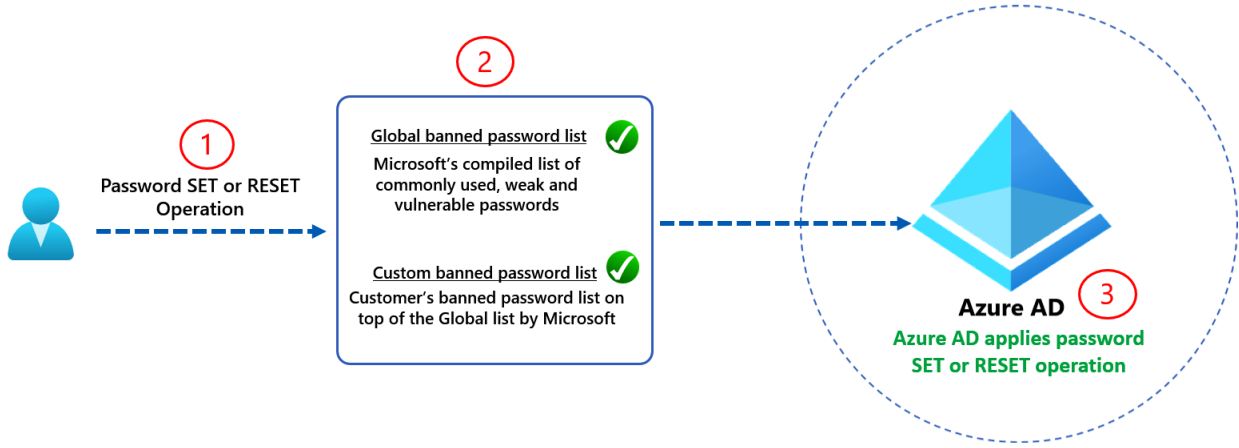
Email

Mobile phone (SMS only)

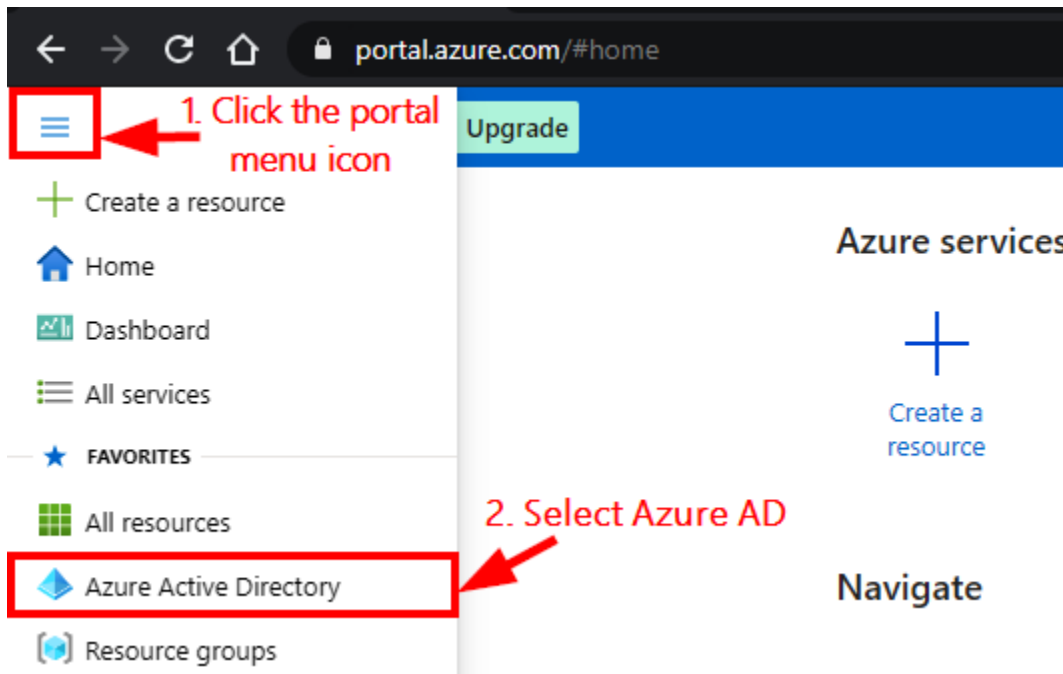
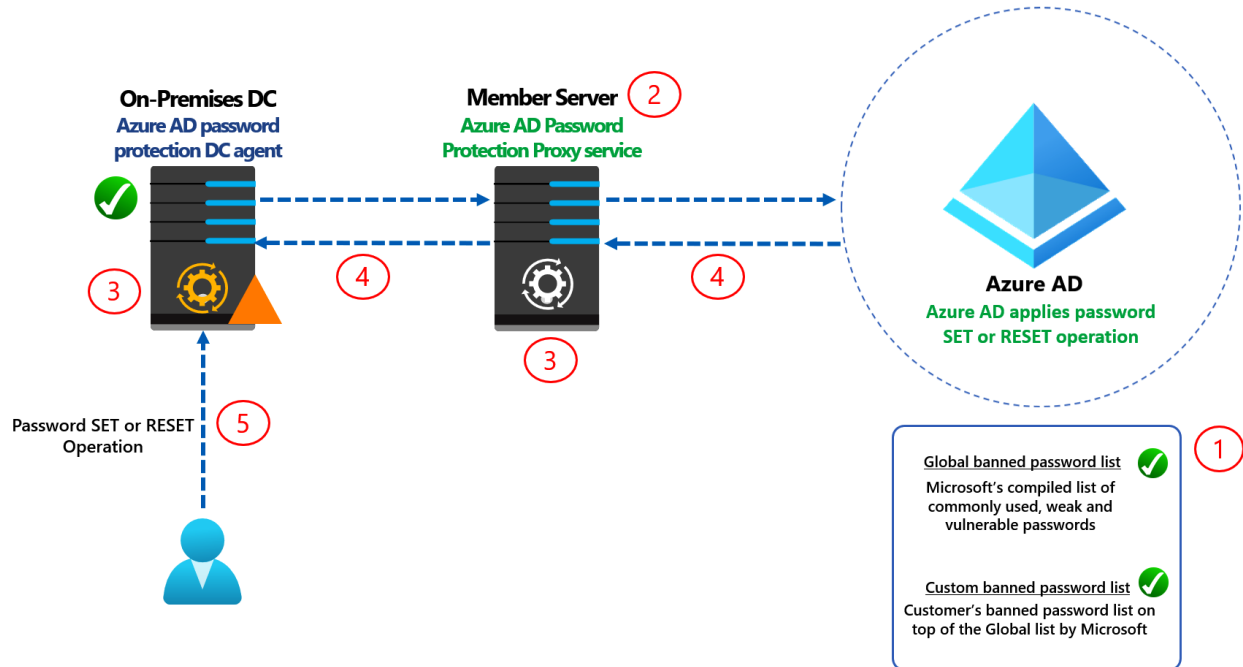
Office phone ⓘ

Security questions

Chapter 4: Azure AD Identity Security



	Azure AD Free	Azure AD Office 365	Azure AD Premium P1	Azure AD Premium P2
Global banned password	✓	✓	✓	✓
Custom banned password			✓	✓
Active Directory Domain Services (AD DS) Integration			✓	✓



azurebluetea... ×

Azure Active Directory

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses** 1
- Azure AD Connect

Licenses | Licensed fe

azureblueteam (Default Directory) - Azure

- Overview
- Diagnose and solve problems
- Manage** 2
 - Licensed features**
 - All products
 - Self-service sign up products
- Activity
 - Audit logs
- Troubleshooting + Support
 - New support request

Filter by category

Features	Description	Feature available
Password Protection (global banned password)	Learn more	Yes
Password Protection (custom banned password)	Learn more	Yes
Password Protection for Windows Server Active Directory (global and custom banned password)	Learn more	Yes

azurebluetea...

Azure Active Directory

- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security**

Monitoring

Security | ...

Search (Ctrl+)

Getting started

Protect

- Conditional Access
- Identity Protection
- Security Center
- Continuous access evaluation ...

Manage

- Identity Secure Score
- Named locations
- Authentication methods**

MFA

Report

Risky users

Authentication meth

azureblueteam (Default Directory) - Azure

Search (Ctrl+)

Manage

- Policies
- Password protection**

Custom smart lockout

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

Custom banned passwords

Enforce custom list ⓘ Yes No ¹

Custom banned password list ⓘ ✓ ²

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No ³

Mode ⓘ Enforced Audit

- ⚙ User settings ¹
- 👤 Properties**
- 🛡 Security
- Monitoring**
- 🔄 Sign-ins
- 📄 Audit logs
- 👤 Provisioning logs (Preview)
- 📊 Logs
- 📄 Diagnostic settings
- 💡 Workbooks
- 📊 Usage & insights

Technical contact

Global privacy contact

Privacy statement URL

Access management for Azure resources

David Okeyode (david-packt-az500@outlook.com) can manage access groups in this tenant. [Learn more](#)

Yes No

[Manage Security defaults](#) ²

Enable Security defaults



Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.

[Learn more](#)

Enable Security defaults

Yes No 1

We'd love to understand why you're disabling Security defaults so we can make improvements.

- My organization is using Conditional Access
- My organization is unable to use critical business applications
- My organization is getting too many MFA challenges

2

Other

3

Testing ✓

Save 4



Sign in

to continue to Microsoft Azure

brenda@azureblueteam.io

1

No account? [Create one!](#)

[Can't access your account?](#)

[Sign in with Windows Hello or a security key](#) [?](#)

2

Next



brenda@azureblueteam.io

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

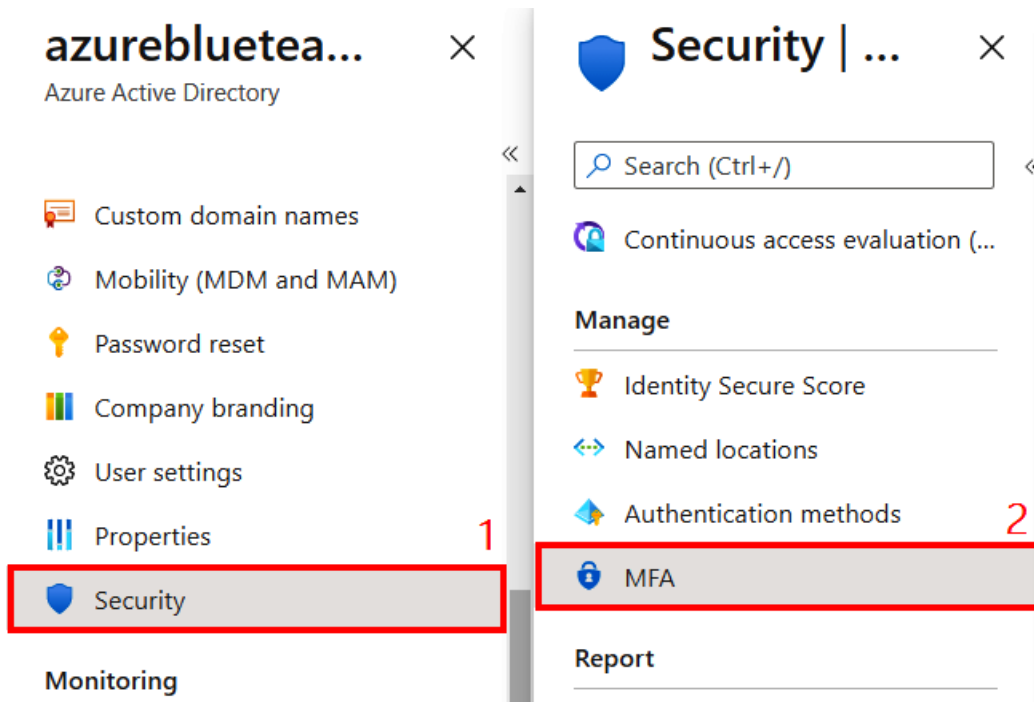
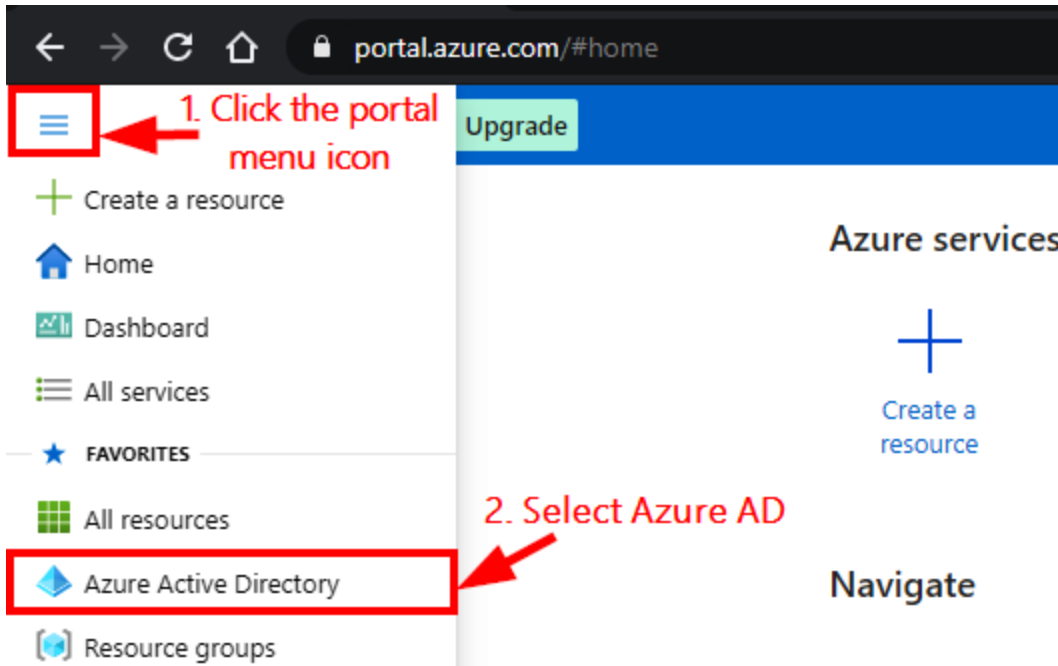
●●●●●●●●

Unfortunately, your password contains a word, phrase or pattern that is banned by your organisation. Please try again with a different password. [View details](#)

●●●●●●●●

●●●●●●●●

Sign in



Multi-Factor Authentication | Getting started

<<

- Getting started
- Diagnose and solve problems

Settings

- Account lockout
- Block/unblock users
- Fraud alert
- Notifications
- OATH tokens
- Phone call settings
- Providers

♥ Got feedback?

Azure Multi-Factor Authentication

Use MFA to protect your users and data. There are many ways

Configure

[Additional cloud-based MFA settings](#)

Learn more

[Deploy cloud-based Azure Multi-Factor Authentication](#)

[Configure Azure Multi-Factor Authentication](#)

[What is conditional access in Azure Active Directory?](#)

[Best practices for conditional access in Azure Active Directory](#)

verification options [\(learn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device [\(learn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember M more days. [Learn more about reauthentication prompts.](#)

save

multi-factor authentication

users service settings

1

Before you begin, take a look at the multi-factor auth deployment guide.



Multi-Factor Auth status: Any

bulk update

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input checked="" type="checkbox"/>	Brenda Tao	brenda@azureblueteam.io	Disabled
<input type="checkbox"/>	David Okeyode	david-packt-az500@outlook.com	Disabled
<input type="checkbox"/>	Davy Flury	davy@davidpacktaz500outlook.onmicrosoft.com	Disabled
<input type="checkbox"/>	Emmy Crown	emmy@azureblueteam.io	Disabled
<input type="checkbox"/>	Jack Robinson	jack@davidpacktaz500outlook.onmicrosoft.com	Disabled
<input type="checkbox"/>	Jefferson Pinchen	jefferson@davidpacktaz500outlook.onmicrosoft.com	Disabled
<input type="checkbox"/>	John Lakeside	john@azureblueteam.io	Disabled

Brenda Tao
brenda@azureblueteam.io

quick steps

Enable

Manage user settings



Sign in

to continue to Microsoft Azure

brenda@azureblueteam.io

No account? [Create one!](#)

[Can't access your account?](#)

[Sign in with Windows Hello or a security key](#)

2

Next



brenda@azureblueteam.io

More information required

Your organisation needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

Keep your account secure

Your organisation requires you to set up the following methods of proving who you are.

Method 1 of 2: App



App

2

Phone

Microsoft Authenticator



Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

Once you've installed the Microsoft Authenticator app on your device, choose "Next".

Next

Method 1 of 2: App



App

2

Phone

Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app to your account.

Once you've scanned the QR code, choose "Next".



[Can't scan image?](#)

Back

Next

Method 1 of 2: App



App

2

Phone

Microsoft Authenticator



Notification approved

Back

Next

Method 2 of 2: Phone



App



Phone

Phone

You can prove who you are by texting a code to your phone.

What phone number would you like to use?

Text me a code

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next

Method 2 of 2: Phone



App



Phone

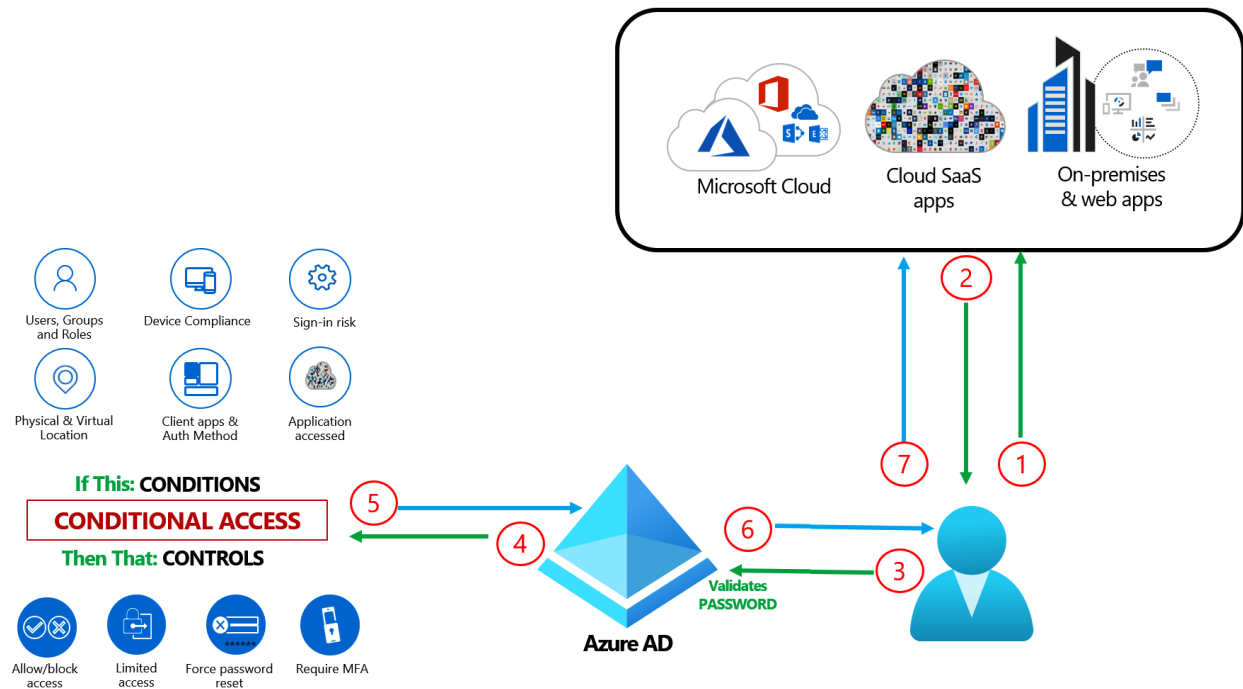
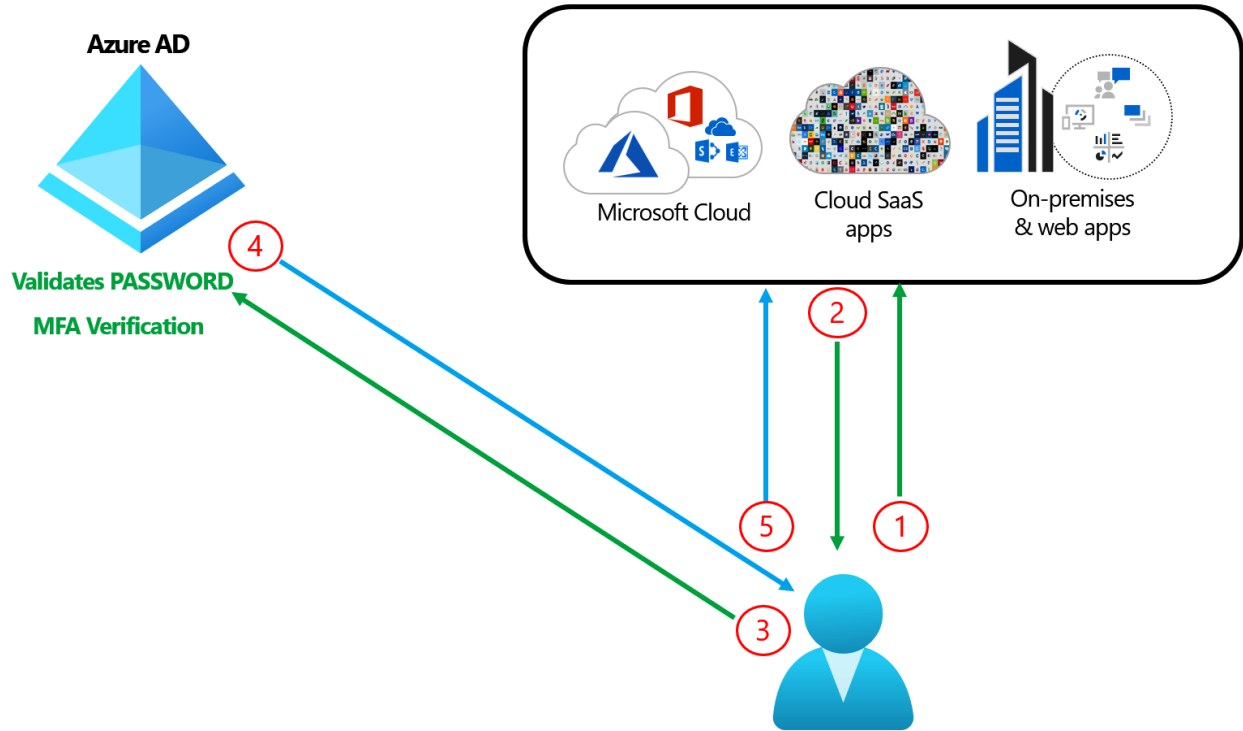
Phone

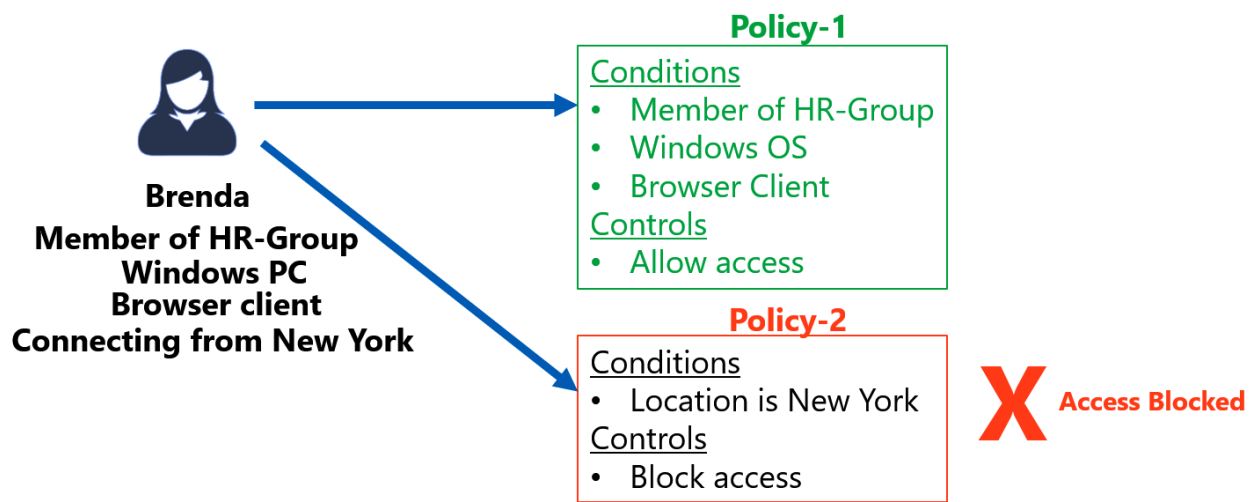
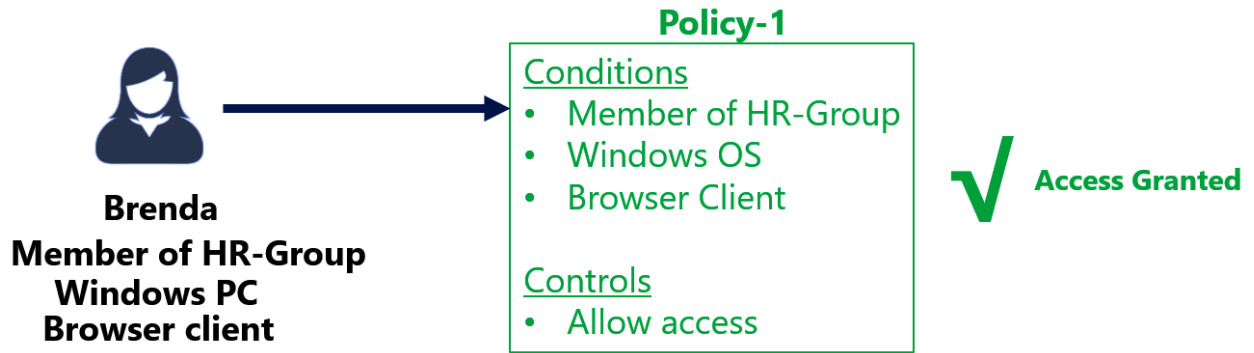
We just sent a 6-digit code to +44 [REDACTED]. Enter the code below.

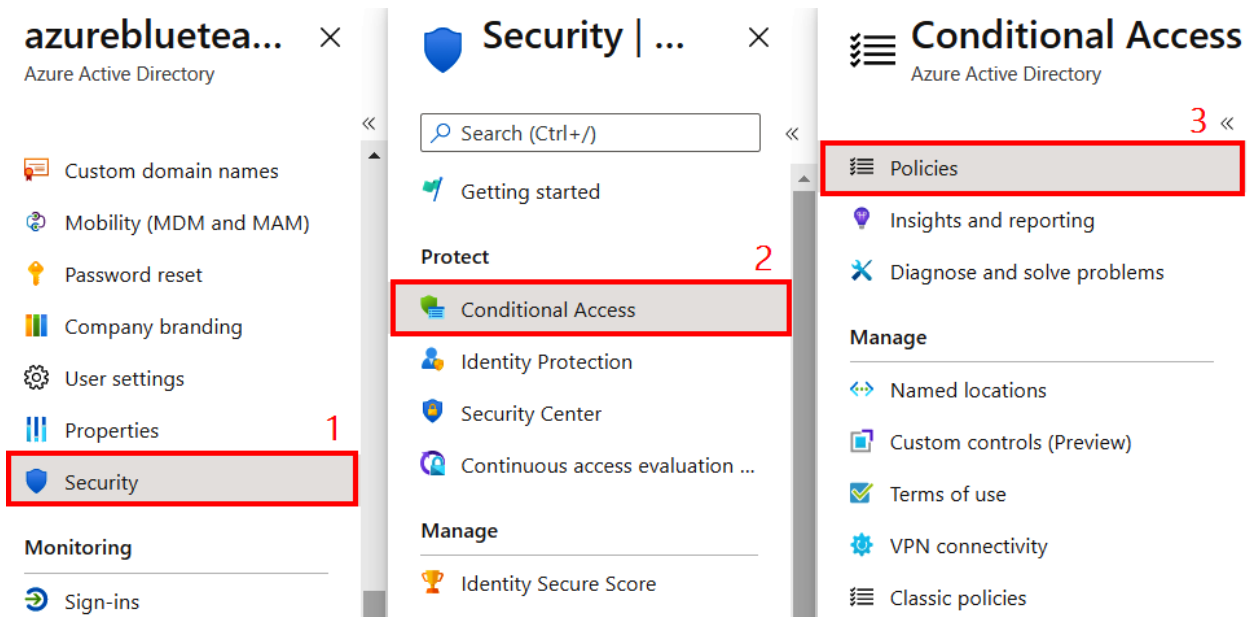
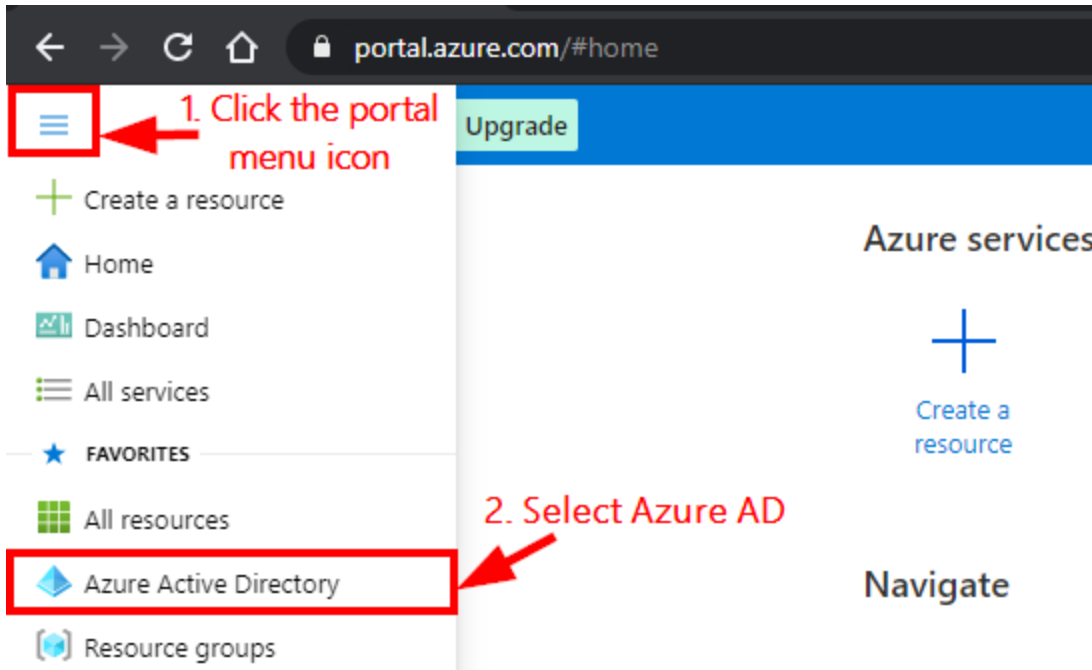
[Resend code](#)

Back

Next







What is conditional access?

Conditional Access gives you the ability to enforce access requirements when specific conditions occur. Let's take a few examples

Conditions	Controls
When any user is outside the company network	They're required to sign in with multi-factor authentication
When users in the 'Managers' group sign-in	They are required be on an Intune compliant or domain-joined device

[Want to learn more about conditional access?](#)

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

✓ 1

Assignments

Users and groups ⓘ 2
 Specific users included ⓘ

Cloud apps or actions ⓘ
No cloud apps or actions selected >

Conditions ⓘ
0 conditions selected >

Access controls

Enable policy

Report-only On Off

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users [Learn more](#)

Include Exclude

None
 All users
 Select users and groups

All guest and external users ⓘ
 Directory roles ⓘ

3 Users and groups

Select
0 users and groups selected ⓘ >

Select

Users and groups

- 4 BT Brenda Tao
brenda@azureblueteam.io
Selected
- CL cloud-architects
- DO David Okeyode
david-packt-az500@outlook.com
- DF Davy Flury

Selected items

BT Brenda Tao
brenda@azureblueteam.io

5

New


Conditional access policy

Azure-Management-External-Policy ✓

Assignments

Users and groups ⓘ >

Specific users included >

1 Cloud apps or actions ⓘ  >
No cloud apps or actions selected

Conditions ⓘ >

0 conditions selected

Access controls

Grant ⓘ >

0 controls selected

Session ⓘ >

0 controls selected


Enable policy

Report-only On Off

Create

Include Exclude

- None
- All cloud apps
- Select apps

2 Select  >
None

Cloud apps


Search

- AW Azure Windows VM Sign-In 372140e0-b3b7-4226-8ef9-d57986...
- MA Microsoft Azure Linux Virtual ce6ff14a-7fdc-4685-bbe0-f6afdfca...
- 3 MA Microsoft Azure Manager 797f4846-ba00-4fd7-ba43-dac1f8f...
- Microsoft Cloud App Security 05a65629-4c1b-48c1-a78b-804c4a...
- Microsoft Search in Bing 9ea1ad79-fdb6-4f9a-8bc3-2b70f96...

Selected items

MA Microsoft Azure I 797f4846-ba00-4fd... Remove

Select 4

 Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal. Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected.

New

Conditional access policy

make decisions, and enforce organizational policies. [Learn more](#)

Name *

Azure-Management-External-Policy ✓

Assignments

Users and groups ⓘ >

Specific users included

Cloud apps or actions ⓘ >

1 app included

1 **Conditions** ⓘ >

0 conditions selected

Access controls

Grant ⓘ >

0 controls selected

Enable policy

Report-only On Off

Create

client apps, or device state. [Learn more](#)

User risk ⓘ >

Not configured

2 **Sign-in risk** ⓘ >

Not configured

Device platforms ⓘ >

Not configured

Locations ⓘ >

Not configured

Client apps ⓘ >

Not configured

Device state (Preview) ⓘ >

Not configured

Sign-in risk

3 ✕

Control user access to respond to specific sign-in risk levels. [Learn more](#)

Configure ⓘ

Yes No

Select the sign-in risk level this policy will apply to

High

Medium

Low

No risk

Select

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Azure-Management-External-Policy ✓

Assignments

Users and groups ⓘ >

Specific users included

Cloud apps or actions ⓘ >

1 app included

Conditions ⓘ >

0 conditions selected

Access controls

Enable policy

Report-only

On

Off

Create

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ >

Not configured

Sign-in risk ⓘ >

Not configured

Device platforms ⓘ >

Not configured

Locations ⓘ >

Not configured

Client apps ⓘ >

Not configured

Device state (Preview) ⓘ >

1

Device platforms



Apply policy to selected device platforms. [Learn more](#)

Configure ⓘ

Yes

No

Include ⓘ

Exclude

Any device

Select device platforms

Android

iOS

Windows Phone

Windows

macOS

Done

2

client apps, or device state. [Learn more](#)

User risk ⓘ	>
Not configured	

Sign-in risk ⓘ	>
Not configured	

Device platforms ⓘ	>
Not configured	

Locations ⓘ	>
Not configured	

Client apps ⓘ	>
Not configured	

Device state (Preview) ⓘ	>
Not configured	

Configure ⓘ

Yes No

Include Exclude

- Any location
- All trusted locations
- Selected locations

New

Conditional access policy

Assignments

Users and groups ⓘ >

Specific users included >

Cloud apps or actions ⓘ >

1 app included >

Conditions ⓘ >

0 conditions selected >

Access controls

Grant ⓘ > 1

0 controls selected >

Session ⓘ >

0 controls selected >

Enable policy

Report-only On Off

Create

Grant



Control user access enforcement to block or grant access. [Learn more](#)

Block access 2

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ
[See list of approved client apps](#)

Require app protection policy ⓘ
[See list of policy protected client apps](#)

Require password change ⓘ

For multiple controls

Require all the selected controls

Require one of the selected controls

Select 3

Enable policy

Report-only On 1 Off

Create 2



brenda@azureblueteam.io

You don't have access to this

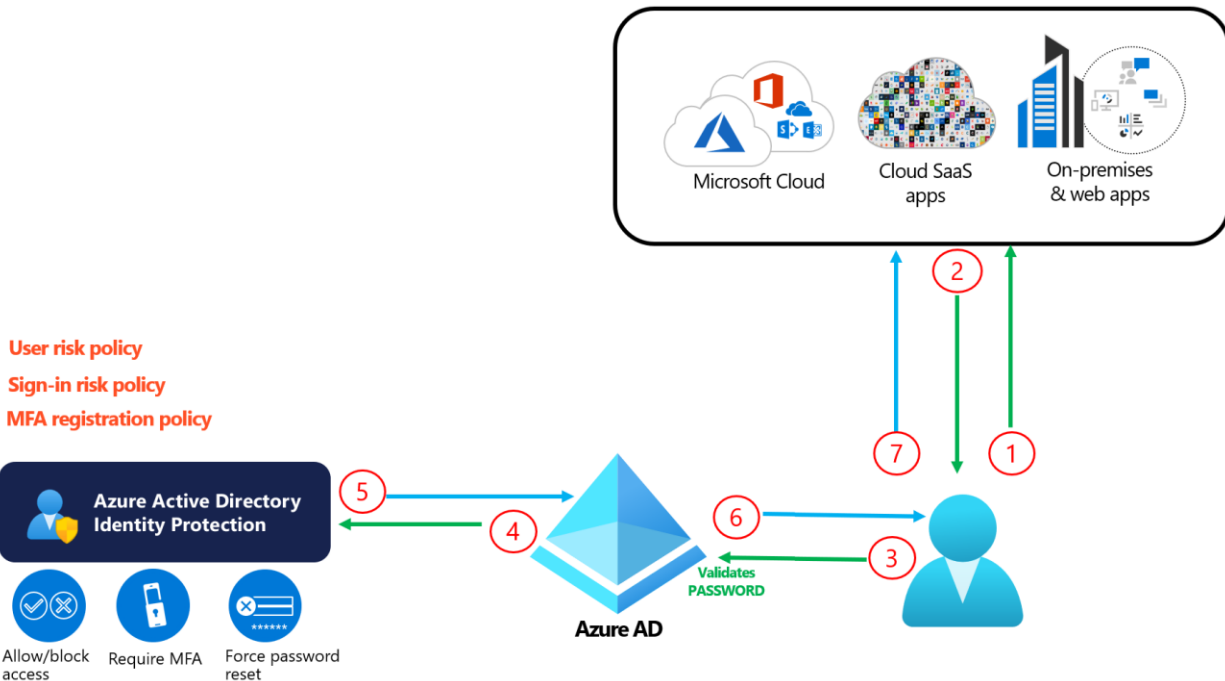
Your sign-in was successful, but you don't have permission to access this resource.

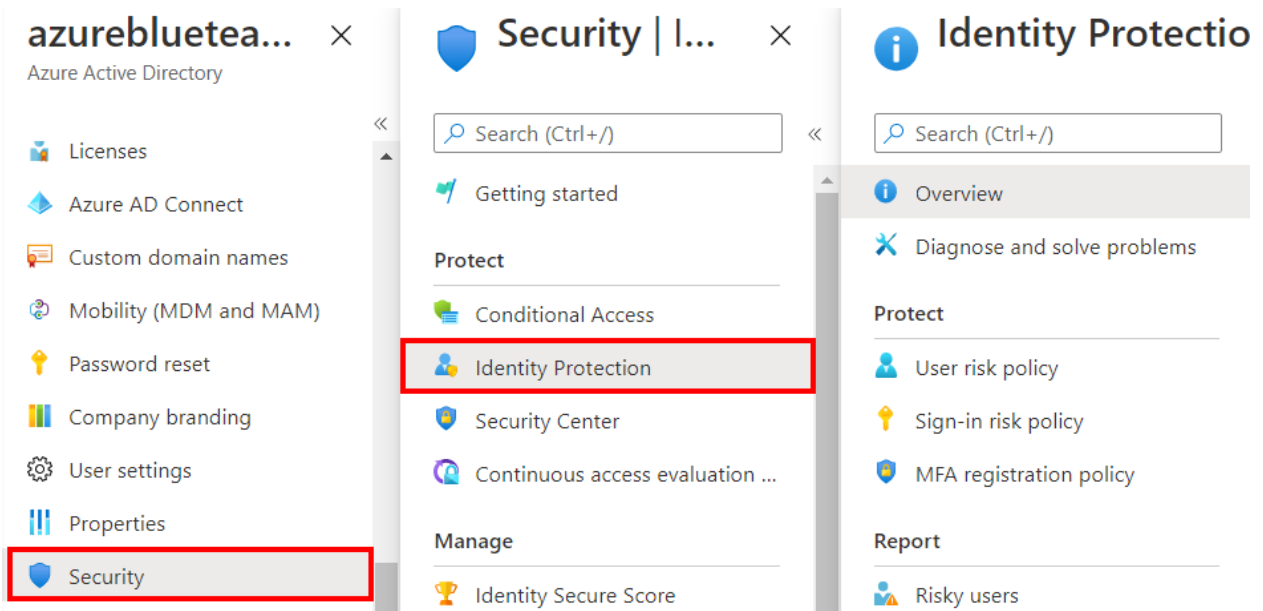
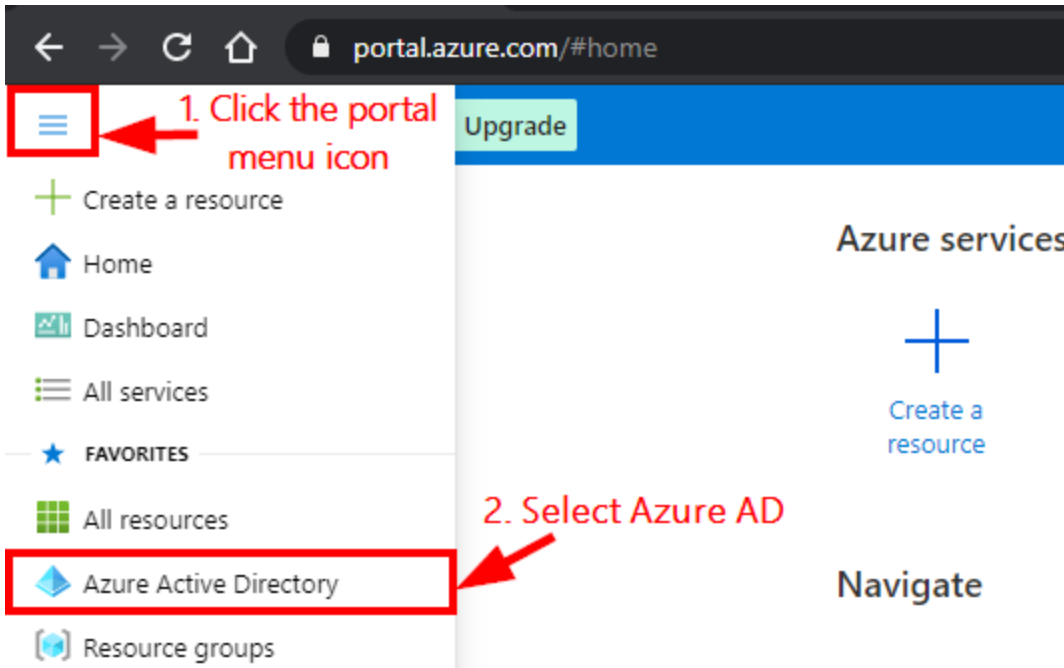
[Sign out and sign in with a different account](#)

[More details](#)

+ New policy 👤 What If ↻ Refresh | ❤️ Got feedback?


Policy Name	State	
Azure-Management-External-Policy	On	1 ⋮
		2 Delete 🗑️






Identity Protection | Overview




 [Learn more](#)


 [Refresh](#)





 Overview

 Diagnose and solve problems


Protect 1


 [User risk policy](#)


 [Sign-in risk policy](#)

 [MFA registration policy](#)


Report 2

 [Risky users](#)

 [Risky sign-ins](#)

 [Risk detections](#)

Notify 3

 [Users at risk detected alerts](#)

 [Weekly digest](#)

Date range = **30 days**

New risky users detected 

12/27

Count

-

[Configure user risk policy >](#)

New risky sign-ins detected 

100


80

Policy Name
User risk remediation policy

Assignments

 Users

1 All users included and 1 user excluded

 User risk ⓘ

2 Low and above

Controls

 Access ⓘ

3 Require password change

Enforce policy 4

On Off

Save


5

Policy Name
Sign-in risk remediation policy

Assignments


 Users

1 All users included and 1 user excluded

 Sign-in risk ⓘ

2 Low and above

Controls

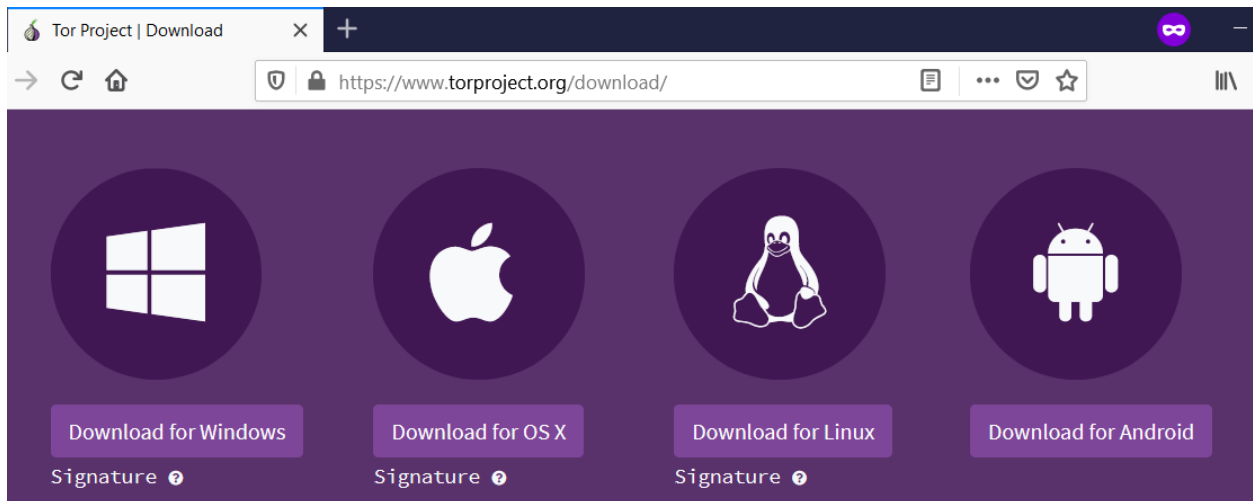
 Access ⓘ

3 Block access

Enforce policy 4

On Off

Save 5





Click "Connect" to connect to Tor.

Click "Configure" to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.

Connect

Configure



← brenda@azureblueteam.io

Enter password

●●●●●●●●●●

[Forgot my password](#)

Sign in



brenda@azureblueteam.io

Your sign-in was blocked

We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin.

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

[More details](#)

Identity Protection | Risky users ✕

Search (Ctrl+/) << ⓘ Learn more ↓ Download ☰ Unselect all ✕ Confirm user(s) compromised ✓ Dismiss user(s) risk ...

Auto refresh : **Off** Show dates as : **Local** Risk state : **2 selected** Status : **Active**

+ Add filters

<input checked="" type="checkbox"/> User ↑↓	Risk state ↑↓	Risk level ↑↓	Risk last updated ↑↓
<input checked="" type="checkbox"/> Brenda Tao	At risk	Medium	1/24/2021, 3:37:43 PM ...

2 →

1

Risky users

Details

🔄 User's sign-ins 🔄 User's risky sign-ins ⚠️ User's risk detections | 🔄 Reset password ...

Basic info	Recent risky sign-ins	Detections not linked to a sign-in	Risk history
User: Brenda Tao		Risk state: At risk	← 3
Roles: Global admin		Risk level: Medium	
Username: brenda@azureblueteam.io		Details: -	

Search (Ctrl+)

Download Learn more Export Data Settings Configure trusted IPs Troubleshoot

- Overview
- Diagnose and solve problems

Protect

- User risk policy
- Sign-in risk policy
- MFA registration policy

Report

- Risky users
- Risky sign-ins**
- Risk detections

Auto refresh : Off Date : Last 7 days Show dates as : Local Risk state : 2 selected
Risk level (real-time) : None Selected Risk level (aggregate) : None Selected
Detection type(s) : None Selected Add filters

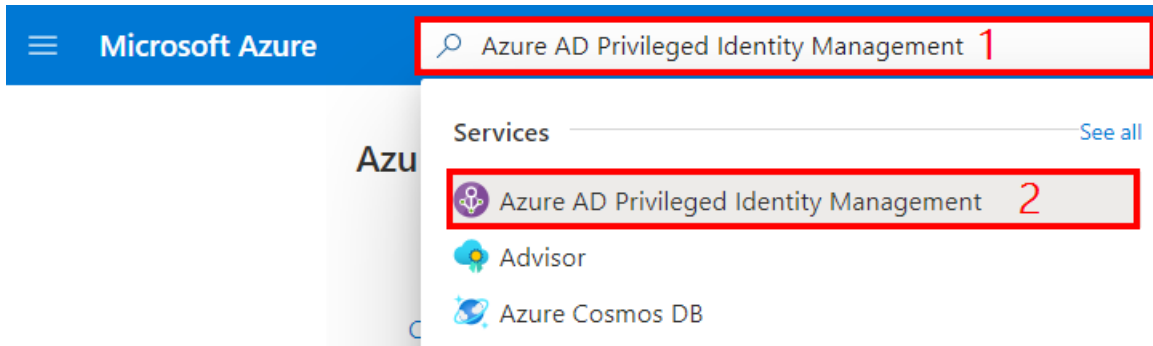
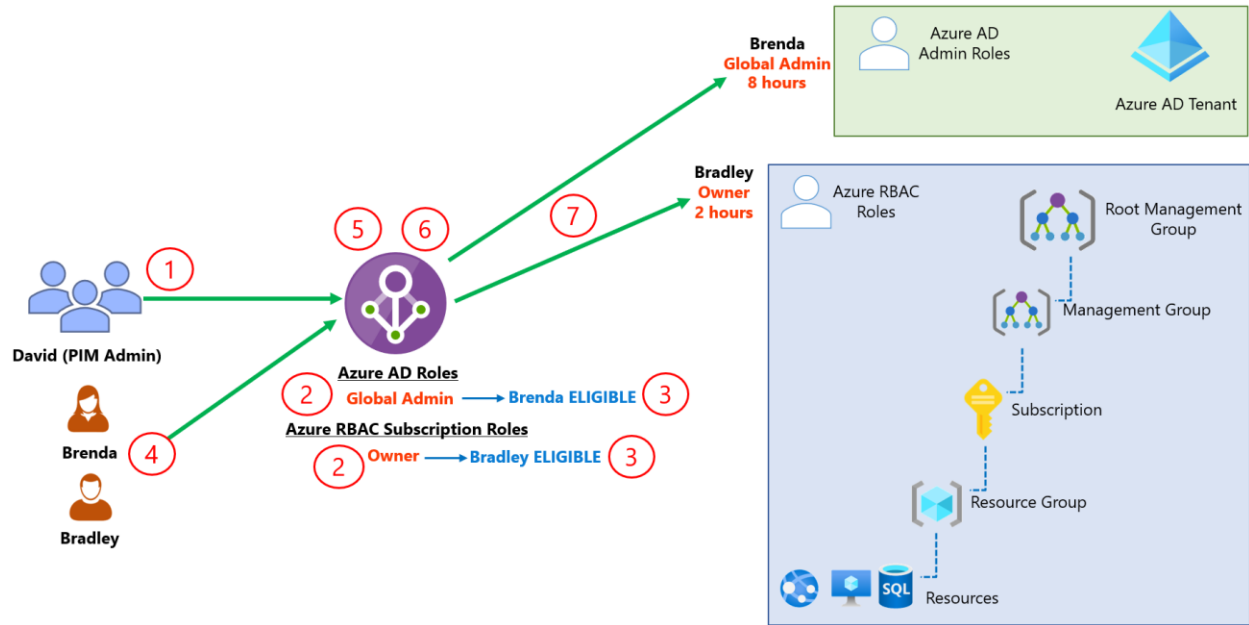
Date	User	IP address	Location	Risk state
<input type="checkbox"/> 1/24/2021, 3:30:59 PM	Brenda Tao	185.██████████	Schoenwalde-Glien, ...	At risk
<input type="checkbox"/> 1/24/2021, 3:23:25 PM	Brenda Tao	185.██████████	Schoenwalde-Glien, ...	At risk

Users can have detections on sign-ins that are currently not supported in the sign-ins report. Such risky sign-ins do not appear here. To see all the detections, go to Risk detections.

1


2


Chapter 5: Azure AD Identity Governance





⚡ Quick start

Tasks


 My roles


 My requests


 Approve requests

 Review access


Manage

 Azure AD roles **1**

 Privileged access groups (Preview)

 Azure resources


Activity


 Quick start


 Overview

Tasks


 My roles

 Pending requests


 Approve requests

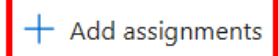

 Review access

Manage


 Roles **2**


 Assignments


 Alerts


<< **3**  Add assignments 


Role

 Application Administrator


 Application Developer

 Attack Payload Authenticated User

 Attack Simulation Admin

 Authentication Administrator

 Azure DevOps Administrator

 Azure Information Protection Administrator

 B2C IEF Keyset Administrator

 B2C IEF Policy Administrator

Add assignments

Privileged Identity Management | Azure AD roles

Membership Setting

i You can also assign roles to groups now. [Learn more](#)

Resource

Default Directory

Resource type

Directory

Select role ⓘ

1 **Billing Administrator**

Scope type ⓘ

Directory

Select member(s) * ⓘ

2 **No member selected**

Next >

Cancel

Privileged Identity Management | Azure AD roles

Only groups eligible for role assignment are displayed. [Learn more](#)

Search

BT

Brenda Tao
brenda@azureblueteam.io
Selected

3

DO

David Okeyode
david-packt-az500@outlook.com

DF

Davy Flury
davy@davidpacktaz500outlook.onmicrosoft.com

Selected items

BT

Brenda Tao
brenda@azureblueteam.io

Remove

Select

4

Add assignments

Privileged Identity Management | Azure AD roles

Membership **Setting**

Assignment type ⓘ

Eligible 1

Active

Maximum allowed eligible duration is permanent.

Permanently eligible

Assignment starts

01/24/2021



7:03:58 PM

Assignment ends

01/24/2022



7:03:58 PM

Assign

2

< Prev

Cancel



Default Directory | Assignments

Privileged Identity Management | Azure AD roles

- Quick start
- Overview
- Tasks
- My roles
- Pending requests
- Approve requests
- Review access
- Manage
- Roles
- Assignments** 1
- Alerts

<< + Add assignments ⚙ Settings ↻ Refresh ↓ Export |

2 Eligible assignments Active assignments Expired assign

🔍 Search by member name or principal name

Name	Principal name	Type
Billing Administrator		
Brenda Tao	brenda@azureblueteam	User



Default Directory | Roles

Privileged Identity Management | Azure AD roles

- My roles
- Pending requests
- Approve requests
- Review access
- Manage
- Roles** 1
- Assignments
- Alerts

<< + Add assignments ↻ Refresh ↓ Export | ❤

- Azure Information Protection Administrator
- B2C IEF Keyset Administrator
- B2C IEF Policy Administrator
- Billing Administrator** 2
- Cloud Application Administrator
- Cloud Device Administrator
- Compliance Administrator
- Compliance Data Administrator



Billing Administrator | Role settings

Privileged Identity Management | Azure AD roles




Edit

2

Manage

 Assignments

 Description

 Role settings

1

Activation

Setting

Activation maximum duration (hours)

Require justification on activation

Require ticket information on activation

On activation, require Azure MFA

Require approval to activate

Approvers

Edit role setting - Billing Administrator

Privileged Identity Management | Azure AD roles

Activation 1 Assignment Notification

Activation maximum duration (hours)

3 2

On activation, require Azure MFA None 3

Require justification on activation

Require ticket information on activation

4 Require approval to activate

5
1 Member(s), 0 Group(s) selected

Update

Next: Assignment 6


Edit role setting - Billing Administrator

Privileged Identity Management | Azure AD roles

Activation **1** **Assignment** Notification

Allow permanent eligible assignment

Expire eligible assignments after

1 Year 

2 Allow permanent active assignment

Expire active assignments after

6 Months 

Require Azure Multi-Factor Authentication on active assignment

Require justification on active assignment

Update

Prev: Activation

3

Next: Notification

Edit role setting - Billing Administrator

Privileged Identity Management | Azure AD roles

Activation Assignment **Notification** ¹

Send notifications when members are assigned as eligible to this role:

Type	Default recipients
Role assignment alert	<input checked="" type="checkbox"/> Admin
Notification to the assigned user (assignee)	<input checked="" type="checkbox"/> Assignee
Request to approve a role assignment renewal/extensi...	<input checked="" type="checkbox"/> Approver

Send notifications when members are assigned as active to this role:

Type	Default recipients
------	--------------------

Update ²

Prev: Assignment

 Refresh |  Got feedback?

Eligible assignments Active assignments Expired assignments

 Search by role

Role	↑↓	Scope	↑↓	Membership	↑↓	End time	Action
Billing Administrator		Directory		Direct		Permanent	Activate

Activate - Billing Administrator



Privileged Identity Management | Azure AD roles

Roles **Activate** Status

Custom activation start time

Duration (hours) ⓘ

Slider control for duration, set to 3 hours.

*Reason (max 500 characters) ⓘ

Text input field containing "Role needed for some tasks" with a green checkmark. A red box highlights the text, and a red "1" is next to the label.

Buttons: **Activate** (highlighted with a red box and a red "2") and **Cancel**.

Overview

Refresh

Tasks

My roles

Pending requests

Approve requests (highlighted with a red box and a red "1")

Review access

Role Requestor

No requests pending approval

Manage

Roles

Assignments

Alerts

Access reviews

Approve (highlighted with a red box and a red "3") **Deny** **Refresh**

Role ↑↓ Requestor

Billing Administrator (highlighted with a red box and a red "2") Brenda Tao

Approve Request



Brenda Tao
brenda@azureblueteam.io

Role	Billing Administrator
Requestor	Brenda Tao
Request Time	2/7/2021, 6:24 PM
Reason	Role needed for some tasks
Ticket number	
Ticket system	
Start time	2/7/2021, 6:31 PM
End Time	2/7/2021, 9:31 PM

Justification * ⓘ


1


Role approved to complete needed tasks for three hours ✓

Confirm 2

4 david-packt-az500@out... AZUREBLUETEAM (DEFAULT DIRE...

✓ Update request status 6:40 PM ✕
Brenda Tao is approved

 Refresh

 Got feedback?

Eligible assignments


Active assignments

Expired assignments

 Search by role


Role	Scope	Membership	State	End time	Action
Global Administrator	Directory	Direct	Assigned	Permanent	Deactivate
Billing Administrator	Directory	Direct	Activated	2/7/2021, 9:40:11 PM	Deactivate


Microsoft Azure


 Azure AD Privileged Identity Management

Services

[See all](#)


 Azure AD Privileged Identity Management


 Advisor


 Azure Cosmos DB

 Review access


Manage

 Azure AD roles

 Privileged access groups (Previ...


 Azure resources

Activity


 My audit history


Manage

 Roles

 Assignments

 Alerts

 Access reviews

 Discovery and insights (Preview)

 Settings

Create an access review

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

Review name * 1 ✓

Description ⓘ 2 ✓

Start date * 3 📅

Frequency 4 ▼

Duration (in days) ⓘ 14 5

End ⓘ 6 Never End by Occurrences

Number of times

End date 📅

Users

Review role membership (permanent and eligible) *

8

Reviewers

Reviewers 9 ▼

Select reviewers *

10

▼ Upon completion settings

▼ Advanced settings

11

☰ New 🔍 Filter 📅 Group ⚙️ Settings

Access reviews for Azure AD directory roles

🔍 Search by name or owner

Role	Owner	Start Date ↑↓	End Date ↑↓	Status
Global Administrator Review				
Global Administrator	David Okeyode david-packt-az500@outlook.com	2/7/2021	12/31/9999	Active

Global Administrator Review

Overview « 🗑️ Delete series

Current

- Results
- Reviewers
- Settings
- Audit logs

Series

- Reviewers
- Settings
- Scheduled review
- Review history
- Audit logs

Essentials

Owner : David Okeyode[david-packt-az500_outlook.com#EXT#@]
Role : Global Administrator
Access review period : 2/7/2021 - No end date
Object Id : 8e23dc46-4d1f-451b-b830-6eb303526687

Current

Status	Count
Not reviewed	3
Approved	0
Denied	0
Don't know	0

Global Administrator Review | Results

Overview « 🛑 Stop ↺ Reset ⬇️ Download

Search

User	Outcome	Reas...↑↓	Reviewe...↑↓	Applie...↑↓	Apply re...↑↓	Recommended action
syncadmin syncadmin@azureblueteam.io	Not reviewed					Deny Last signed in more than 30 days ago
David Okeyode david-packt-az500_outlook.co...	Not reviewed					Approve Last signed in less than 30 days ago (2/7/2021)
Brenda Tao brenda@azureblueteam.io	Not reviewed					Approve Last signed in less than 30 days ago (2/7/2021)

Brenda Tao - Audit Logs

Download Refresh Columns Got feedback?

Date : **Last 7 days** Show dates as : **Local** Service : **All** Category : **All** Activity : **All** Add filters

Date	Service	Category	Activity	Status
2/7/2021, 9:40:12 PM	PIM	RoleManagement	Remove member from role (PIM activ...	Success
2/7/2021, 9:40:12 PM	Core Directory	RoleManagement	Remove member from role	Success
2/7/2021, 6:40:12 PM	PIM	RoleManagement	Add member to role completed (PIM ...	Success
2/7/2021, 6:40:11 PM	Core Directory	RoleManagement	Add member to role	Success
2/7/2021, 6:40:11 PM	PIM	RoleManagement	Add member to role request approve...	Success
2/7/2021, 6:24:42 PM	PIM	RoleManagement	Add member to role approval reques...	Success
2/7/2021, 6:24:41 PM	Access Reviews	Policy	Create request	Success
2/7/2021, 6:24:37 PM	PIM	RoleManagement	Add member to role requested (PIM ...	Success
2/7/2021, 6:11:24 PM	Core Directory	UserManagement	Update user	Success

Global Administrator Review | Settings

« Save Discard

Overview

Current

- Results
- Reviewers
- Settings**
- Audit logs

Series

- Reviewers
- Settings

General Reviewers Scheduling **When completed**

Auto apply results to resource Enable Disable

If reviewers don't respond No change No change Remove access Approve access Take recommendations

Default Directory | Review access

Privileged Identity Management | Azure AD roles

« Access reviews for Azure AD directory roles

- Quick start
- Overview
- Tasks
 - My roles
 - Pending requests
 - Approve requests
 - Review access** 1

Review Name	Role	End Date
Global Administrator Review 2	Global Administrator	2/21/2021 14 day(s)

Select the user(s) from the list, and approve or deny their role membership using the buttons below

Search

User	Reason	Reviewed by	Audit Details	Recommended action
Not reviewed				
<input type="checkbox"/> syncadmin syncadmin...			View	Deny Last signed in more than 30 days ago
<input type="checkbox"/> David Okey... david-pack...			View	Approve Last signed in less than 30 days ago (2...
<input checked="" type="checkbox"/> Brenda Tao brenda@az...			View	Approve Last signed in less than 30 days ago (2...

Reason * ⓘ

2 role still needed ✓

3 **Approve** Deny Reset

Default Directory | Access reviews

Privileged Identity Management | Azure AD roles

Approve requests
Review access

Manage

- Roles
- Assignments
- Alerts
- Access reviews**
- Discovery and insights (Previe...)
- Settings

New Filter Group Settings

Access reviews for Azure AD directory roles

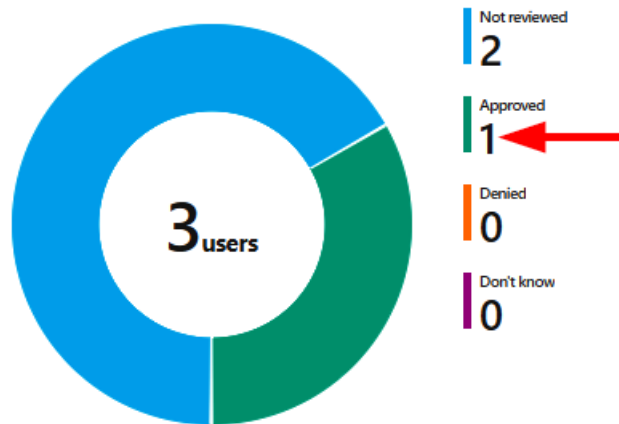
Search by name or owner

Role	Owner	Start Date	End Date
Global Administrator Review			
Global Administra...	David Okeyode david-packt-az500@o...	2/7/2021	12/31/9999

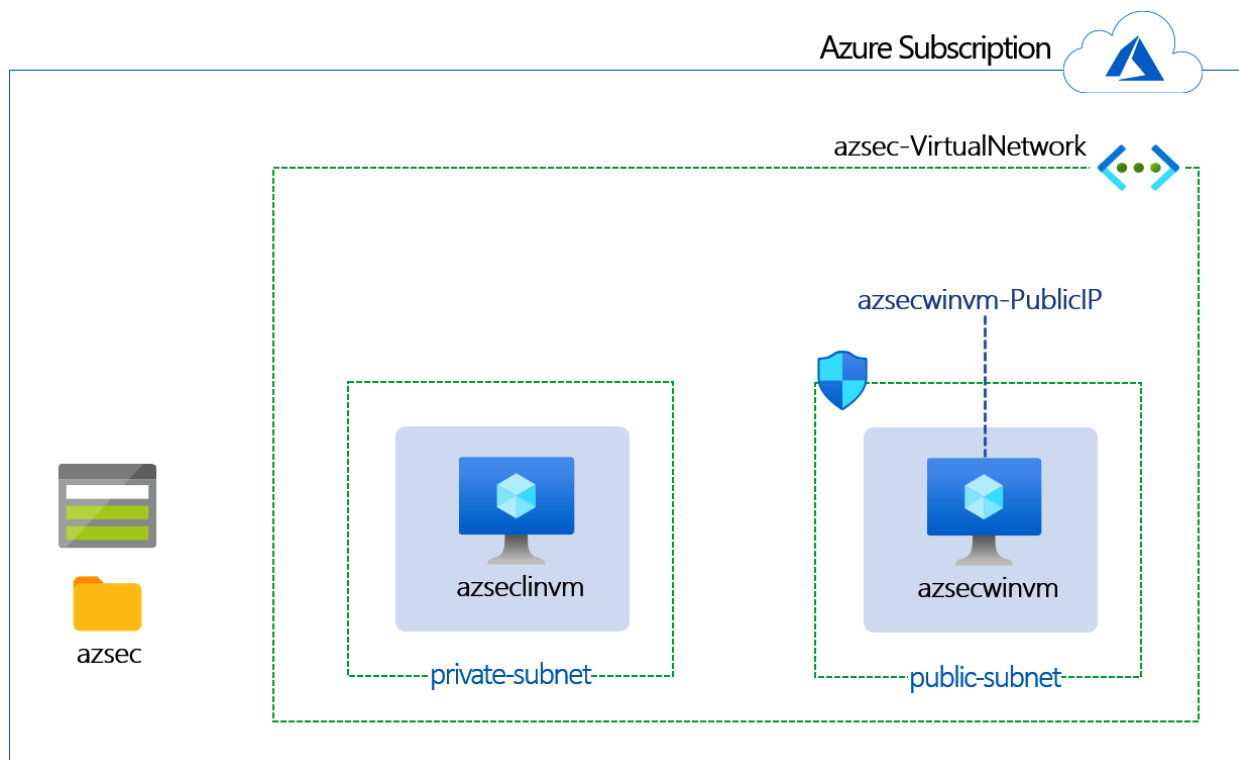
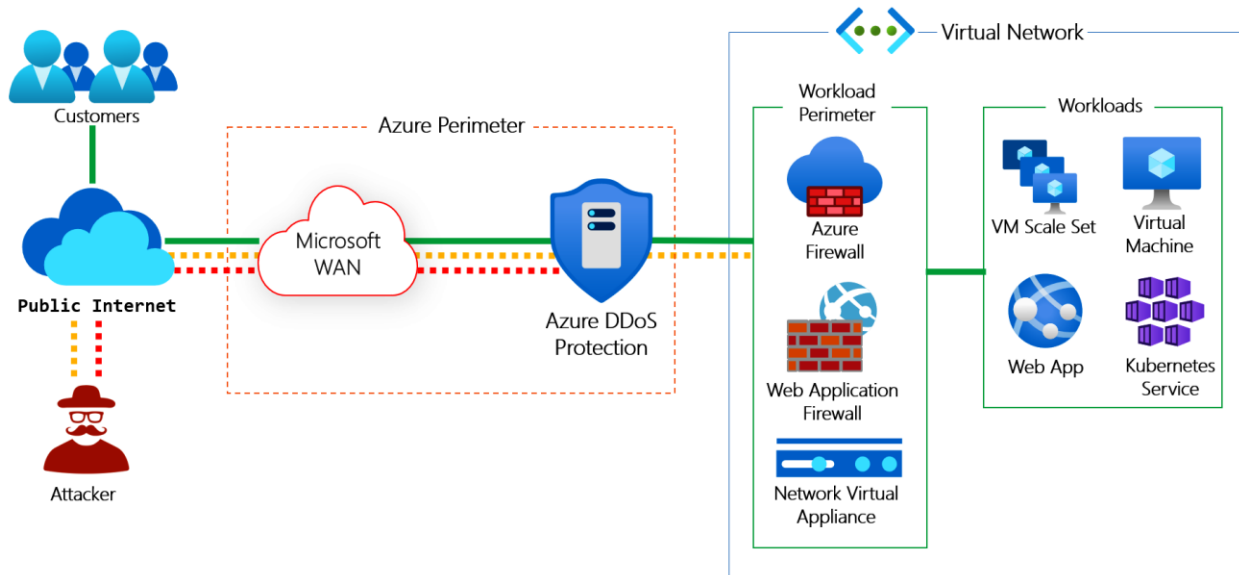
Delete series

Role : Global Administrator
Access review period : 2/7/2021 - No end date
Object Id : 8e23dc46-4d1f-451b-b830-6eb303526687

Current



Chapter 6: Implementing Perimeter Security



Azure Security Engineer Book - Chapter 6

Windows VM

- Windows Server 2019 Datacenter
- Putty
- Google Chrome

Linux VM

- Ubuntu 18.04



Sign in

to continue to Microsoft Azure

No account? [Create one!](#)

[Can't access your account?](#)

[Sign in with a security key](#) (?)

[Next](#)

Custom deployment ...

Deploy from a custom template

Subscription * ⓘ

1 AzureBlueTeam-PROD (1c63ad39-68ee-444a-90a8-a2ccaf67f671) ▼

Resource group * ⓘ

2 (New) azuresec-c6-rg ▼

[Create new](#)

Instance details

Region * ⓘ

3 UK South ▼

Storagename ⓘ

[concat('azsecvmstrg', uniqueString(resourceGroup().id))]

Vm-dns ⓘ

[concat('azsecwinvm-', uniqueString(resourceGroup().id))]

Admin User ⓘ

azureadmin ✓

Admin Password * ⓘ

4 ✓

Vmsize * ⓘ

1x Standard B2ms
2 vcpus, 8 GB memory
[Change size](#)

Location ⓘ

[resourceGroup().location]

_artifacts Location ⓘ

[deployment().properties.templateLink.uri]

_artifacts Location Sas Token ⓘ

5 **Review + create**

< Previous

Next : Review + create >

Custom deployment

Deploy from a custom template

✓ Validation Passed

Basics **Review + create**

Summary

Customized template
9 resources

Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal terms associated

Create

< Previous

Next

[Download a template for automation](#)

Microsoft.Template-20210202023536 | Outputs

Deployment

Search (Ctrl+/) <<

Overview

Inputs

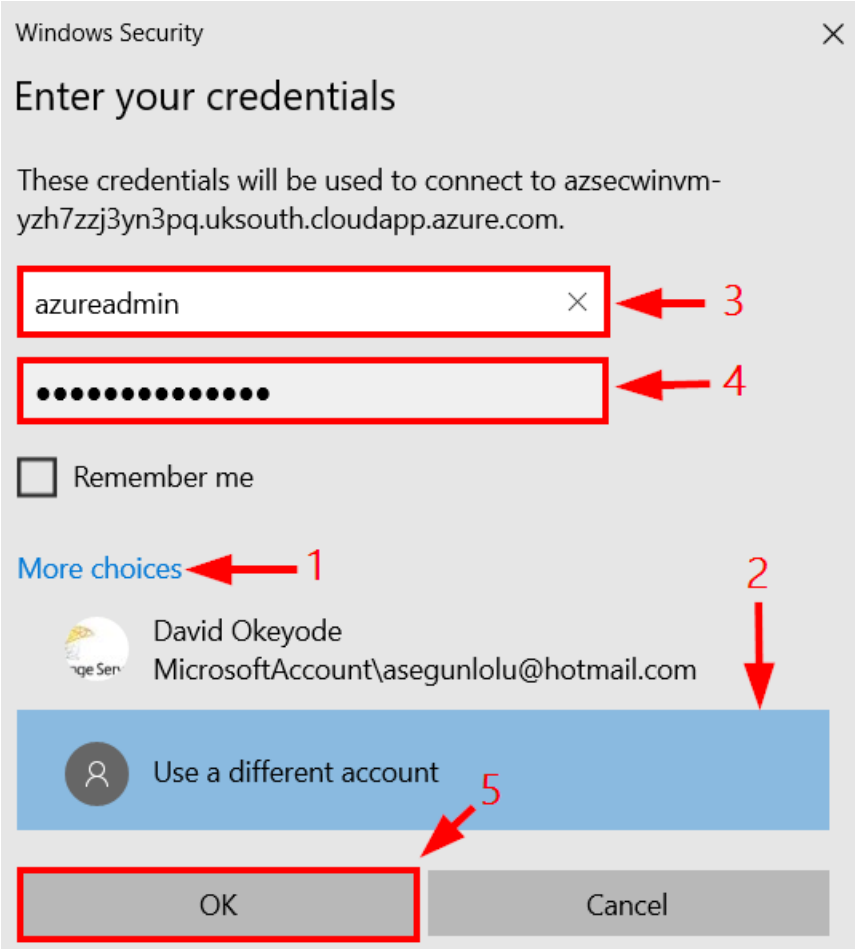
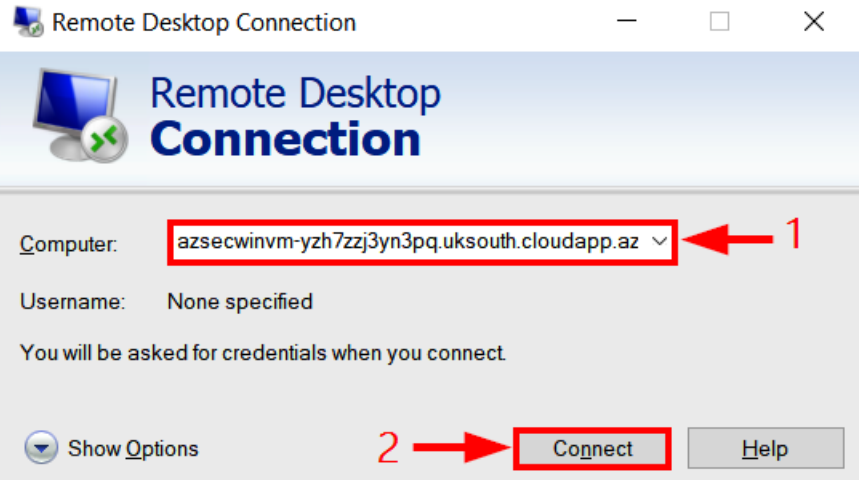
Outputs

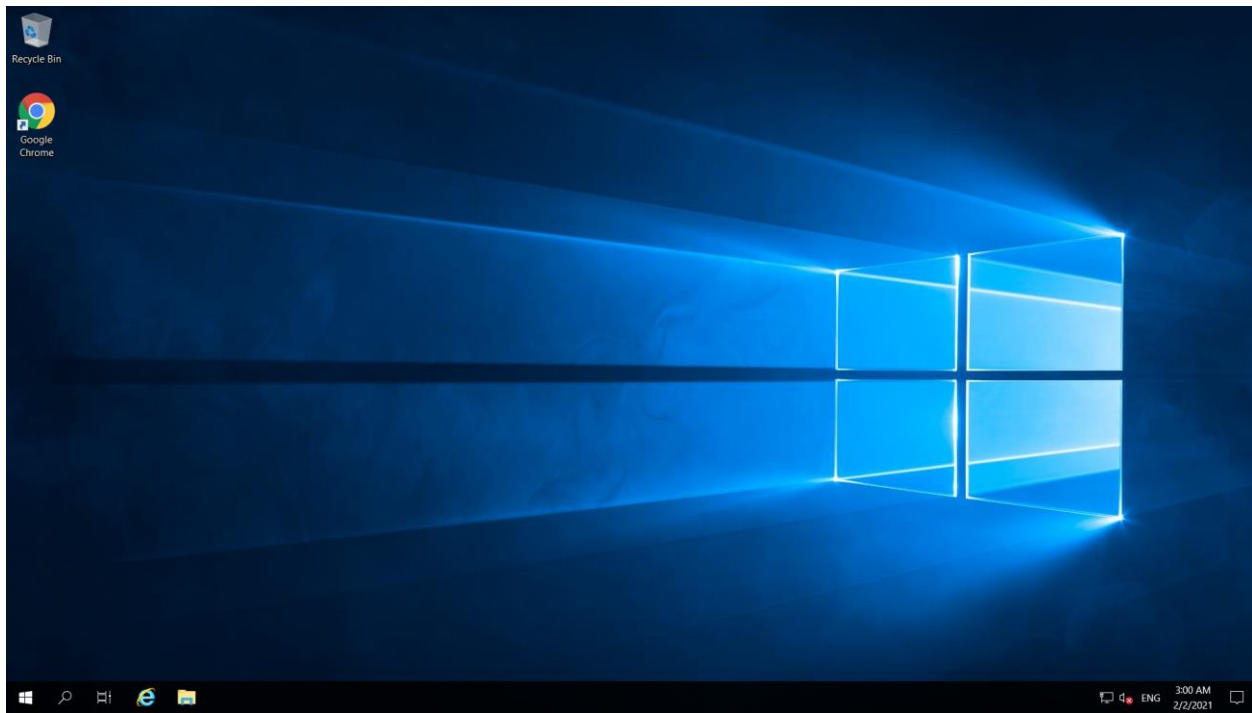
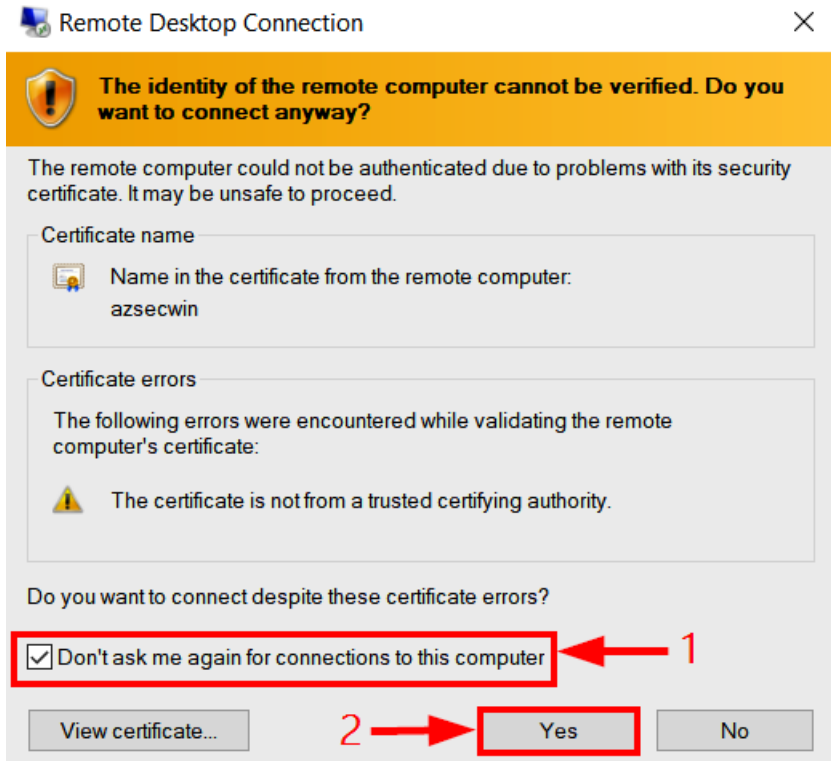
Template

winvm-dns

azsecwinvm-yzh7zzj3yn3pq.uksouth.cloudapp.azure.com







- ☰ 1
- + Create a resource 2
- 🏠 Home
- 📊 Dashboard

New

DDoS protection plan ←

Create a DDoS protection plan ...

i You can create a single DDoS protection plan and apply it to resources in all of your subscriptions.

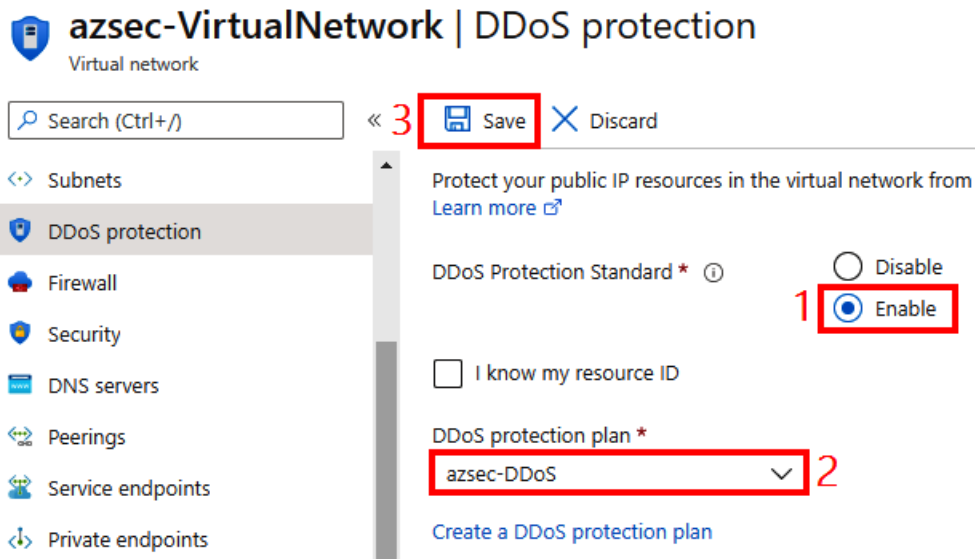
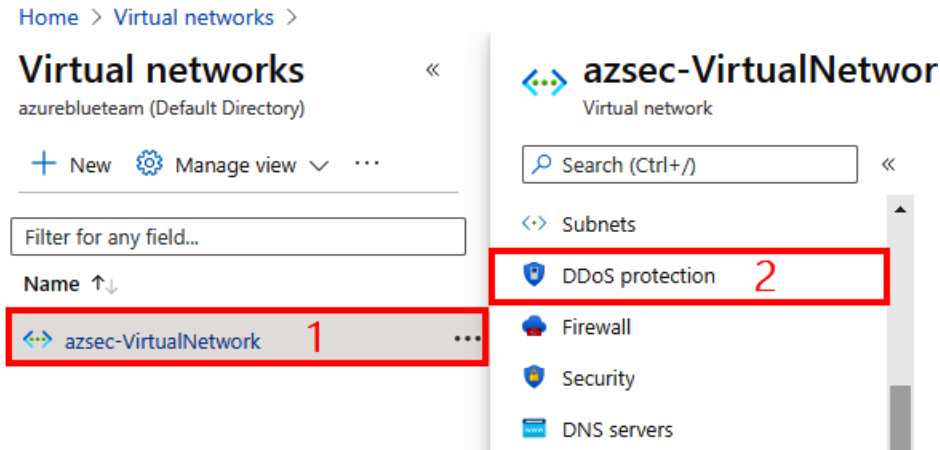
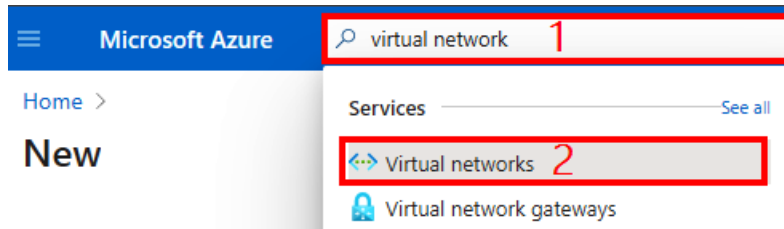
Name *
azsec-DDoS ✓ 1

Subscription *
AzureBlueTeam-PROD (1c63ad39-68ee-444a-90a8-a2ccaf67f671) ∨ 2

Resource group *
azuresec-c6-rg ∨ 3
[Create new](#)

Location *
(Europe) UK South ∨ 4

Create 5 [Automation options](#)



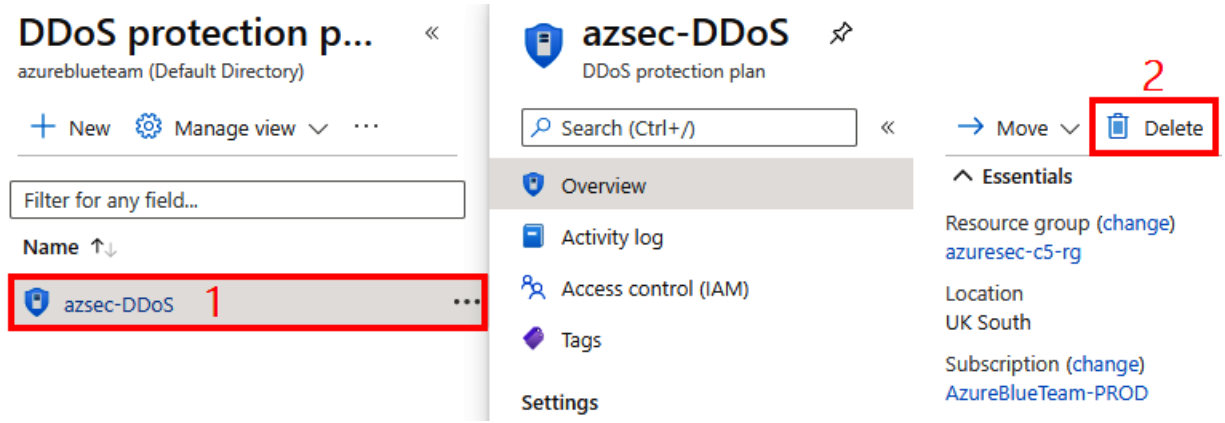
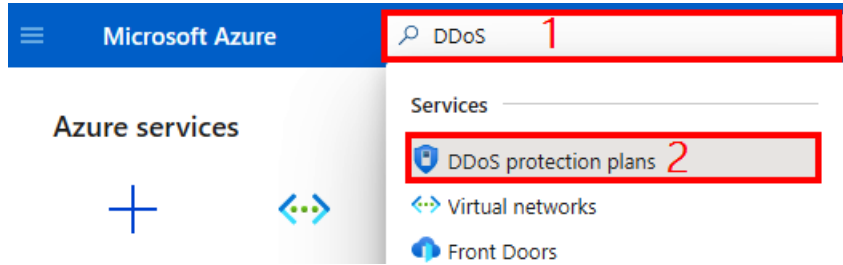
Save Discard

2 DDoS standard protection plan metrics can be found by selecting protected public IP addresses in the DDoS metrics blade. →

Protect your public IP resources in the virtual network from Distributed Denial of Service attacks. [Learn more](#)

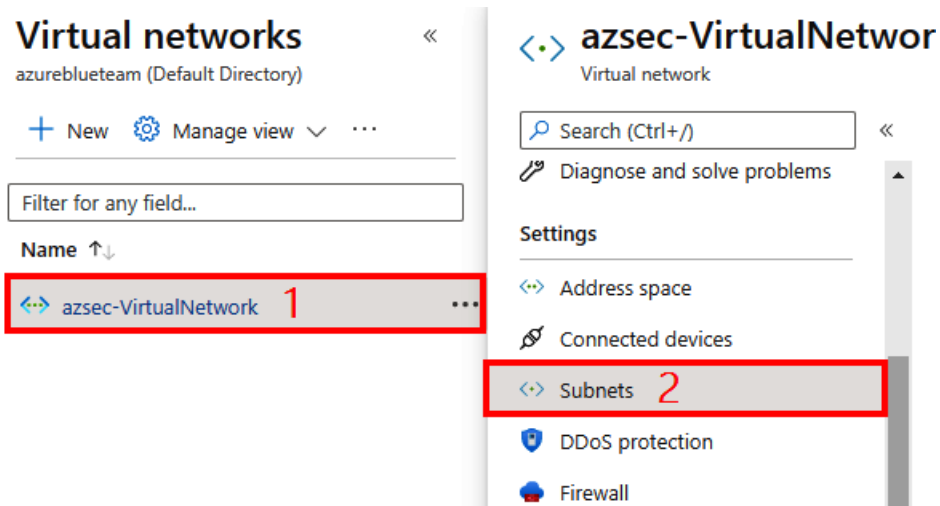
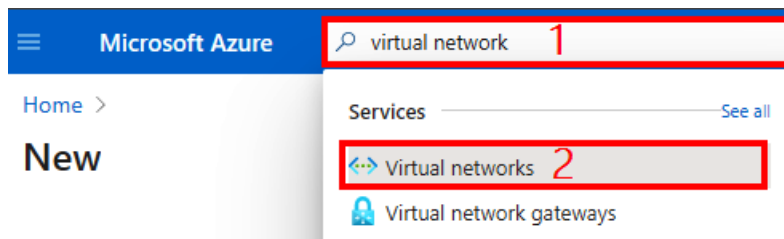
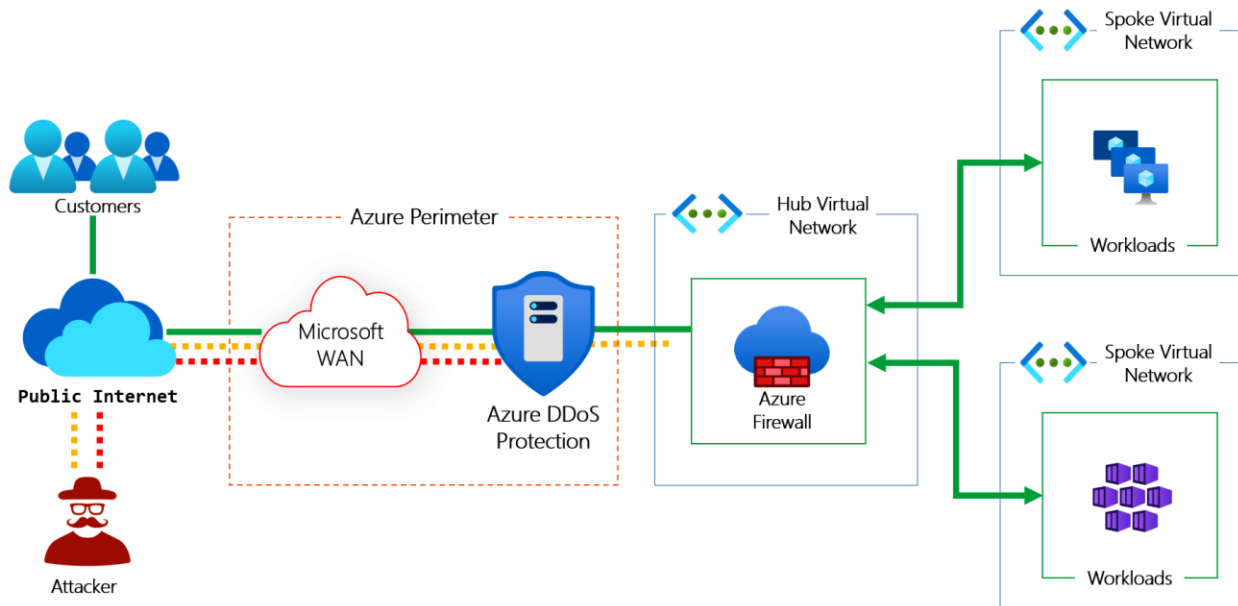
DDoS Protection Standard * **1** **Disable**
 Enable

If you disable DDoS Protection Standard, public IP resources will be exposed to DDoS attacks and all learned policy thresholds will be lost. ✕



Delete the DDoS protection plan

Do you want to delete the DDoS protection plan 'azsec-DDoS'?



azsec-VirtualNetwork | Subnets

Virtual network

Search (Ctrl+/)

<< 2 **+ Subnet** + Gateway subnet Refresh Manage users

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Address space
- Connected devices
- Subnets** 1
- DDoS protection

Search subnets

Name ↑↓	IPv4 ↑↓
public-subnet	10.0.0.0/24 (250 available)
private-subnet	10.0.1.0/24 (250 available)

Add subnet



Name * 1
AzureFirewallSubnet ✓

Subnet address range * ① 2
10.0.2.0/24
10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)

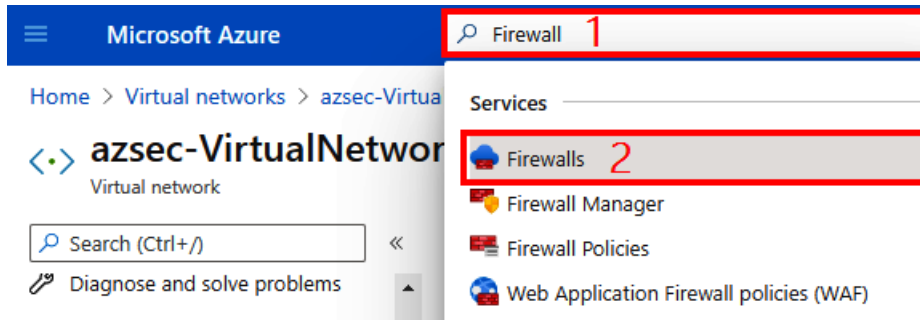
Add IPv6 address space ①

NAT gateway ①
None

Network security group
None

Route table
None

3
Save Cancel



Home > Firewalls >

Create a firewall

virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more.](#)

Project details

Subscription * 1 AzureBlueTeam-PROD (699f5153-f723-4d1c-9bfa-bb173c35ec53) ▼

Resource group * 2 azuresec-c5-rg ▼
[Create new](#)

Instance details

Name * 3 azsec-Firewall ✓

Region * 4 UK South ▼

Availability zone ⓘ None ▼

Choose a virtual network
 Create new Use existing 5

Virtual network 6 azsec-VirtualNetwork (azuresec-c5-rg) ▼

Public IP address * 7 (New) azsec-FirewallIp ▼
[Add new](#)

Forced tunneling ⓘ Disabled

8

[Review + create](#)

[Previous](#)

[Next: Tags >](#)

[Download a template for automation](#)

✔ Your deployment is complete

Deployment name: Microsoft.AzureFirewall-20210208173535
Subscription: AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5...)
Resource group: azuresec-c5-rg

∨ Deployment details (Download)

∧ Next steps

[Go to resource](#)

azsec-Firewall

Firewall

Search (Ctrl+/)

 Delete  Lock

Overview

Activity log

Access control (IAM)


Tags

Settings

DNS

Rules

Public IP configuration

 This firewall can be managed by Azure Firewall Manager. →

Essentials

Resource group (change)
azuresec-c5-rg

Location
UK South

Subscription (change)
AzureBlueTeam-PROD

Subscription ID
32d25af6-ccc1-4942-bdb7-5443dcab4d8a

Firewall subnet
AzureFirewallSubnet

Firewall public IP
azsec-FirewallIp

Firewall private IP
10.0.2.4

Management subnet
-

Make a note
of this value



Microsoft Azure

route tables

Home >

Microsoft.AzureF
Deployment

Search (Ctrl+/)

Overview

Services

- Route tables
- Route filters
- ExpressRoute circuits
- ExpressRoute Direct

Create Route table

[Basics](#) [Tags](#) [Review + create](#)

Project details

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

Subscription * ⓘ **1** AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5443dcab4d8a) ▼

Resource group * ⓘ **2** azuresec-c5-rg ▼
[Create new](#)

Instance details

Region * ⓘ **3** UK South ▼

Name * ⓘ **4** private-subnet-routetable ✓

Propagate gateway routes * ⓘ **5** Yes No

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

✓ Your deployment is complete



Deployment name: Microsoft.RouteTable-20210208175148
Subscription: AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5...
Resource group: azuresec-c5-rg

∨ [Deployment details](#) (Download)

∧ [Next steps](#)

[Go to resource](#)

Search (Ctrl+/) << 2 **+ Add**

Settings

- Configuration
- Routes 1**
- Subnets
- Properties

Search routes

Name

No results.

Add route


private-subnet-routetable

Route name * ✓ 1

Address prefix * ⓘ ✓ 2

Next hop type ⓘ ✓ 3

Next hop address * ⓘ ✓ 4

 Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to

OK

5

<> private-subnet-routetable | Subnets

Route table

Search (Ctrl+/)

<<

+ Associate 2

Settings

Configuration

Routes

<> Subnets 1

Properties

Search subnets

Name ↑↓

Address range ↑↓

No results.

Associate subnet

×

private-subnet-routetable

Virtual network ⓘ

1 azsec-VirtualNetwork

Subnet ⓘ

2 private-subnet

OK 3

azsec-Firewall | Rules

Firewall

Search (Ctrl+/)

Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - DNS
 - Rules 1**
 - Public IP configuration
 - Threat intelligence

This firewall can be managed by Azure Firewall Manager. →

NAT rule collection Network rule collection 2 **Application rule collection**

+ Add application rule collection 3

Priority	Name
No results	

Azure infrastructure application rule collection is enabled by default. [Learn more.](#)

Add application rule collection



Name * 1

Priority * 2

Action * 3

Rules

FQDN tags

name	Source type	Source	FQDN tags
<input type="text"/>	IP address	*, 192.168.10.1, 192.168.10.0/24, 192....	0 selected

FQDN tags may require additional configuration. [Learn more.](#)

Target FQDNs

name 4	Source type 5	Source 6	Protocol:Port 7	Target FQDNs 8
<input type="text" value="allow-bing-search-engine"/> ✓	IP address	10.0.0.0/16 ✓	http:80, http:443 ✓	www.bing.com
<input type="text"/>	IP address	*, 192.168.10.1, 192.168.10.0...	http, http:8080, https, mssql:...	www.microsoft.com, *.micr

Add 9

azsec-Firewall | Rules

Firewall

Search (Ctrl+/) <<

Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - DNS
 - Rules**
 - Public IP configuration

NAT rule collection **Network rule collection** Application rule collection

+ Add network rule collection

Priority	Name
No results	

Add network rule collection

×

Name * **1** egress-firewall-network-rule

Priority * **2** 200

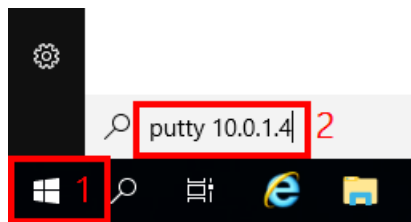
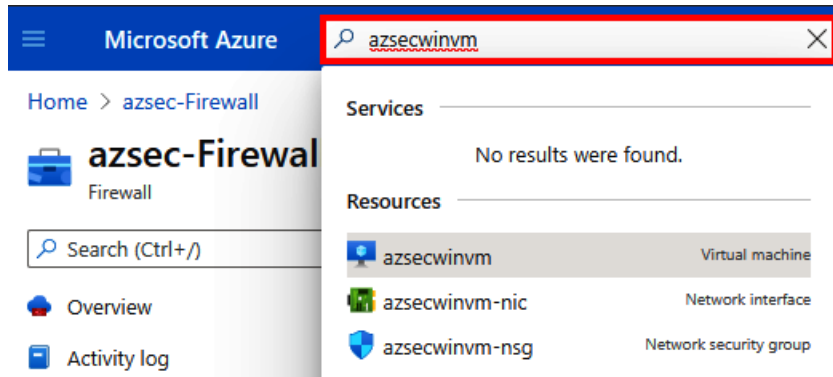
Action * **3** Allow

Rules

IP Addresses

name 4	Protocol 5	Source type 6	Source 7	Destination type 8	Destination Addr.. 9	Destination 10
allow-dns ✓	UDP	IP address	10.0.0.0/16 ✓	IP address	*	53
	0 selected	IP address	*, 192.168.10.1, 192...	IP address	*, 192.168.10.1, 192...	8080, 8080-

Add **11**

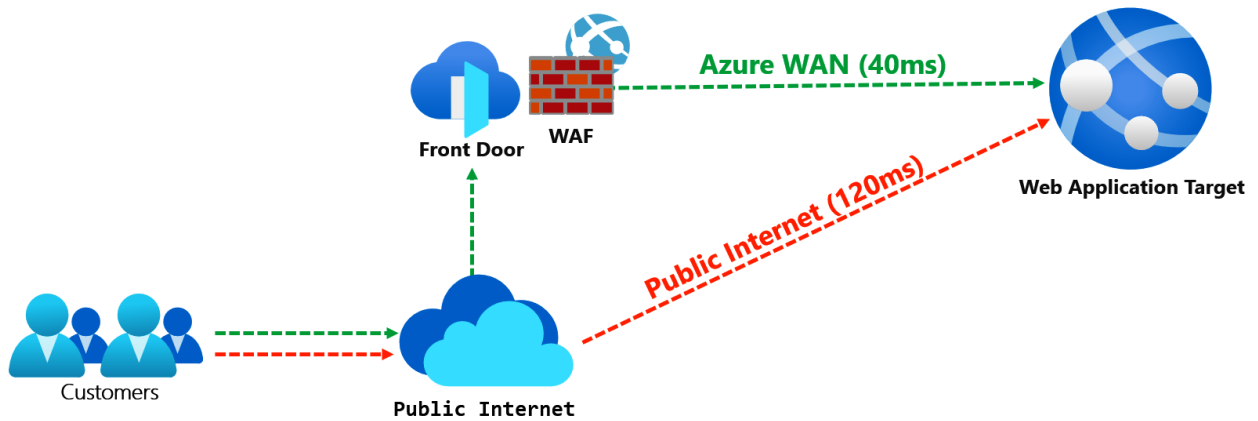
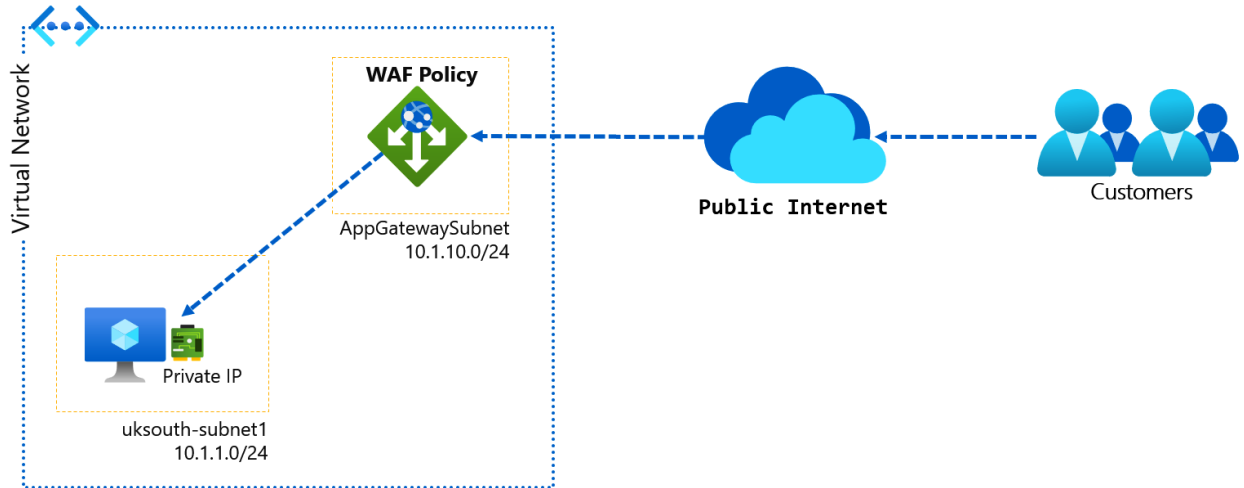


azureadmin@azsecwinvm: ~

```
login as: azureadmin  
azureadmin@10.0.1.4's password:  
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1039-azure x86_64)
```

```
azureadmin@azsecwinvm:~$  
azureadmin@azsecwinvm:~$ curl www.google.com  
HTTP request from 10.0.1.4:43142 to www.google.com:80. Url: www.google.com. Action: Deny. No rule matched. Proceeding with default action  
azureadmin@azsecwinvm:~$
```

```
azureadmin@azsecwinvm:~$  
azureadmin@azsecwinvm:~$ curl www.bing.com  
<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information into action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-sca
```



Home > Virtual networks > azsec-VirtualNetwork

Virtual networks

azureblueteam (Default Directory)

+ New Manage view

Filter for any field...

Name ↑↓

azsec-VirtualNetwork 1

azsec-VirtualNetwork | Subnets

Virtual network

Search (Ctrl+/)

Settings

Address space

Connected devices

Subnets 2

DDoS protection

Firewall

Security

DNS servers

3
+ Subnet + Gateway subnet

Search subnets

Name ↑↓

IPv4

public-subnet

10.0.0.

private-subnet

10.0.1.

Add subnet



Name * 1

AppGwSubnet ✓

Subnet address range * ⓘ 2

10.0.3.0/24

10.0.3.0 - 10.0.3.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

None

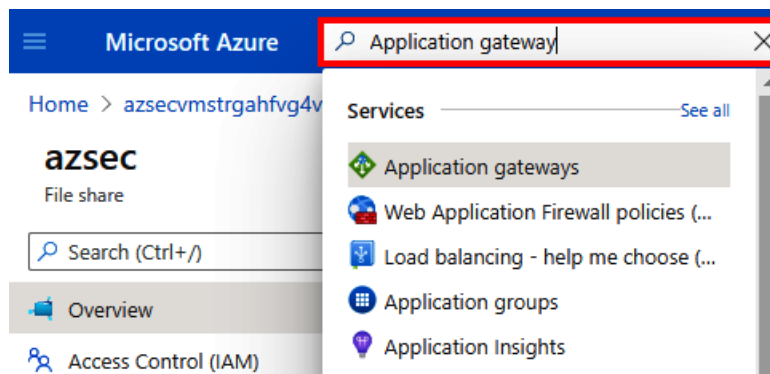
Network security group

None

Route table

None

3
Save Cancel



Create application gateway

your resources.


Subscription * ⓘ	1	AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5443dcab4d8a) ▾
Resource group * ⓘ	2	azuresec-c5-rg ▾ Create new
Instance details		
Application gateway name *	3	azsec-app-gw ✓
Region *	4	UK South ▾
Tier ⓘ	5	WAF V2 ▾
Enable autoscaling	6	<input checked="" type="radio"/> Yes <input type="radio"/> No
Minimum instance count * ⓘ	7	1 ✓
Maximum instance count	8	2 ✓
Firewall status ⓘ		<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled 9
Firewall mode ⓘ		<input type="radio"/> Detection <input checked="" type="radio"/> Prevention 10
Availability zone ⓘ		None ▾
HTTP2 ⓘ	11	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Configure virtual network		
Virtual network * ⓘ	12	azsec-VirtualNetwork ▾ Create new
Subnet * ⓘ	13	AppGwSubnet (10.0.3.0/24) ▾ Manage subnet configuration

Previous

Next : Frontends >

14

Create application gateway

 Changes you make on this tab may affect any configuration you've done on other t

✓ Basics **2 Frontends** ③ Backends ④ Configuration ⑤ Tag

Traffic enters the application gateway via its frontend IP address(es). An application private IP address, or one of each type.

Frontend IP address type ⓘ **1** Public Private Both

Public IP address * **2** (New) azsec-app-gw

[Add new](#)

[Previous](#)

[Next : Backends >](#)

3

[Home](#) > [Application gateways](#) >

Create application gateway

✓ Basics ✓ Frontends **1** **3 Backends** ④ Configuration ⑤ Tags ⑥ Review + create

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, app services, IP addresses, or fully qualified domain names (FQDN).

[Add a backend pool](#) **2**

Backend pool	Targets
No results	

Add a backend pool.



A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name * 1 linux-web-server ✓

Add backend pool without targets Yes 2 No

Backend targets

1 item

Target type 3	Target 4	
Virtual machine	azseclinvn-nic (10.0.1.4)	
IP address or FQDN		

5 Add

Create application gateway

✓ Basics ✓ Frontends 3 Backends 4 Configuration 5 Tags


A backend pool is a collection of resources to which your application gateway can send virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified

[Add a backend pool](#)

Backend pool	Targets
linux-web-server	> 1 target

Next : Configuration >


Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration you haven't already, or edit previous configurations.



Frontends


+ Add a frontend IP

Public: (new) azsec-ap|
aw



Routing rules

+ Add a routing rule



Backend pools

+ Add a backend pool

linux-web-server

Add a routing rule



Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * **1** ✓

2 *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 * ⓘ **3** ✓

Frontend IP * ⓘ **4** ✓

Protocol ⓘ **5** HTTP HTTPS

Port * ⓘ **6** ✓

Additional settings

Listener type ⓘ **7** Basic Multi site

Error page url Yes No **8**

Add a routing rule



Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * ✓

* Listener *** Backend targets** 1

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type 2 Backend pool Redirection

Backend target * ⓘ 3 ✓
[Add new](#)

HTTP settings * ⓘ 4 ✓
[Add new](#)

Add a HTTP setting



[← Discard changes and go back to routing rules](#)

HTTP settings name * 1 ✓

Backend protocol HTTP HTTPS

Backend port *

Additional settings

Cookie-based affinity ⓘ Enable Disable

Connection draining ⓘ Enable Disable

Request time-out (seconds) * ⓘ




Add 2

Create application gateway



- ✓ Basics
- ✓ Frontends
- ✓ Backends
- 4 Configuration**
- 5 Tags
- 6 Review + create

Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration if you haven't already, or edit previous configurations.

 Frontends + Add a frontend IP Public: (new) azsec-apj gw ◀ ▶	 Routing rules + Add a routing rule webapp-http-rule ◀ ▶ Manage HTTP settings	 Backend pools + Add a backend pool linux-web-server ◀ ▶
--	--	--

- Previous
- Next : Tags >**

Create application gateway

✓ Validation passed

- ✓ Basics
- ✓ Frontends
- ✓ Backends
- ✓ Configuration
- ✓ Tags
- 6 Review + create**

Basics

Subscription	AzureBlueTeam-PROD
Resource group	azuresec-c5-rg
Name	azsec-app-gw
Region	UK South
Tier	WAF_v2
Enable autoscaling	Enabled

- Create**
- Previous
- Next
- [Download a template for automation](#)

✔ Your deployment is complete

Deployment name: Microsoft.ApplicationGateway-20210209005148
Subscription: AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5...
Resource group: azuresec-c5-rg

∨ Deployment details (Download)

∧ Next steps

[Go to resource group](#)

azsec-app-gw Application gateway

Search (Ctrl+)

Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Web application firewall

Essentials

JSON View

Resource group (change)	: azuresec-c5-rg
Location	: UK South
Subscription (change)	: AzureBlueTeam-PROD
Subscription ID	: 32d25af6-ccc1-4942-bdb7-5443dcab4d8a
Virtual network/subnet	: azsec-VirtualNetwork/AppGwSubnet
Frontend public IP address	: 51.11.42.50 (azsec-app-gw)
Frontend private IP address	: -
Tier	: WAF V2

→ ↻ ⚠ Not secure 51.11.42.50 📄 ⭐ 🔴 ⚙️ 🏠 InPrivate



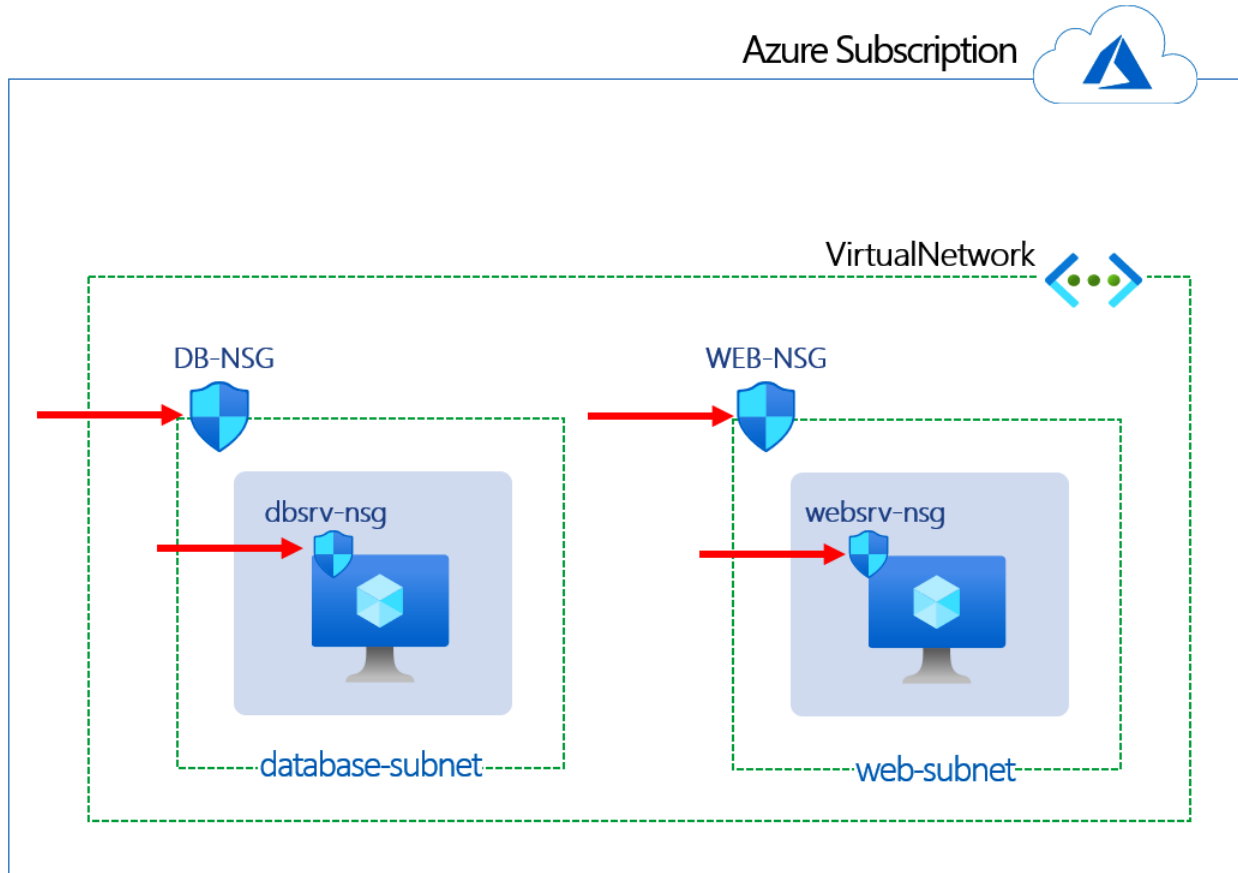
ubuntu

Apache2 Ubuntu Default Page

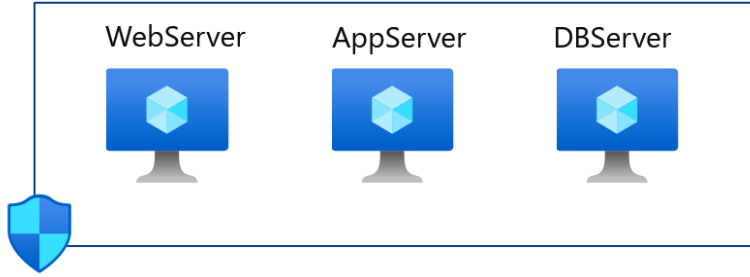
It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`)

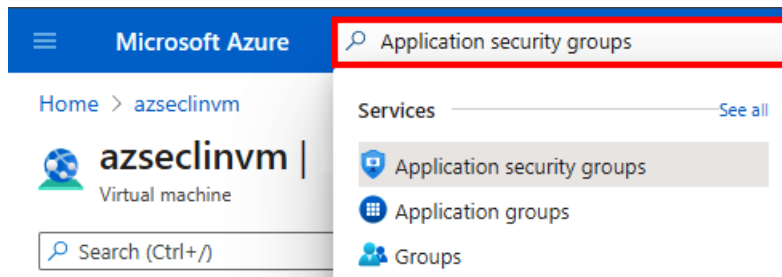
Chapter 7: Implementing Network Security



Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
▼ Inbound Security Rules						
100	nsgRule1	3389	Tcp	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
▼ Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny



	NAME	SOURCE	DESTINATION	PORT
Allow	Allow-Web-to-App	WebServer	AppServer	8080
Allow	Allow-App-to-DB	AppServer	DBServer	3308 (MySQL)



Create an application security group

Basics | Tags | Review + create

Project details

Subscription * 1 AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5443dcab4d8a) ✓

Resource group * 2 azuresec-c5-rg ✓
[Create new](#)

Instance details

Name * 3 web-server-asg ✓

Region * 4 (Europe) UK South ✓

Review + create 5 | < Previous | Next : Tags > | [Download a template for automation](#)

Microsoft Azure

azseclinv

Home >

Microsoft.Ap
Deployment

Search (Ctrl+)

Overview

Inputs

Services

No results were found.

Resources

- azseclinv Virtual machine
- azseclinv-nic Network interface
- azseclinv_OsDisk_1_f76108fcf9774d... Disk

azseclinv | Networking

Virtual machine

Search (Ctrl+)

Attach network interface Detach network interface

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings 1

- Networking 2
- Connect
- Disks
- Size

azseclinv-nic

IP configuration ⓘ

ipconfig1 (Primary)

Network Interface: azseclinv-nic Effective security rules Topology

Virtual network/subnet: azsec-VirtualNetwork/private-subnet NIC Public IP: -

Inbound port rules Outbound port rules Application security groups 3

Configure the application security groups

azseclinv-nic

IP configuration ⓘ

ipconfig1 (Primary)

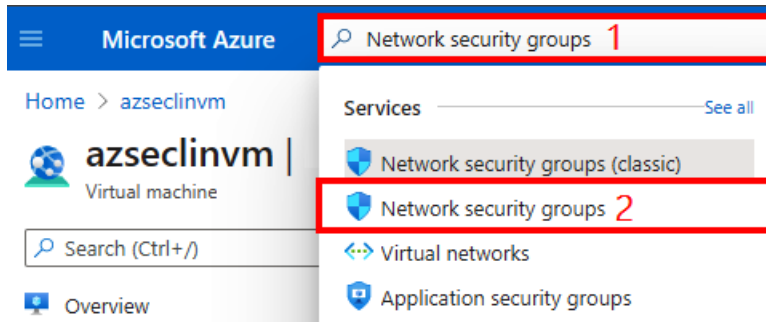
Network Interface: azseclinv-nic Effective security rules Topology

Virtual network/subnet: azsec-VirtualNetwork/private-subnet NIC Public IP: - NIC Private IP: 10.0.1.4
Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

web-server-asg

Configure the application security groups



Create network security group

Basics Tags Review + create

Project details

Subscription * 1 AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5443dcab4d8a) ▾

Resource group * 2 azuresec-c5-rg ▾
[Create new](#)

Instance details

Name * 3 private-vm-nsg ✓

Region * 4 (Europe) UK South ▾

Review + create 5 < Previous Next : Tags > [Download a template for automation](#)

private-vm-nsg | Inbound security rules

Network security group

Search (Ctrl+*/*)

<< 2

+ Add

Default rules

Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Inbound security rules 1
- Outbound security rules
- Network interfaces

Priority	Name
65000	AllowVnetInBound
65001	AllowAzureLoadBalanc...
65500	DenyAllInBound



Add inbound security rule



private-vm-nsg



Basic

Source * ⓘ 1

Source port ranges * ⓘ 2

Destination * ⓘ 3

Destination application security group * ⓘ 4

Destination port ranges * ⓘ 5

Protocol * 6

Any **TCP** UDP ICMP

Action * 7

Allow Deny

Priority * ⓘ 8

Name * 9

Description 10

Add 11

private-vm-nsg | Network interfaces

Network security group

Search (Ctrl+/) << + Associate 2

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces 1**
- Subnets

Search network interfaces

Name	↑↓
No results.	

Associate network interface

i Choose a network interface to associate with this network security group

i These are the network interfaces in the selected subscription and location 'UK South'.

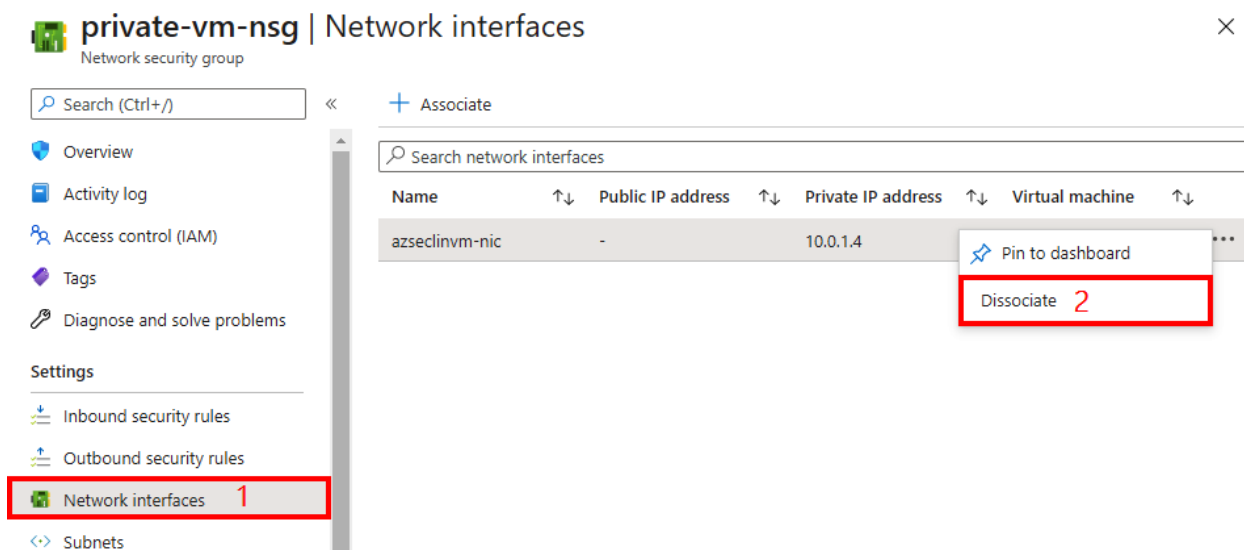
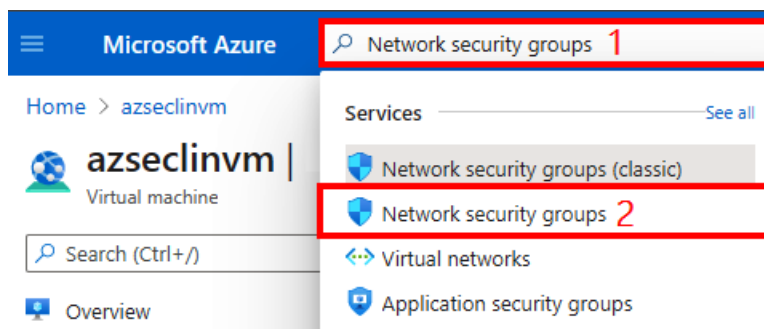
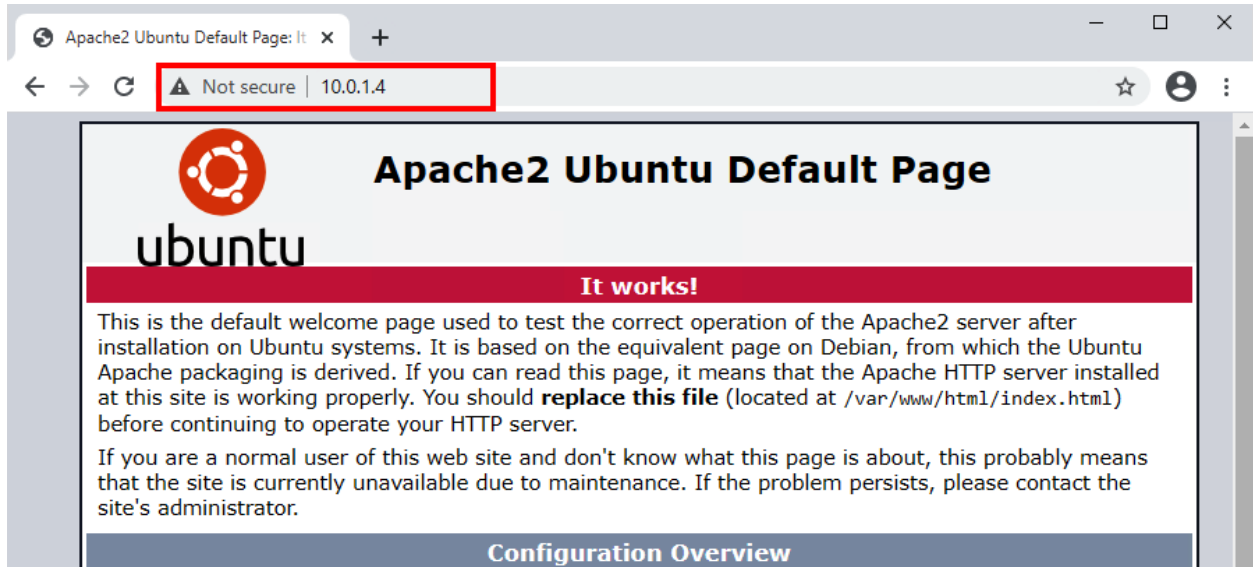
- azseclinvm-nic**
azuresec-c5-rg
- azsecwinvm-nic
azuresec-c5-rg

Settings

putty 10.0.1.4 2

1

Windows taskbar with icons for search, task view, Edge, and File Explorer.



Allow access from

- All networks Selected networks

i Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address
No network selected.		

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#)

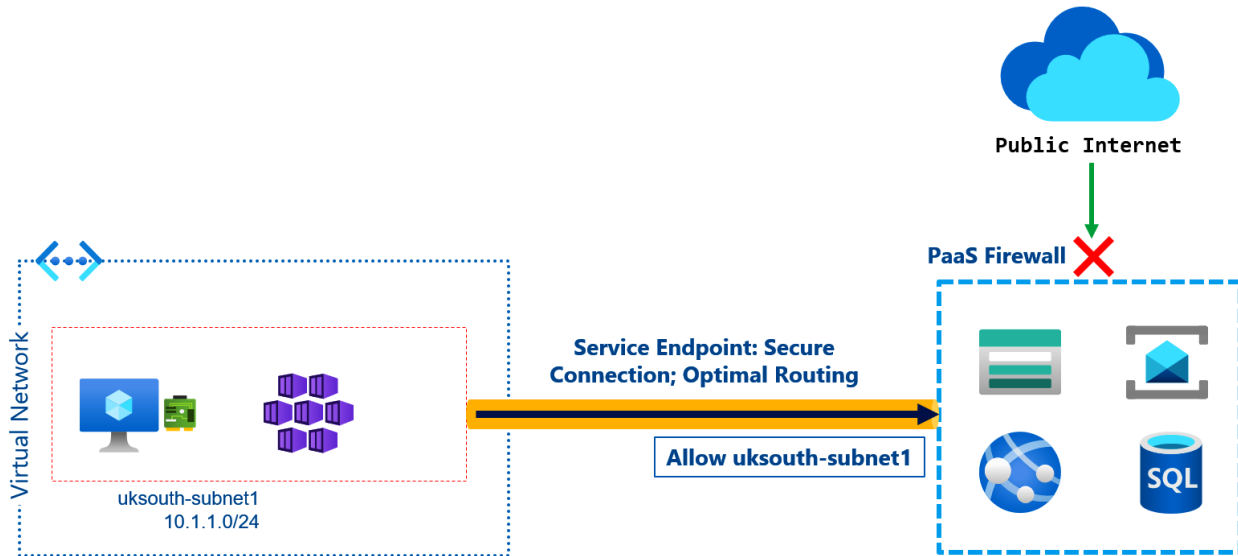
Add your client IP address ('109.145.121.23') **i**

Address range

1.1.1.1	
2.2.2.2	 
<input type="text" value="IP address or CIDR"/>	

Exceptions

- Allow trusted Microsoft services to access this storage account **i**
- Allow read access to storage logging from any network
- Allow read access to storage metrics from any network



Microsoft Azure

Search: azsecvmstrg

Home > private-vm-nsg

private-vm-n
Network security group

Search (Ctrl+)

Overview

Services: No results were found.

Resources: azsecvmstrgahfvg4vhezzem Storage account

azsecvmstrgahfvg4vhezzem | File shares

Storage account

Search (Ctrl+)

Azure CDN

Add Azure Search

File service

File shares 1

Table service

Tables

Queue service

File share Refresh

File share settings

Active Directory: Not configured Soft

Search file shares by prefix (case-sensitive)

Name: azsec 2

azsec

File share

Search (Ctrl+/) <<

1 Connect ↑ U

Overview

Access Control (IAM)

Settings

Properties

Operations

Snapshots

Backup

Search files by pre

Name

No files found.

Connect

azsec

⚠ 'Secure transfer required' is enabled on the storage account. SMB clients must support 3.0 encryption to connect. Additionally, your storage account is secured to a specific set of supported networks. When firewall rules are configured, only applications requesting data over the specified set of networks can access a storage account. Click here to learn more about connecting Azure files.

Windows **2** Linux macOS

Mount point

azsec

To connect to this file share from a Linux computer, run this command:

3

```
sudo mkdir /mnt/azsec
if [ ! -d "/etc/smbcredentials" ]; then
sudo mkdir /etc/smbcredentials
fi
if [ ! -f "/etc/smbcredentials/azsecvmstrgahfvg4vhezzem.cred" ]; then
sudo bash -c 'echo "username=azsecvmstrgahfvg4vhezzem" >>
/etc/smbcredentials/azsecvmstrgahfvg4vhezzem.cred'
```

Copy this information

Storage accounts

azureblueteam (Default Directory)

+ New ⚙ Manage view ⌵ ...

Filter for any field...

Name ↑↓

1 azsecvmstrgahfvg4vhezzem ...

azsecvmstrgahfvg4vhezzem | Networking

Storage account

Search (Ctrl+/) <<

Save ✕ Discard ↻ Refresh

LUKS

Configuration

Encryption

Shared access signature

2 Networking

Security

Properties

Locks

Blob service

Containers

📘 Firewall settings allowing access to stor

Allow access from **3**

All networks

Selected networks

📘 Configure network security for your stor

Virtual networks

4 + Add existing virtual network + Ad

Virtual Network

Subnet

No network selected.

Add networks



Subscription *

1

AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5443dca... ▾

Virtual networks * ⓘ

2

azsec-VirtualNetwork ▾

Subnets *

3

private-subnet (Service endpoint required) ▾

i The following networks don't have service endpoints enabled for 'Microsoft.Storage'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait.

Virtual network	Service endpoint status
▾ azsec-VirtualNetw...	...
private-subnet	Not enabled ...

4

Enable

Add networks



Subscription *

AzureBlueTeam-PROD (32d25af6-ccc1-4942-bdb7-5443dca...

Virtual networks *

azsec-VirtualNetwork

Subnets *

private-subnet

Enabling selected networks with service endpoints for 'Microsoft.Storage' is complete.

Virtual network	Service endpoint status	
azsec-VirtualNetw...		...
private-subnet	Enabled	...

azsecvmstrgahfvfg4vhezzem | Networking

Storage account

Search (Ctrl+)

Save Discard Refresh

- LUKS
- Configuration
- Encryption
- Shared access signature
- Networking
- Security
- Properties
- Locks
- Blob service
- Containers
- Custom domain

Firewall settings allowing access to storage services will remain in effect for up to a minute after

Allow access from
 All networks Selected networks

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status
azsec-VirtualNetwo...	1		
	private-subnet	10.0.1.0/24	✓ Enabled

51.140.30.255 - Remote Desktop Connection

```
azureadmin@azseclinvm: ~  
azureadmin@azseclinvm:~$ sudo df -Th  
Filesystem      Type      Size  Used Avail Use% Mounted on  
udev            devtmpfs  3.9G   0    3.9G  0% /dev  
tmpfs           tmpfs     797M  664K  796M  1% /run  
/dev/sdb1      ext4      29G   1.4G   28G   5% /  
tmpfs           tmpfs     3.9G   0    3.9G  0% /dev/shm  
tmpfs           tmpfs     5.0M   0    5.0M  0% /run/lock  
tmpfs           tmpfs     3.9G   0    3.9G  0% /sys/fs/cgroup  
/dev/sdb15     vfat     105M   3.7M  101M  4% /boot/efi  
/dev/sdal      ext4      16G   45M   15G   1% /mnt  
tmpfs           tmpfs     797M   0    797M  0% /run/user/1000  
azureadmin@azseclinvm:~$
```

```

sudo mkdir /mnt/azsec
if [ ! -d "/etc/smbcredentials" ]; then
sudo mkdir /etc/smbcredentials
fi
if [ ! -f "/etc/smbcredentials/azsecvmstrgahfvg4vhezzem.cred" ]; then
sudo bash -c 'echo "username=azsecvmstrgahfvg4vhezzem" >> /etc/smbcredentials/azsecvmstrgahfvg4vhezzem.cred'
sudo bash -c 'echo "password=deobh44cwqKsr8XtXPt0oPoa54sfffQ37FDic7jxFQBJQ2EsrnqiT4a36VeDt0Bn1KVUIxhDZYduw0AeGmG72g==" >>
/etc/smbcredentials/azsecvmstrgahfvg4vhezzem.cred'
fi
sudo chmod 600 /etc/smbcredentials/azsecvmstrgahfvg4vhezzem.cred

sudo bash -c 'echo "//azsecvmstrgahfvg4vhezzem.file.core.windows.net/azsec /mnt/azsec cifs
nofail,vers=3.0,credentials=/etc/smbcredentials/azsecvmstrgahfvg4vhezzem.cred,dir_mode=0777,file_mode=0777,serverino" >> /etc/fstab'
sudo mount -t cifs //azsecvmstrgahfvg4vhezzem.file.core.windows.net/azsec /mnt/azsec -o
vers=3.0,credentials=/etc/smbcredentials/azsecvmstrgahfvg4vhezzem.cred,dir_mode=0777,file_mode=0777,serverino

```

```

51.140.30.255 - Remote Desktop Connection
azureadmin@azseclinvm: ~
azureadmin@azseclinvm:~$ sudo df -Th
Filesystem                                Type      Size  Used Avail Use% Mounted on
udev                                       devtmpfs  3.9G   0    3.9G   0% /dev
tmpfs                                       tmpfs     797M  664K  796M   1% /run
/dev/sdb1                                  ext4      29G   1.4G   28G    5% /
tmpfs                                       tmpfs     3.9G   0    3.9G   0% /dev/shm
tmpfs                                       tmpfs     5.0M   0    5.0M   0% /run/lock
tmpfs                                       tmpfs     3.9G   0    3.9G   0% /sys/fs/cgroup
/dev/sdb15                                 vfat     105M   3.7M  101M   4% /boot/efi
/dev/sdal                                  ext4      16G   45M   15G    1% /mnt
tmpfs                                       tmpfs     797M   0    797M   0% /run/user/1000
//azsecvmstrgahfvg4vhezzem.file.core.windows.net/azsec cifs     5.0T   0    5.0T   0% /mnt/azsec
azureadmin@azseclinvm:~$

```

Home > Storage accounts > azsecvmstrgahfvg4vhezzem

Storage accounts

azureblueteam (Default Directory)

+ New ⚙️ Manage view ∨ ⋮

Filter for any field...

Name ↑↓

azsecvmstrgahfvg4vhezzem 1 ⋮

azsecvmstrgahfvg4vhezzem | File shares

Storage account

🔍 Search (Ctrl+/)

+ File share 🔄 Refresh

🛡️ Data protection

☁️ Azure CDN

🔍 Add Azure Search

File service

📁 File shares 2

Table service

📊 Tables

File share settings

Active Directory: Not configured

🔍 Search file shares by prefix (case-se

Name

📁 azsec 3



This machine doesn't seem to have access.

This storage account is located in a VNET.

Recent changes to "Firewalls and virtual networks" settings may not be in effect yet. If you expect this machine to be able to connect to the content of this file share, check that this machine is a part of the VNET or try waiting a few minutes for changes in settings to take effect, and then refresh this page.

[Learn more](#)

Summary

Session ID
2aecdcca799141198493cd690603a468

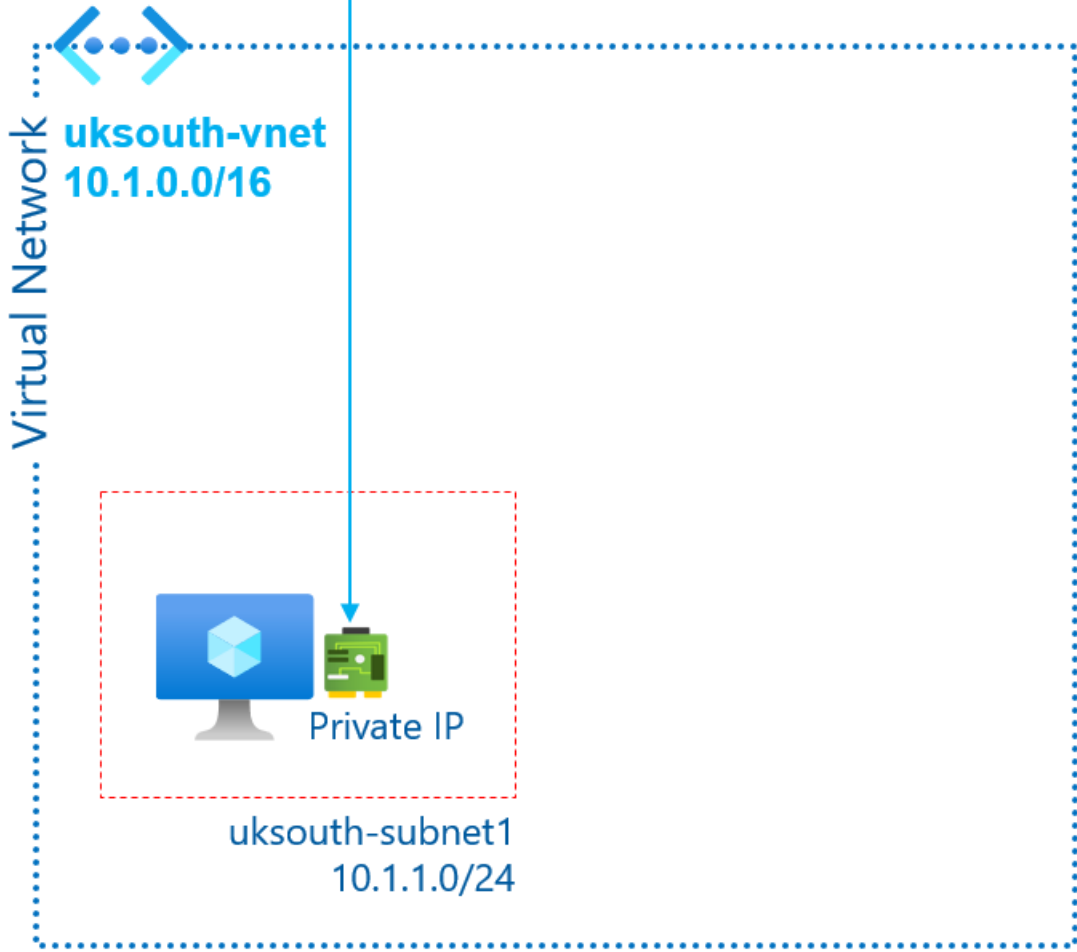
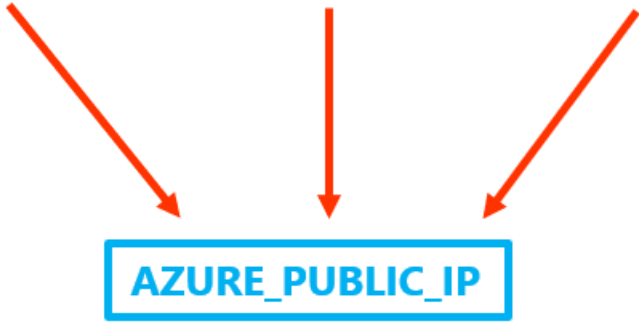
Resource ID
/subscriptions/32d25af6-ccc1-4942-bdb7-5443dcab4d8...

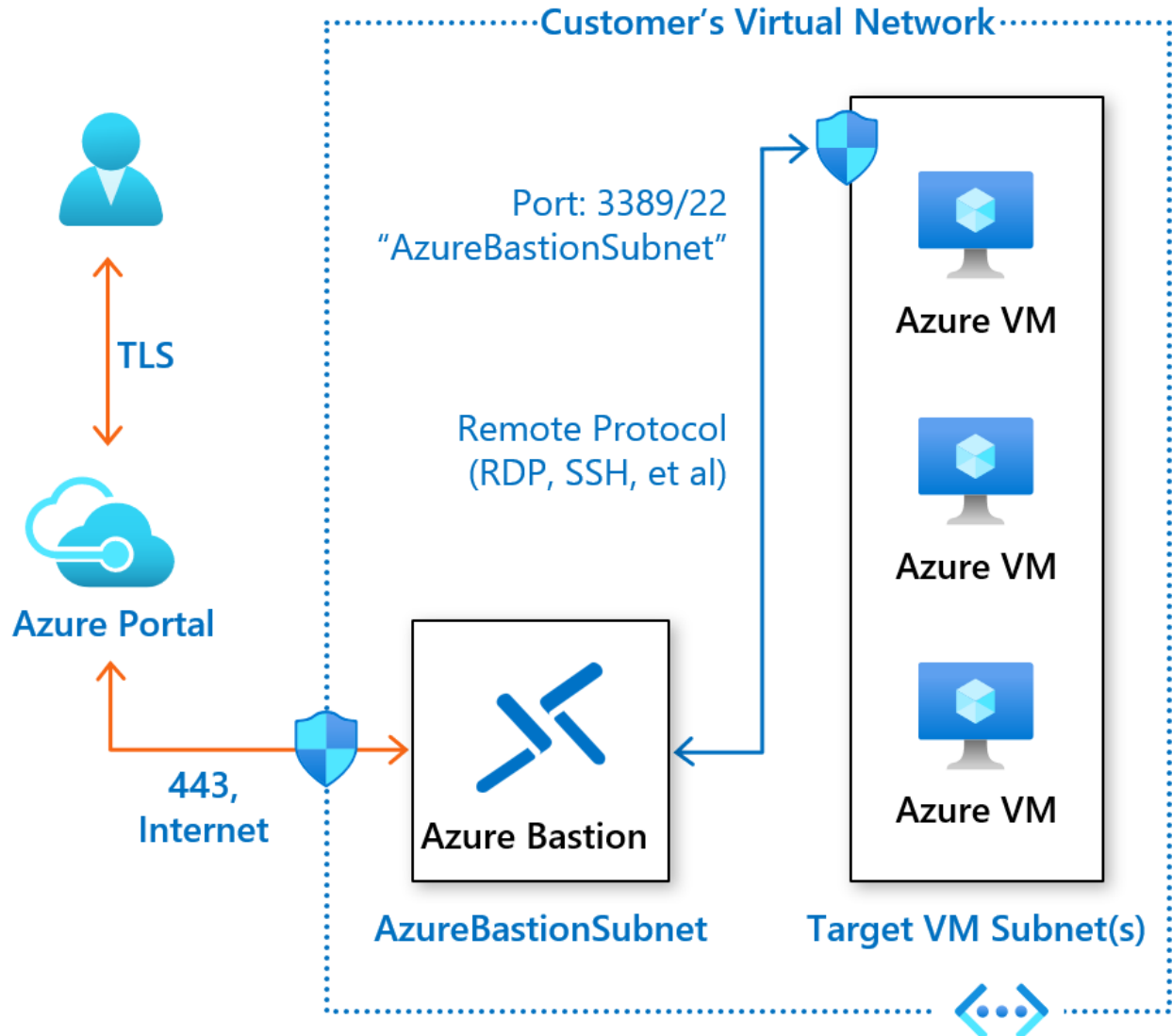
Extension
Microsoft_Azure_FileStorage

Content
FilesGridBladev2

Error code
403

Port Scan **Vulnerability Scan** **Brute Force Attacks**





Virtual networks

azureblueteam (Default Directory)

+ New Manage view ...

Filter for any field...

Name ↑↓

azsec-VirtualNetwork

azsec-VirtualNetwork | Subnets

Virtual network

Search (Ctrl+)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

+ Subnet

+ Gateway subnet

Refresh

Search subnets

Name ↑↓

IPv4 ↑↓

public-subnet 10.0.0.0/24 (250 availa...

AzureFirewallSubnet 10.0.2.0/24 (250 availa...

private-subnet 10.0.1.0/24 (250 availa...

AppGwSubnet 10.0.3.0/24 (250 availa...

Add subnet

×

Name * 1

AzureBastionSubnet

Subnet address range * 2

10.0.4.0/24

10.0.4.0 - 10.0.4.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space

NAT gateway

None

Network security group

None

Route table

None

Save

Cancel

Virtual machines


azureblueteam (Default Directory)


+ Add ▾ ⌚ Reservations ▾ ⋮

i Try the new virtual machine resource browser! This experience is faster and has improved sorting and filtering capabilities. Please note that the new experience will not show classic virtual machines and does not include support for some columns such as maintenance status.

Filter by name...

Name ↑↓






 azseclinvm ⋮

 azsecwinvm **1** ⋮







azsecwinvm | Connect

Virtual machine

🔍 Search (Ctrl+/) <<

-  Overview
-  Activity log
-  Access control (IAM)
-  Tags
-  Diagnose and solve problems

Settings

-  Networking
-  **Connect** **2**
-  Disks
-  Size
-  Security
-  Advisor recommendations

⚠ To improve security, enable just-in-time access on this VM. →

RDP SSH **BASTION** **3**

i Bastion is an Azure service that allows fast, secure connections to an

Use Bastion **4**

Name * 1
azsec-VirtualNetwork-bastion ✓

Virtual network ⓘ
azsec-VirtualNetwork

Subnet * 2
AzureBastionSubnet ✓
[Manage subnet configuration](#)

Public IP address

Public IP address * 3 ⓘ
 Create new Use existing

Public IP address name * 4
azsec-VirtualNetwork-ip ✓

Public IP address SKU
Standard

Assignment
 Dynamic Static

Resource group * ⓘ
azuresec-c5-rg ✓
[Create new](#)

Create 5



Connect using Azure Bastion

Azure Bastion Service enables you to securely and seamlessly RDP & SSH to your VMs in your Azure virtual network, without exposing a public IP on the VM, directly from the Azure portal, without the need of any additional client/agent or any piece of software. [Learn more about Azure Bastion.](#)

Using Bastion: **azsec-VirtualNetwork-bastion**, Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Open in new window

Username * ⓘ

azureadmin ✓

Password * ⓘ

..... ✓

Connect



Microsoft Azure

Resource groups

Azure services

- Create a resource
- Virtual networks

Services [See all](#)

- Resource groups
- Subscriptions
- Resource Graph Explorer
- Resource Graph queries

Resource groups

azureblueteam (Default Directory)

[+](#) New [⚙️](#) Manage view [↻](#) Refresh [↓](#) Export to CSV [🔗](#) Open query | [📄](#) Assign

Filter for any field... Subscription == **AzureBlueTeam-PROD** Location == **all** ✕

Showing 1 to 2 of 2 records.

<input type="checkbox"/>	Name ↑↓	Subscription ↑↓	Location ↑↓
<input type="checkbox"/>	azuresec-c6-rg	AzureBlueTeam-PROD	UK South
<input type="checkbox"/>	NetworkWatcherRG	AzureBlueTeam-PROD	UK South

...

+ Add Edit columns **Delete resource group**

1

Essentials

Subscription (change)
AzureBlueTeam-PROD

Subscription ID
1c63ad39-68ee-444a-90a8-a2ccaf67f671

Tags (change)
Click here to add tags

Filter for any field... Type == all Location

Showing 1 to 10 of 10 records. Show hidden types

Name Type

< Previous Page 1 of 1 Next >

Are you sure you want to delete



Warning! Deleting the "azuresec-c6-rg" resource group you're about to take can't be undone. Going further will group and all the resources in it permanently.

TYPE THE RESOURCE GROUP NAME:

2 azuresec-c6-rg

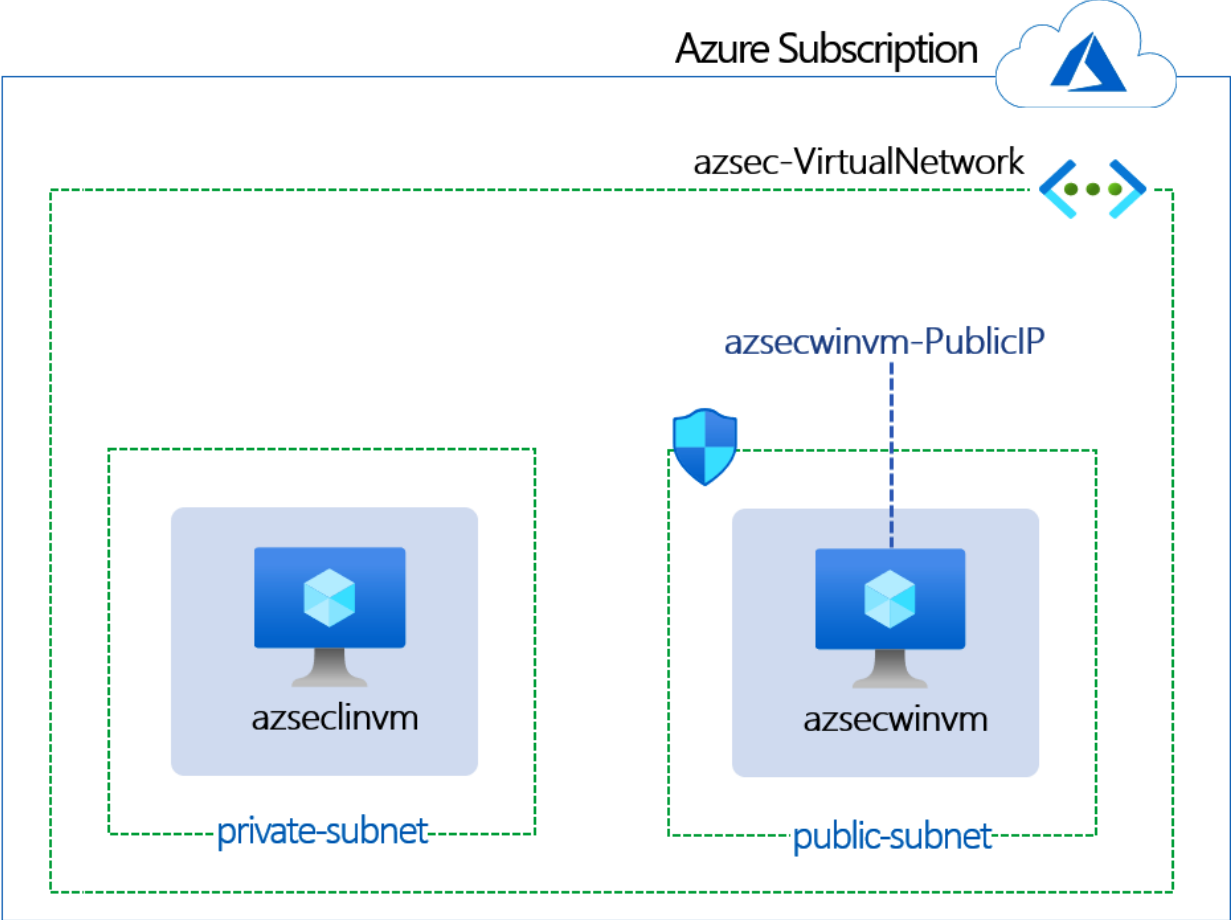
AFFECTED RESOURCES

There are 12 resources in this resource group that will be deleted.

Name	Type
azseclinv	Virtual machine
apacheinstall (azseclinv/ap...	Microsoft.Compute...
azseclinv_OsDisk_1_8b2f0f0...	Disk

3 Delete Cancel

Chapter 8: Implementing Host Security



Azure Security Engineer Book - Chapter 6



Deploy to Azure



Visualize

Windows VM

- Windows Server 2019 Datacenter
- Putty
- Google Chrome

Linux VM

- Ubuntu 18.04



Sign in

to continue to Microsoft Azure

No account? [Create one!](#)

[Can't access your account?](#)

[Sign in with a security key](#) 

Next

Custom deployment ...

Deploy from a custom template

manage all your resources.

Subscription * ⓘ

1 AzureBlueTeam-PROD (a50ed1ee-5ea2-4719-8652-030a06b805df) ▼

Resource group * ⓘ

2 (New) azuresec-c6-rg ▼

[Create new](#)

Parameters

Region * ⓘ

3 UK South ▼

Storagename ⓘ

[concat('azsecvmstrg', uniqueString(resourceGroup().id))]

Vm-dns ⓘ

[concat('azsecwinvm-', uniqueString(resourceGroup().id))]

Admin User ⓘ

azureadmin ✓

Admin Password * ⓘ

4 ✓

Vmsize * ⓘ

1x Standard B2ms
2 vcpus, 8 GB memory
[Change size](#)

Location ⓘ

[resourceGroup().location]

_artifacts Location ⓘ

[deployment().properties.templateLink.uri]


5 [Review + create](#)

[< Previous](#)

[Next : Review + create >](#)


Custom deployment

Deploy from a custom template

 Validation Passed

Basics Review + create

Summary

 Customized template
9 resources

Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)









By clicking "Create," I (a) agree to the applicable legal terms associated

Create

< Previous

Next

[Download a template for automation](#)

 <p>CIS Microsoft Windows Server 2016 Benchmark L1 By Center For Internet Security, Inc. Hardened according to a CIS Benchmark - the consensus-based best practice for secure</p> <p>★★★★★ (1) Software plans start at US\$0.02/hour</p> <p>Get it now</p>	 <p>CIS Microsoft Windows Server 2016 Benchmark L2 By Center For Internet Security, Inc. Hardened according to a CIS Benchmark - the consensus-based best practice for secure</p> <p>Software plans start at US\$0.02/hour</p> <p>Get it now</p>	 <p>CIS Ubuntu Linux 20.04 LTS Benchmark L1 By Center For Internet Security, Inc. Hardened according to a CIS Benchmark - the consensus-based best practice for secure</p> <p>Software plans start at US\$0.015/hour</p> <p>Get it now</p>	 <p>CIS Debian Linux 10 Benchmark L1 By Center For Internet Security, Inc. Hardened according to a CIS Benchmark - the consensus-based best practice for secure</p> <p>Software plans start at US\$0.02/hour</p> <p>Get it now</p>
 <p>CIS Microsoft Windows Server 2012 Benchmark L2 By Center For Internet Security, Inc. Hardened according to a CIS Benchmark - the consensus-based best practice for secure</p> <p>Software plans start at US\$0.02/hour</p> <p>Get it now</p>	 <p>CIS Ubuntu Linux 16.04 LTS Benchmark L1 By Center For Internet Security, Inc. Hardened according to a CIS Benchmark - the consensus-based best practice for secure</p> <p>Software plans start at US\$0.02/hour</p> <p>Get it now</p>	 <p>CIS Debian Linux 9 Benchmark L1 By Center For Internet Security, Inc. Hardened according to a CIS Benchmark - the consensus-based best practice for secure</p> <p>Software plans start at US\$0.02/hour</p> <p>Get it now</p>	 <p>CIS SUSE Linux 15 Benchmark L1 By Center For Internet Security, Inc. Hardened according to a CIS Benchmark - the consensus-based best practice for secure</p> <p>Software plans start at US\$0.015/hour</p> <p>Get it now</p>

Approved VM images

This policy requires that only approved custom images are deployed in your environment. You specify an array of approved image IDs.

Azure Policy Docs

See more information and a complete walk-through of using this sample on docs.microsoft.com.

Try with Azure portal



Microsoft Antimalware Extension



Windows Server 2019

+ Policy definition + Initiative definition Export definitions Refresh

Scope	Definition type	Type
AzureBlueTeam-PROD	All definition types	All types

Now export your definitions and assignments to GitHub and manage them using actions! Click on 'Export definition'

Name
Deploy default Microsoft IaaSAntimalware extension for Windows Server
Microsoft IaaSAntimalware extension should be deployed on Windows servers
Microsoft Antimalware for Azure should be configured to automatically update protection signatures

Microsoft Azure

azsecwinvm

Azure services

Create a resource

More services

Services

No results were found.

Resources

azsecwinvm	Virtual machine
azsecwinvm-nic	Network interface
azsecwinvm-nsg	Network security group
azsecwinvm-PublicIP	Public IP address

azsecwinvm | Extensions

Virtual machine

Search (Ctrl+ /)

Size

Security

Advisor recommendations 1

Extensions

Continuous delivery

+ Add 2

Search to filter items...

Name	Type
No resource extensions found.	

New resource ...



Azure Performance Diagnostics
Microsoft Corp.



Application Insights Agent (.NET Preview)
Microsoft Corp.



Microsoft Antimalware
Microsoft Corp.



AMD GPU Driver Extension
Microsoft Corp.

Microsoft Antimalware ...



Microsoft Corp.

Microsoft Antimalware for Azure Virtual Machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your system. The solution can be enabled and configured from the Azure Portal, Service Management REST API, and Microsoft Azure PowerShell SDK cmdlets.

To **enable** antimalware with the **default configuration**, click **Create** on the Add Extension blade without inputting any configuration setting values.

To **enable** antimalware with a **custom configuration**, input the supported values for the configuration settings provided on the **Add Extension** blade and click **Create**. Please refer to the **tooltips** provided with each configuration setting on the Add Extension blade to see the supported configuration values.

To **enable antimalware event collection** for a virtual machine, click any part of the **Monitoring lens** in the virtual machine blade, click **Diagnostics** command on Metric blade, select **Status ON** and check **Windows Event system logs**. The antimalware events are

Create

Install extension ...



Real-time protection ⓘ

Enable Disable

Run a scheduled scan ⓘ

Enable Disable

Scan type ⓘ

Quick Full

Scan day ⓘ

Saturday

Scan time ⓘ

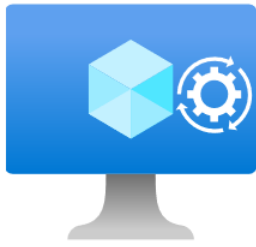
120

+ Add

Search to filter items...

Name	↑↓	Type	↑↓	Version	↑↓	Status	↑↓
laaSAntimalware		Microsoft.Azure.Security.IaaSAntimalware		1.*		Provisioning succeeded	...

Enable Update Management



Azure VM

Report Status



Log Analytics

Deploy Update



Automation Account





Microsoft Azure

log analytics workspace

Azure services


Create a resource

Services [See all](#)

-  Log Analytics workspaces
-  Activity log
-  Log Analytics query packs
-  Workspaces

Log Analytics workspaces

azureblueteam (Default Directory)

+ New Open recycle bin Manage view Refresh

Filter for any field...

Subscription == **AzureBlueTeam-PROD**

Showing 0 to 0 of 0 records.

Create Log Analytics workspace

Project details

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

Subscription * ⓘ 1 AzureBlueTeam-PROD (a50ed1ee-5ea2-4719-8652-030a06b805df) ▼

Resource group * ⓘ 2 azuresec-c6-rg ▼

[Create new](#)

Instance details

Name * ⓘ 3 update-mgmt-workspace ✓

Region * ⓘ 4 UK South ▼

5 Review + Create << Previous Next : Pricing tier >

Microsoft Azure

automation accounts

>

Microsoft.Log

Deployment

arch (Ctrl+)

Services [See all](#)

- Automation Accounts
- Storage accounts
- Integration accounts

Add Automation Account ...

Name * ⓘ

update-mgmt-aac ✓ 1

Subscription *

AzureBlueTeam-PROD (a50ed1ee-5ea2... ▾ 2

Resource group *

azuresec-c6-rg ▾ 3

[Create new](#)

Location *

UK South ▾ 4

5 Create Azure Run As account * ⓘ

Yes No

6

Microsoft Azure

virtual machines

Automation Accounts

Virtual machines

Virtual machines (classic)

SQL virtual machines

Virtual machines

azureblueteam (Default Directory)

+ Add Switch to classic Reservations Manage view Refresh Export to CSV Open query

Filter for any field... Subscription == AzureBlueTeam-PROD Resource group == all Location

Showing 1 to 2 of 2 records.

Name	Subscription	Resource group	Location	Status
azsecinvm	AzureBlueTeam-PROD	azuresec-c6-rg	UK South	Running
azsecwinvm	AzureBlueTeam-PROD	AZURESEC-C6-RG	UK South	Running

- Assign tags
- Start
- Restart
- Stop
- Delete
- Services
- Maintenance
- Feedback
- Leave preview

Enable Update Management ...



Update Management

Enable consistent control and compliance of these virtual machines with Update Management.

Configuration (used when enabling new VMs) ⓘ

AUTO: Auto-configure Log Analytics workspace and Automation account based on VMs subscription and location

CUSTOM: Choose existing Log Analytics workspace and Automation account

1

Log Analytics workspace: DefaultWorkspace-a50ed1ee-5ea2-4719-8652-030a06b805df-SUK [\(change\)](#)

Automation account: Automate-a50ed1ee-5ea2-4719-8652-030a06b805df-SUK

2

Summary

Ready to enable ⓘ

2 →

Already enabled ⓘ

0 ✓

Cannot enable ⓘ

0 ⚡

Custom Configuration



1
AzureBlueTeam-PROD (a50ed1ee-5ea2-4719-8652-030a06b805df)

Location ⓘ 2
UK South

Workspace 3
update-mgmt-workspace

⊗ The workspace is not yet linked to an Automation account. Select the account to link below.
Note: at this time linked account for this workspace must be from **UK South**.

Automation account Subscription 4
AzureBlueTeam-PROD (a50ed1ee-5ea2-4719-8652-030a06b805df)

Location ⓘ
UK South

Account 5
update-mgmt-aac

6

Enable Update Management ...



Update Management

Enable consistent control and compliance of these virtual machines with Update Management.

CUSTOM: Choose existing Log Analytics workspace and Automation account

Log Analytics workspace: update-mgmt-workspace ([change](#))
Automation account: update-mgmt-aac

Summary

Ready to enable ⓘ Already enabled ⓘ Cannot enable ⓘ

2 →

0 ✓

0 -

Name ↑↓ Update Managem...↑↓ Details

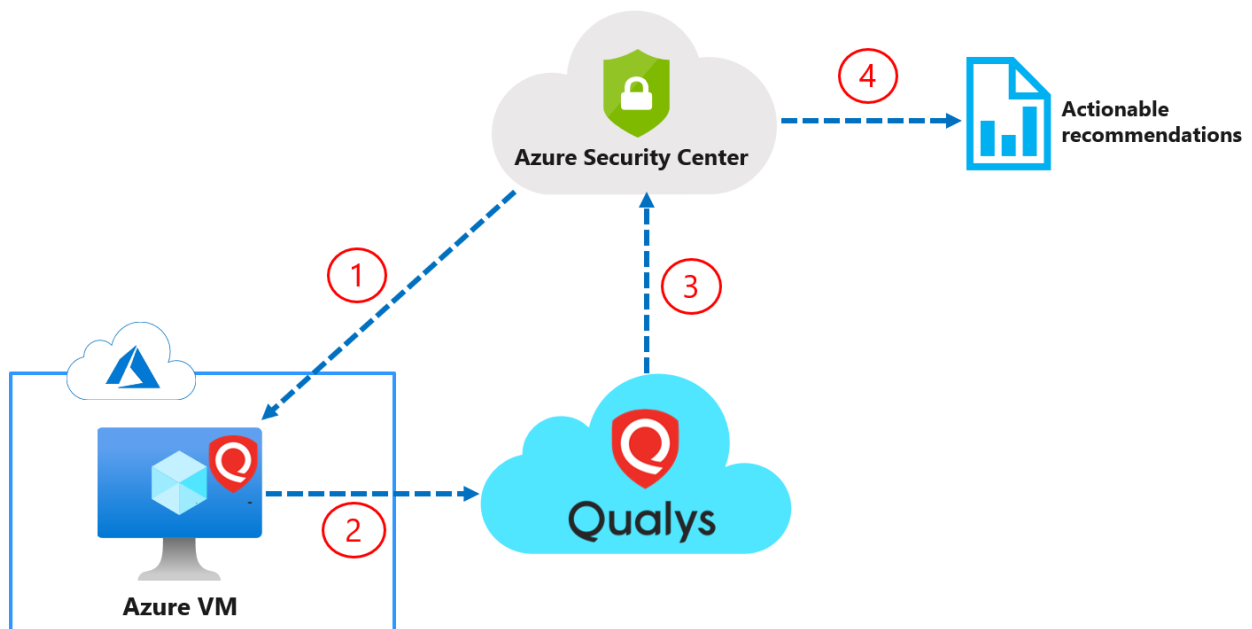
azseclinvm → Ready to enable

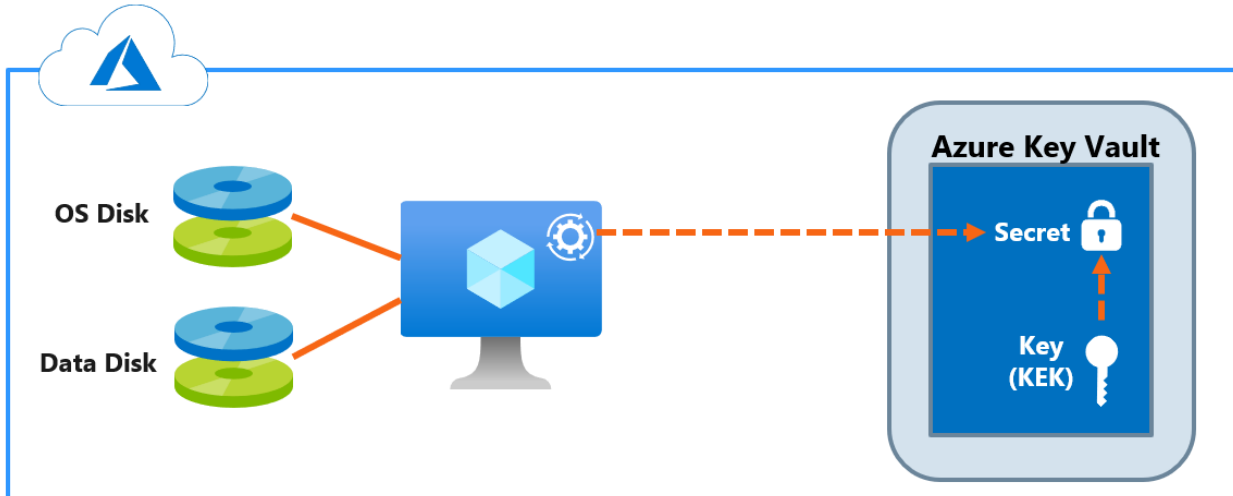
azsecwinvm → Ready to enable

Enable

Cancel

Number of virtual machines to enable Update Management: 2





Microsoft Azure

Azure services

+ Create a resource

Key vaults

Services

- Key vaults
- Backup vaults
- Recovery Services vaults
- SSH keys

Key vaults

azureblueteam (Default Directory)

+ New [Manage deleted vaults](#) [Manage view](#) [Refresh](#)

Filter for any field... Subscription == **AzureBlueTeam-PROD**

Create key vault ...



Subscription *

Resource group * **1** [Create new](#)

Instance details

Key vault name * ⓘ **2**

Region * **3**

Pricing tier * ⓘ **4**

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete ⓘ Enabled

Days to retain deleted vaults * ⓘ

[Review + create](#)

[< Previous](#)

[Next : Access policy >](#) **5**

Basics Access policy Networking Tags Review + create

Enable Access to:

- Azure Virtual Machines for deployment ⓘ
- Azure Resource Manager for template deployment ⓘ

1 Azure Disk Encryption for volume encryption ⓘ

Permission model Vault access policy Azure role-based access control

Review + create

2

< Previous

Next : Networking >

✓ Validation passed

Basics Access policy Networking Tags Review + create

Review + create

Basics

Subscription	AzureBlueTeam-PROD
Resource group	azuresec-c6-rg
Key vault name	azsec-120321
Region	UK South

Create

< Previous

Next >

Download a

✔ Your deployment is complete



Deployment name: azsec-120321

Subscription: AzureBlueTeam-PROD (a50ed1ee-5ea2-4719-8652-0...

Resource group: azuresec-c6-rg

∨ Deployment details [\(Download\)](#)

∧ Next steps

[Go to resource](#)



azsec-120321 | Keys ...

Key vault

<< 2 [+ Generate/Import](#) [Refresh](#)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Events
- Settings**
- Keys**
- Secrets

Name	Status
------	--------

There are no keys available.

Create a key ...

Options

1

Name * ⓘ

2

Key Type ⓘ

3 RSA EC

RSA Key Size

4 2048 3072 4096

Set activation date? ⓘ

Set expiration date? ⓘ

Enabled?

5

Microsoft Azure



Azure services

Virtu machi

Services

No results were found.

Resources

	azsecwinvm	Virtual machine
	azsecwinvm-nic	Network interface

azsecwinvm | Disks ...
Virtual machine

Search (Ctrl+/) << Save Discard Refresh **Additional settings** 2

Settings

- Networking
- Connect
- Windows Admin Center (previ... 1
- Disks**
- Size

OS disk

↔ Swap OS disk

Disk name	Storage type	Size (GiB)
azsecwinOSDisk	Premium SSD	127

Disk settings ...
azsecwinvm

Encryption settings
Azure Disk Encryption (ADE) provides volume encryption for the OS and data [Encryption](#).

Disks to encrypt ⓘ 1

OS and data disks

Azure Disk Encryption is integrated with Azure Key Vault to help manage encryption keys. You can have an existing key vault with encryption permissions set. For additional security, you can create a new key vault and key to protect the secret.

Key vault and key *

Key vault: -
Key: -
Version: -
Click to select a key 2

Select key from Azure Key Vault ...



Key vault *

1 azsec-120321

[Create new](#)

Key

2 Disk-Encryption-KEK

[Create new](#)

Version ⓘ

3 2316e9bb7d43447a80d67d94792f06df

[Create new](#)

Select 4

azsecwinvm | Extensions ...

Virtual machine

Search (Ctrl+/)



+ Add

Windows Admin Center (previ...

Disks

Size

Security

Advisor recommendations

Extensions

Continuous delivery

Search to filter items...

Name	↑↓	Type	↑↓	Vers...↑↓	Status
AzureDiskEncryption		Microsoft.Azure.Security.AzureDiskEncryption		2.*	Provisioning succeeded
installscript1		Microsoft.Compute.CustomScriptExtension		1.*	Provisioning succeeded

Search (Ctrl+/) << + Generate/Import Refresh Restore Backup Manage deleted secrets

Settings

- Keys
- Secrets**
- Certificates

Name	Type	Status
9D1E998F-FBE4-43C0-B473-2D18F6C90...	Wrapped BEK	✓ Enabled

Add port configuration ×

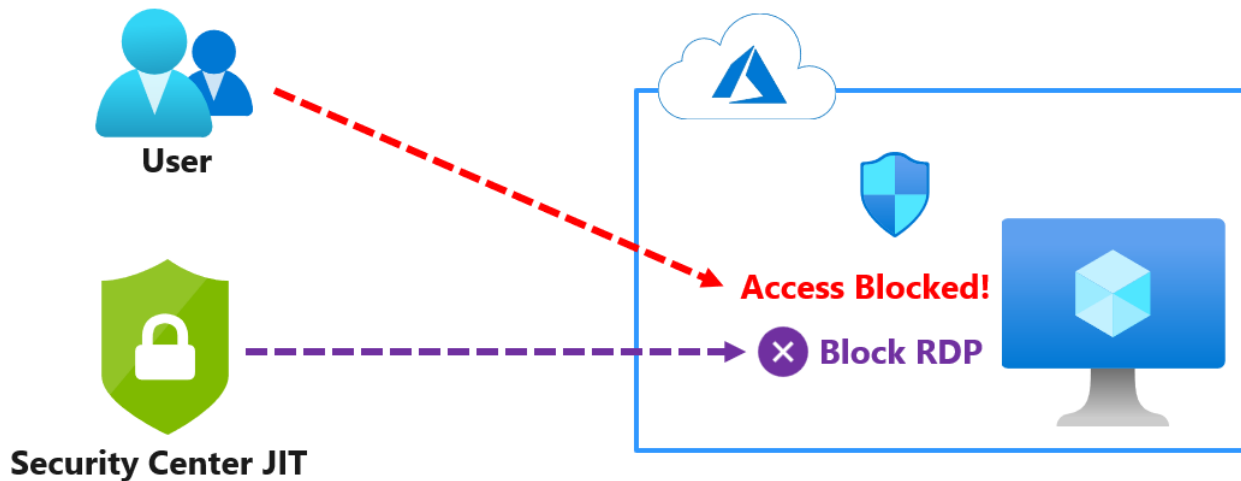
Port *

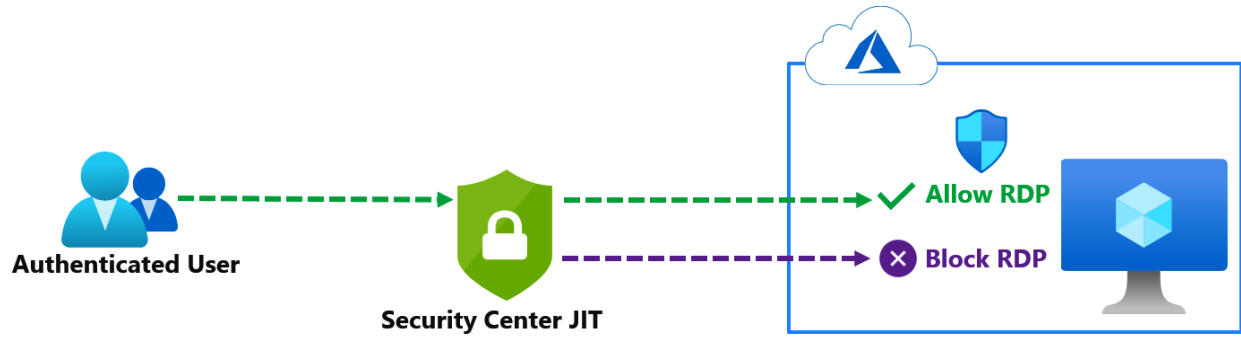
Protocol
 Any TCP UDP

Allowed source IPs
 Per request CIDR block

IP addresses ⓘ

Max request time
 3 (hours)





Security Center | Getting started ...

The screenshot shows the "Getting started" page in the Security Center. On the left, a navigation menu includes "General", "Overview", "Getting started" (selected), "Recommendations", "Security alerts", "Inventory", "Workbooks", and "Community". A search bar at the top left contains "Search (Ctrl+/)". On the right, a summary card displays: "0 SQL servers on machines", "Resource Manager (Preview)", and "DNS (Preview)". At the bottom, a prominent blue button labeled "Upgrade" is highlighted with a red border, followed by the text "or skip ⓘ".

✔ Trial started



Successfully started Azure Defender trial on 1 subscriptions

a few seconds ago

Microsoft Azure

azsecwinvm

> Security Center

Security Center

ch (Ctrl+)

Services

No results were found.

Resources

azsecwinvm	Virtual machine
azsecwinvm-nic	Network interface

azsecwinvm | Configuration

Virtual machine

Search (Ctrl+)



Save



Discard

Continuous delivery

Availability + scaling

1

Configuration

Identity

Just-in-time VM access

To improve security, enable a just-in-time

Enable just-in-time

2

azsecwinvm | Networking

Virtual machine

Search (Ctrl+)



Attach network interface



Detach network interface

Diagnose and solve problems

Settings

Networking

Connect

Windows Admin Center (previ...

Disks

Size

Security

Inbound port rules

Outbound port rules

Network security group **azsecwinvm-nsg** (attached to subnet: public-su)
Impacts 1 subnets, 0 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol
1000	SecurityCenter-JITRule_113572...	3389	Any
1001	nsgRule1	3389	TCP
65000	AllowVnetInBound	Any	Any

azsecwinvm | Configuration

Virtual machine

Search (Ctrl+)



Save



Discard

Availability + scaling

Configuration

Identity

Just-in-time VM access

Just-in-time VM access (JIT) is enabled.
request access.

Open Azure Security Center

Virtual machines

Configured Not Configured Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs



Search to filter items...

Virtual machine	Approved	Last access	Connection details
azsecwinvm	0 Requests	N/A	-

- Properties
- Activity Log
- Edit
- Remove

JIT VM access configuration

azsecwinvm

+ Add  Save  Discard

Configure the ports for which the just-in-time VM

Port	Protocol
3389	Any

Add port configuration

Port *

3389

Protocol

Any TCP UDP

Allowed source IPs

Per request CIDR block

IP addresses ⓘ

*

Max request time

 3 (hours)

Discard **OK**






Configured Not Configured Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs

2 **Request access**

Search to filter items...

	Virtual machine 	Approved	Last access 	Connection details
1 	 azsecwinvm	0 Requests	N/A	 -

Request access



azsecwinvm

Please select the ports that you would like to open per virtual machine.

Port	Toggle	Allowed Source IP	IP Range	Time range (hours)
3389	1 <input checked="" type="checkbox"/> On <input type="checkbox"/> Off	2 <input checked="" type="checkbox"/> My IP <input type="checkbox"/> IP Range	No range	<input type="text" value="3"/>
3 <input checked="" type="checkbox"/> Needed for admin task				4 <input type="button" value="Open ports"/>

Inbound port rules

Network security group azsecwinvm-nsg (attached to subnet: public-subnet)
Impacts 1 subnets, 0 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
100	SecurityCenter-JITRule-1135723682...	3389	Any	86.111.111.111	10.0.0.4	Allow
1000	SecurityCenter-JITRule_1135723...	3389	Any	Any	10.0.0.4	Deny
1001	nsgRule1	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow

azsecwinvm | Activity log

Search (Ctrl+/) << Activity Edit columns Refresh Diagnostics settings Download as CSV

Subscription : AzureBlueTeam-PROD Event severity : All Timespan : Last 6 hou

Resource group : AZURESEC-C6-RG Resource : azsecwinvm Add Filter

16 items.

Operation name	Status	Time	Time stamp
Initiate JIT Network Access Policy	Succeeded	17 minutes ...	Fri Mar 12 2...
Initiate	Succeeded	17 minutes ...	Fri Mar 12 2...
Initiate JIT Network Access Policy	Accepted	17 minutes ...	Fri Mar 12 2...
Initiate	Accepted	17 minutes ...	Fri Mar 12 2...

Chapter 9: Implementing Container Security

Build Container Images



Docker VM



Azure Pipelines



Azure Container Registry Tasks

Store and Distribute Images



Azure Container Registry

Runtime Options

Without Orchestration



Virtual Machine



Container Instances



App Service



Batch



Function

With Orchestration



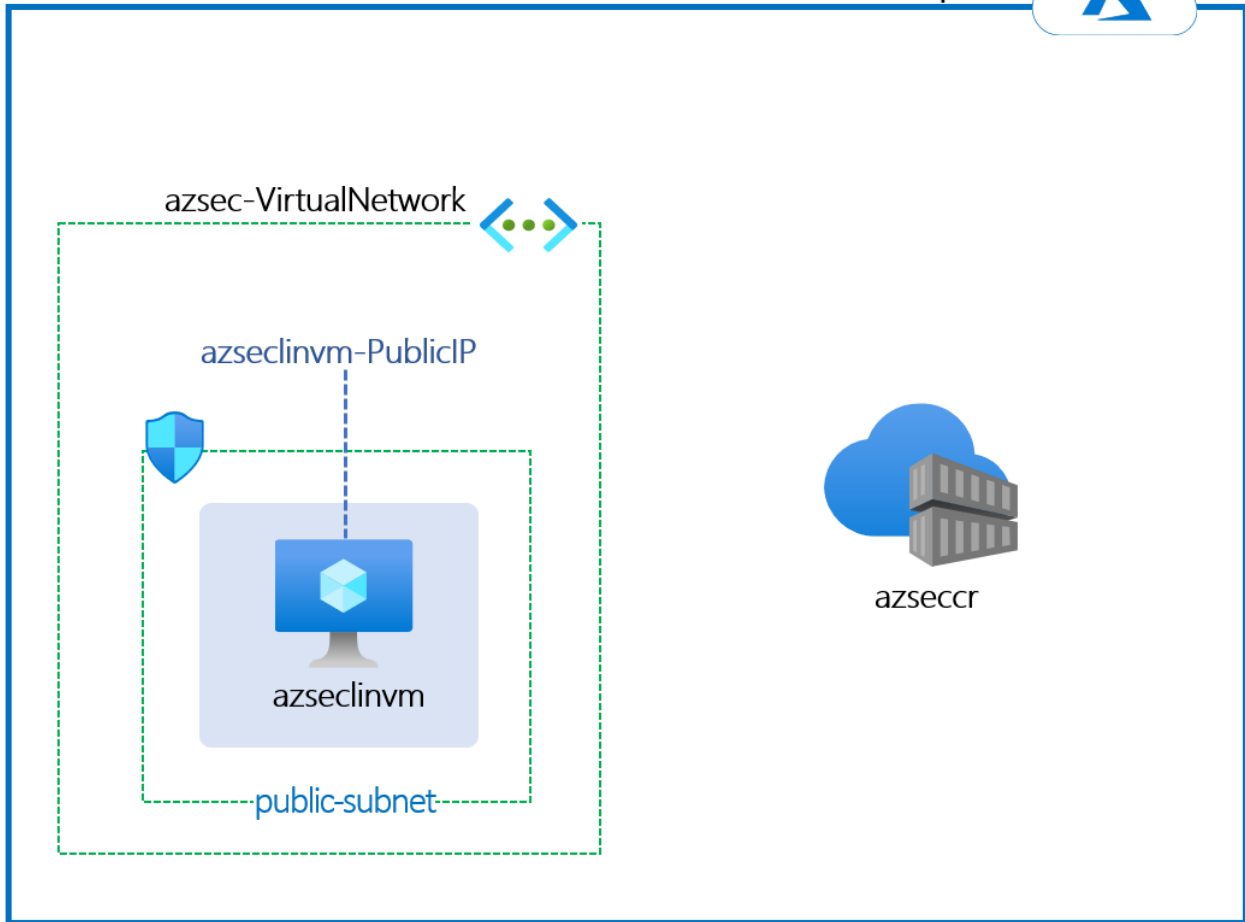
Kubernetes Service



Service Fabric



Azure RedHat OpenShift (ARO)



Azure Security Engineer Book - Chapter 9

Linux VM

- Ubuntu 18.04
- Azure CLI Installed
- Docker Installed
- Kubernetes CLI Installed

Custom deployment ...

Deploy from a custom template

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

Subscription * ⓘ

1 AzureBlueTeam-PROD (1c63ad39-68ee-444a-90a8-a2ccaf67f671) ▼



Resource group * ⓘ

2 (New) azuresec-c9-rg ▼

[Create new](#)

Instance details

Region * ⓘ

3 UK South ▼

Vm-dns ⓘ

[concat('azseclinvm-',uniqueString(resourceGroup().id))]

Admin User ⓘ

azureadmin

Admin Password * ⓘ

4 ✓

Vmsize ⓘ

Standard_B2ms ▼

Location ⓘ

[resourceGroup().location]

Resource Tags

{"Lab":"Azure Security"}

_artifacts Location ⓘ

[deployment().properties.templateLink.uri]

_artifacts Location Sas Token ⓘ

5 **Review + create**

< Previous

Next : Review + create >

Custom deployment ...

Deploy from a custom template

✓ Validation Passed ←

Basics Review + create

Summary

Customized template
8 resources

Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal charge or bill my current payment method for the fees same billing frequency as my Azure subscription, until

Create

< Previous

Next

Microsoft.Template-20210202023536 | Outputs

Deployment

Search (Ctrl+ /) <<

Overview

Inputs

Outputs

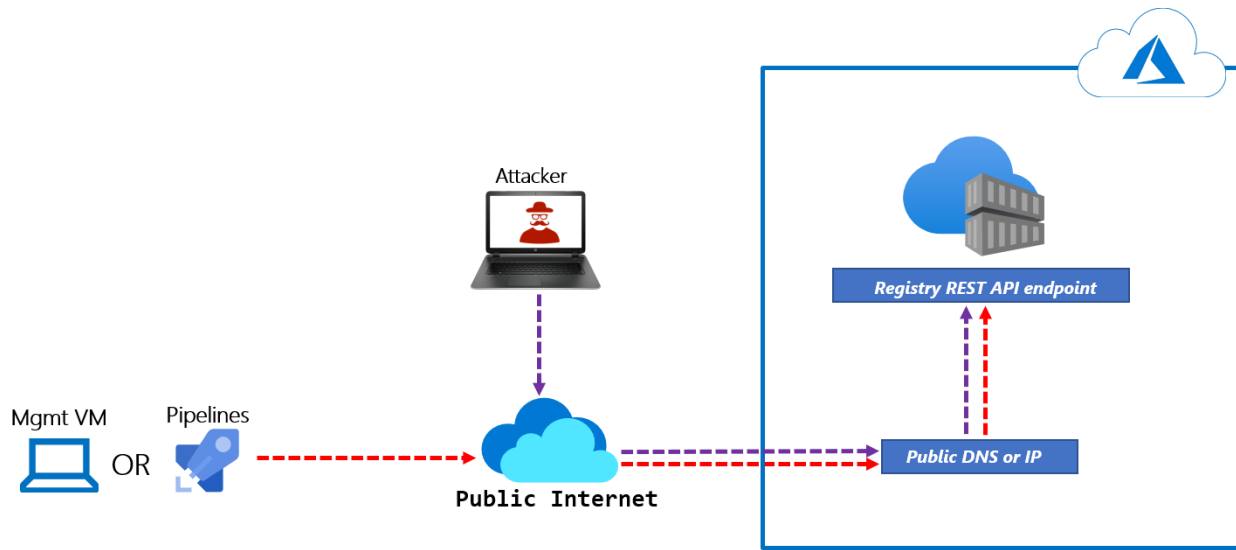
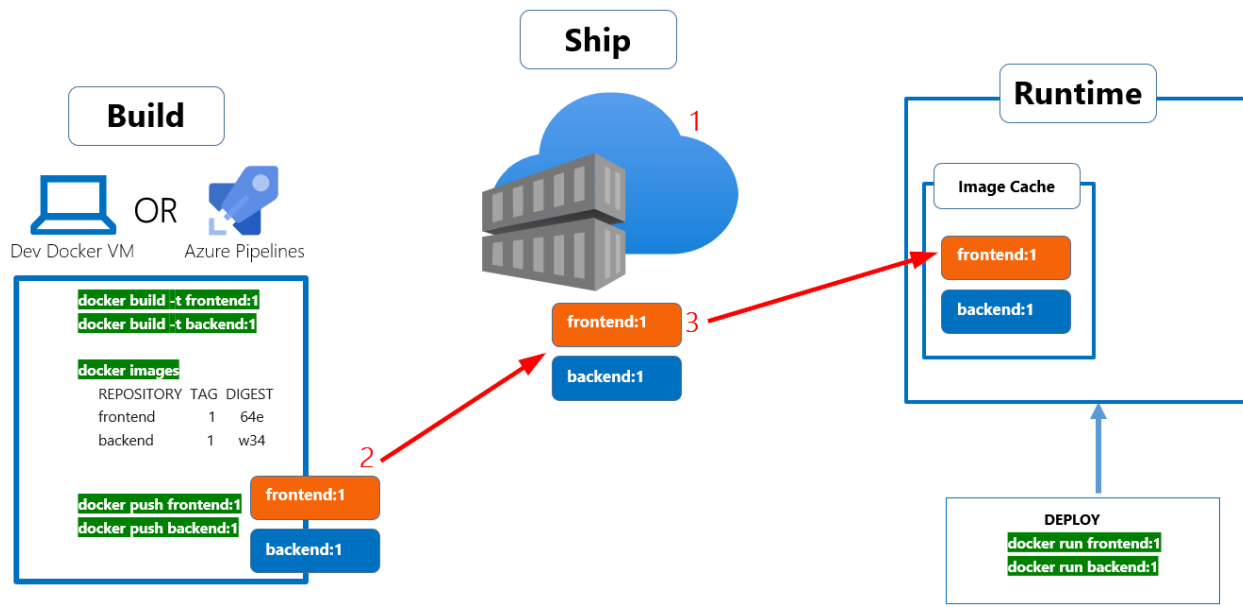
Template

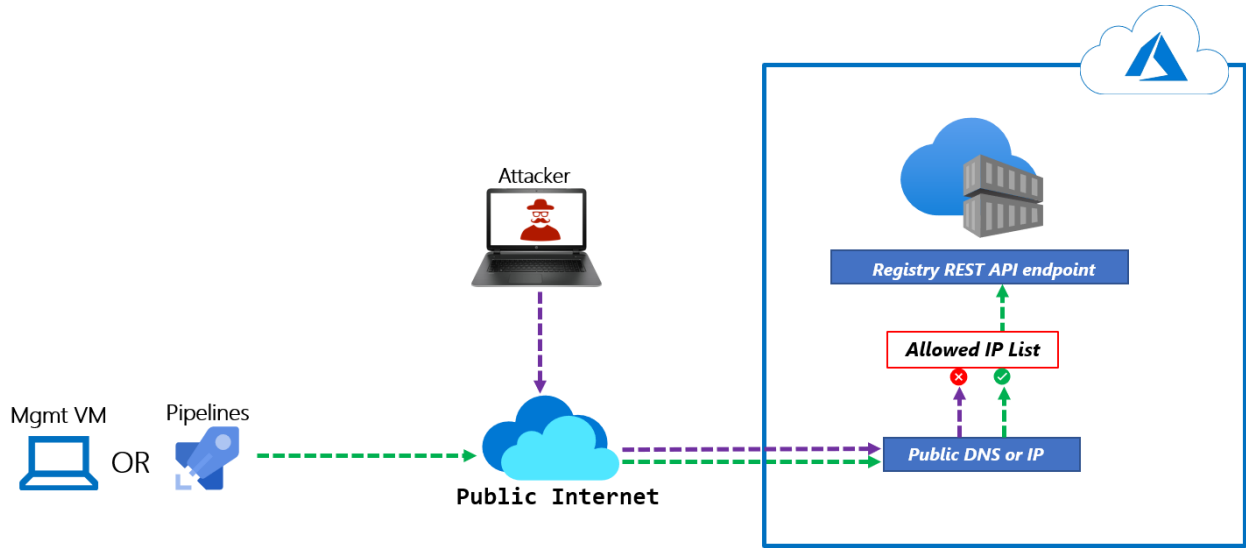
winvm-dns

azsecwinvm-yzh7zzj3yn3pq.uksouth.cloudapp.azure.com



2





doacr0304 | Networking ...
Container registry

Search (Ctrl+ /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Quick start
- Events

Settings

- Access keys
- Encryption
- Identity
- Networking**
- Security
- Locks

Public access Private endpoint

Save Discard Refresh

Allow public network access:

- All networks
- Selected networks
- Disabled

Firewall

Add IP ranges to allow access from the internet or your on-premises

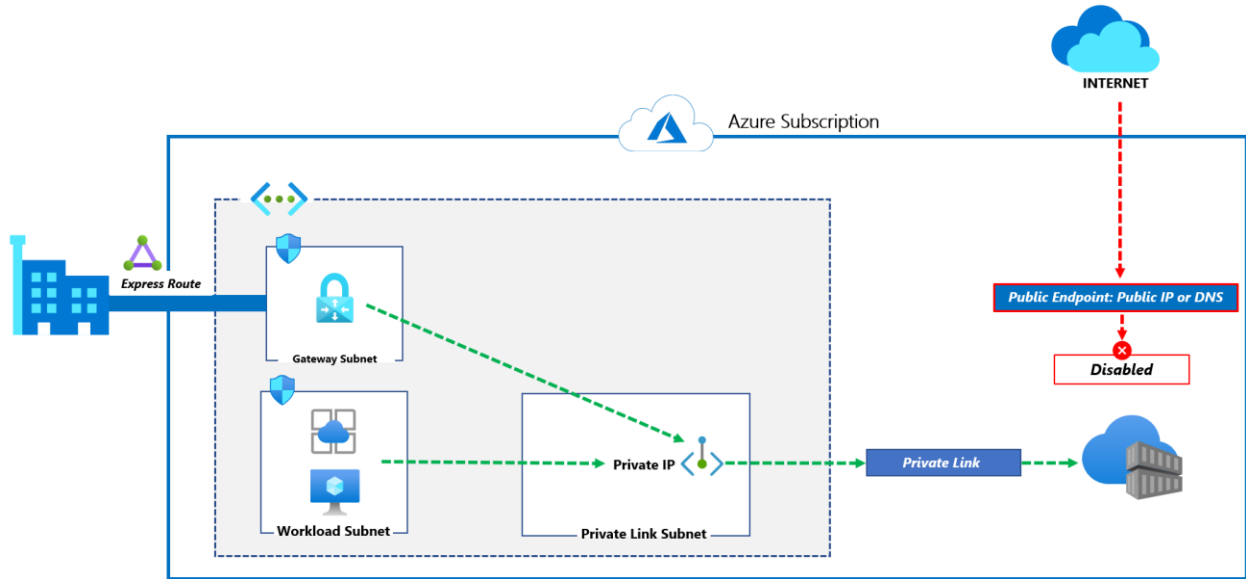
Add your client IP address ('31.54.11.93')

Address range

1.1.1.1

2.2.2.2

IP address or CIDR



doacr0304 | Access keys ...
 Container registry

Search (Ctrl+ /) << Registry name: doacr0304

Login server: doacr0304.azurecr.io

Admin user: Enabled

Username: doacr0304

Name	Password	Regenerate
password	C9lsCaLydvLI/9GpZzedeDhyhLRBkWK9	
password2	3pt0lk7ZBh6pZS+Hb1EPEZ5cVRoQpSIJ	

Enable the admin user

The username is the name of the registry

The passwords are auto-generated and can be regenerated

Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

doacr0304

control (IAM) ...

[+ Add](#) [Download role assignments](#) [Edit columns](#) [Refresh](#)

[Check access](#) [Role assignments](#) [Roles](#) [Roles \(Preview\)](#) [Deny assignm](#)

My access

View my level of access to this resource.

[View my access](#)

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Add role assignment

Role ⓘ


Select a role


Assign access to ⓘ

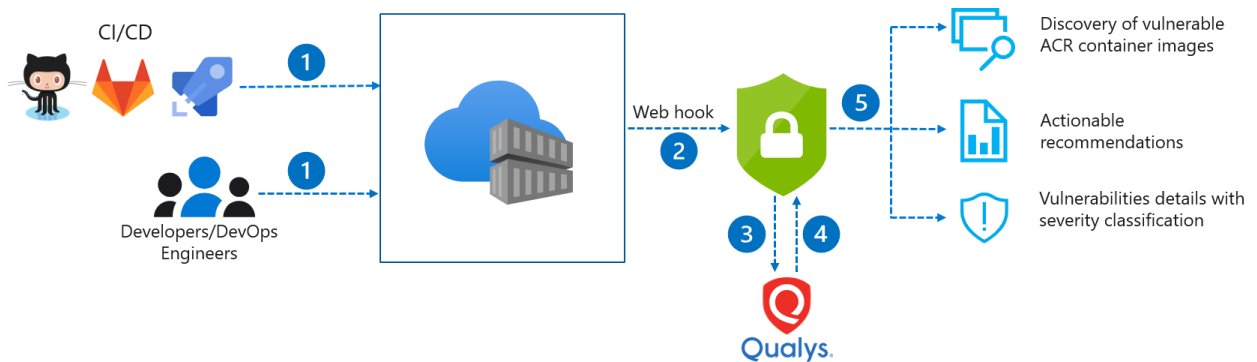
User, group, or service principal

Select ⓘ

Search by name or email address

 Brenda Tao
brenda@azureblueteam.io

 cloud-architects



Microsoft Azure 1 → azseccr

Azu

Services

No results were found.

Resources

2 → azseccryd5w466ms4oru Container registry

azseccryd5w466ms4oru | Access keys ...

Container registry

Search (Ctrl+/) <<

- Overview
- Activity log
- Access control (IAM)
- Tags
- Quick start
- Events

Settings

- Access keys
- Encryption

Registry name	azseccryd5w466ms4oru	
Login server	azseccryd5w466ms4oru.azurecr.io	
Admin user ⓘ	<input checked="" type="checkbox"/> Enabled	
Username	azseccryd5w466ms4oru	
Name	Password	Regenerate
password	aZl9a//l9K7bZcO+J50BZuPBM1D9giDG	
password2	Q/Br4y1BmPuJH5fJQNqyPYyeu6eOMB46	

Registry name: azseccryd5w466ms4oru

Login server: azseccryd5w466ms4oru.azurecr.io

Admin user ⓘ: Disabled

Search (Ctrl+/) << + Add ↓ Download role assignments ≡ Edit columns ↻ Refresh | ✕ Remove | ♥ Got feed

- Overview
- Activity log
- Access control (IAM)**
- Tags
- Quick start
- Events

Settings

- Access keys
- Encryption
- Identity

Check access | Role assignments | Roles | Roles (Preview) | Deny assignments | Classic administr

My access
View my level of access to this resource.
[View my access](#)

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find ⓘ
User, group, or service principal
Search by name or email address

Grant access to this resource
Grant access to resources by assigning
[Add role assignments](#)

View deny assignments

Add role assignment


Role ⓘ **1**

Assign access to ⓘ

Select ⓘ **2**

No users, groups, or service principals found.

Selected members: **3**

 azseclinvm	Remove
--	------------------------

4



Search (Ctrl+ /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Quick start
- Events

Settings

- Access keys
- Encryption
- Identity
- Networking
- Security**
- Locks

1

For enhanced security with just-in-time access,

Visit **Security Center** to manage security

2

Recommendations Azure Defender for

0 !

Recommendations

Security Center scans your container registry for security. To enable the optional Container Registries bundle and



Search (Ctrl+ /) Subscriptions What's new

- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Cloud Security
 - Secure Score
 - Regulatory compliance
 - Azure Defender**
 - Firewall Manager

1



Your subscriptions are not protected by Azure Defender

Add Azure Defender to your subscriptions for a unified view of security across all of your on - premises and cloud workloads, together with threat protection alerts, vulnerability scanning, container security features, and other advanced security features.

2 [Enable Azure Defender](#)











Getting started ...

Enable Azure Defender on 1 subscriptions

<input checked="" type="checkbox"/>	Name	↑↓ Total resources	Azure Defender Plan
<input checked="" type="checkbox"/>	 AzureBlueTeam-PROD	5	Off (30 trial days left)

↑
1

Total: 5 resources

	2 Servers	\$15	Server/Month
	0 App Service instances	\$15	Instance/Month
	0 Azure SQL Database	\$15	Server/Month
	0 Storage accounts	\$0.02	10k transactions
	2 Kubernetes cores	\$2	VM core/Month
	1 Container registries	\$0.29	Image
	0 Key Vaults	\$0.02	10k transactions
	0 SQL servers on machines	\$15 \$0.015	Server/Month Core/Hour
	Resource Manager (Preview)	FREE during preview	○
	DNS (Preview)	FREE during preview	○

Upgrade

← 2

Getting started ...

[Install Agents](#) [Get Started](#)

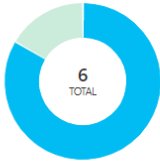
Make the most of Security Center by enabling data collection agents

To receive security alerts and recommendations, agents must be installed on your virtual machines for data collection.

[Learn more >](#)



Azure Defender coverage



2/2
Servers
Upgrade

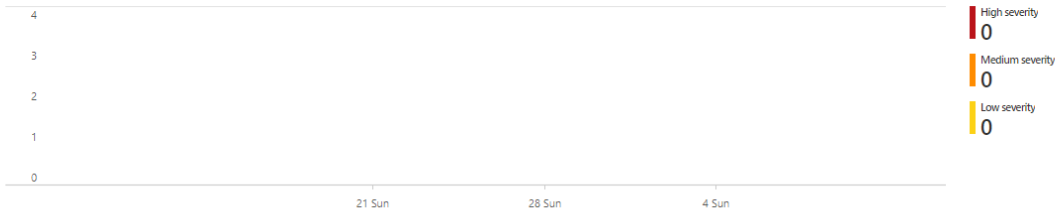
1/1
Kubernetes
Upgrade

1/1
Resource Manager subscriptions
Upgrade

1/1
DNS subscriptions
Upgrade

- Fully covered (83.3%)
- Agent not installed (16.7%) [Install](#)
- Not covered (0%)

Security alerts



Advanced protection

VM vulnerability assessment 2 Unprotected	Just-in-time VM access None Unprotected	Adaptive application control None Unprotected	Container image scanning None Unprotected	Adaptive network hardening None Unprotected
--	--	--	--	--

PuTTY Configuration

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
 - Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)	Port
azseclinvm-y6qa73mxvf7ok.uksouth.clouda	22

Connection type:

Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit

Always Never Only on clean exit

Buttons: About, Help, Open, Cancel


```
azureadmin@azseclinvm:~$  
azureadmin@azseclinvm:~$ sudo su -  
root@azseclinvm:~#  
root@azseclinvm:~# az login --identity  
[  
  {  
    "environmentName": "AzureCloud",  
    "homeTenantId": "7f3e6937-b492-49e7-9856-07d84e1cf2ae",  
    "id": "1c63ad39-68ee-444a-90a8-a2ccaf67f671",  
    "isDefault": true,  
    "managedByTenants": [],  
    "name": "AzureBlueTeam-PROD",  
    "state": "Enabled",  
    "tenantId": "7f3e6937-b492-49e7-9856-07d84e1cf2ae",  
    "user": {  
      "assignedIdentityInfo": "MSI",  
      "name": "systemAssignedIdentity",  
      "type": "servicePrincipal"  
    }  
  }  
]
```

```
root@azseclinvm:~#  
root@azseclinvm:~# az acr login --name azseccryd5w466ms4oru  
Login Succeeded  
root@azseclinvm:~#
```

```
root@azseclinvm:~#  
root@azseclinvm:~# docker images  
REPOSITORY          TAG                IMAGE ID           CREATED            SIZE  
node                 13.5-alpine       e1495e4ac50d      15 months ago    111MB  
root@azseclinvm:~#
```

```
root@azseclinv:~#
root@azseclinv:~# docker tag node:13.5-alpine azseccryd5w466ms4oru.azurecr.io/node:13.5-alpine
root@azseclinv:~#
root@azseclinv:~# docker images
REPOSITORY                                TAG                IMAGE ID           CREATED
SIZE
azseccryd5w466ms4oru.azurecr.io/node     13.5-alpine       e1495e4ac50d      15 months ago
111MB
node                                       13.5-alpine       e1495e4ac50d      15 months ago
111MB
root@azseclinv:~#
```

```
root@azseclinv:~#
root@azseclinv:~# docker push azseccryd5w466ms4oru.azurecr.io/node:13.5-alpine
The push refers to repository [azseccryd5w466ms4oru.azurecr.io/node]
efd6e0da275f: Pushed
b352b61d0fe4: Pushed
d06ff5e5272b: Pushed
6b27de954cca: Pushed
13.5-alpine: digest: sha256:990e2a5ecd6419bfd1ae1af8dc585924712614e9cc79999d943c1158
```

azseccryd5w466ms4oru | Repositories

Container registry

Search (Ctrl+)

Refresh

Search to filter repositories ...

Repositories ↑↓

node

node

Refresh Delete repository

Essentials

Repository node

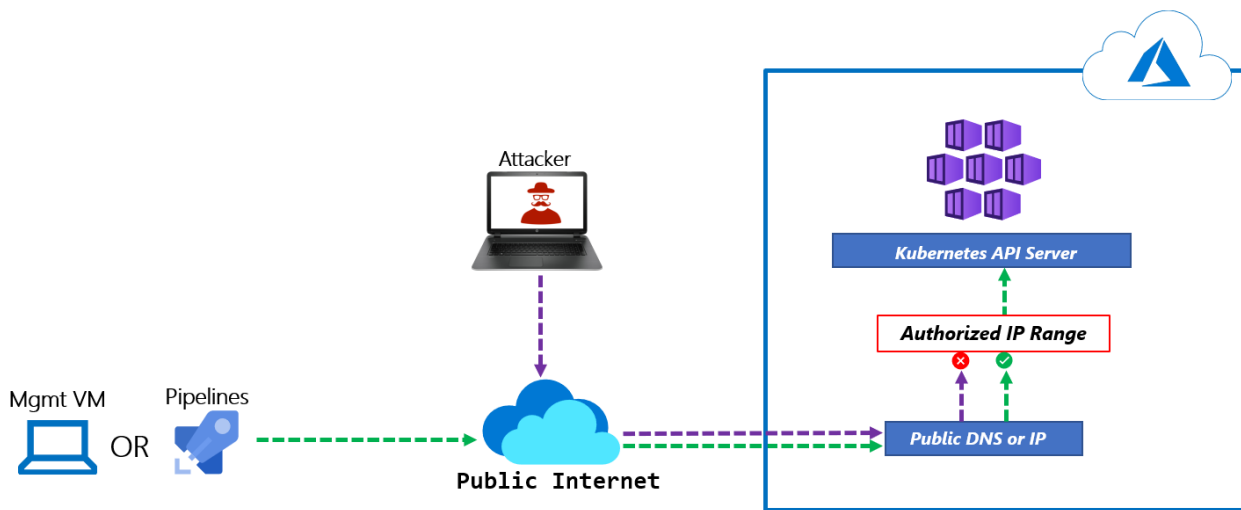
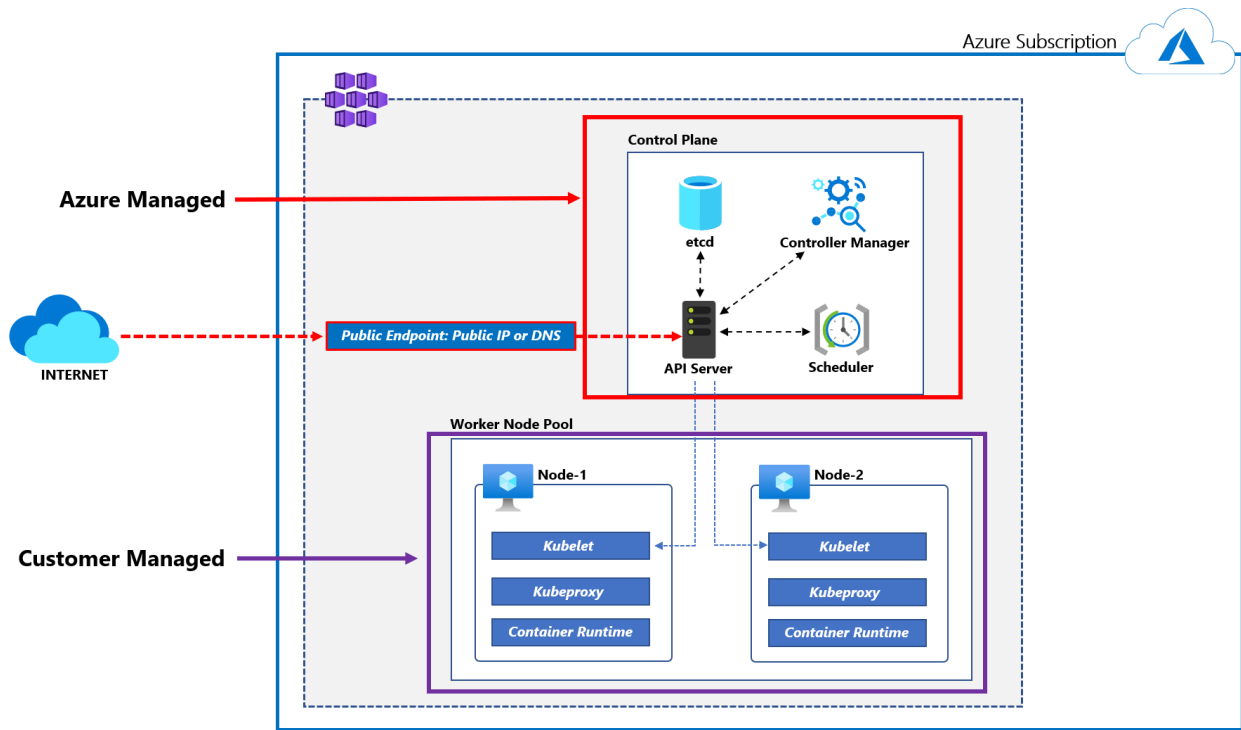
Last updated date 4/5/2021, 5:35 PM GMT+1

Search to filter tags ...

Tags ↑↓

13.5-alpine

```
root@azseclinv:~#
root@azseclinv:~# az acr list
[]
root@azseclinv:~#
```



Search (Ctrl+ /)

4 Save X Discard

- Storage
- Configuration
- Settings
 - Node pools
 - Cluster configuration
 - Scale
 - 1 Networking
 - Dev Spaces
 - Deployment center (preview)
 - Policies
 - Properties
 - Locks
- Monitoring
 - Insights
 - Alerts
 - Metrics

Type (plugin)	Kubenet
Pod CIDR	10.244.0.0/16
Service CIDR	10.0.0.0/16
DNS service IP	10.0.0.10
Docker bridge CIDR	172.17.0.1/16
Network policy	None

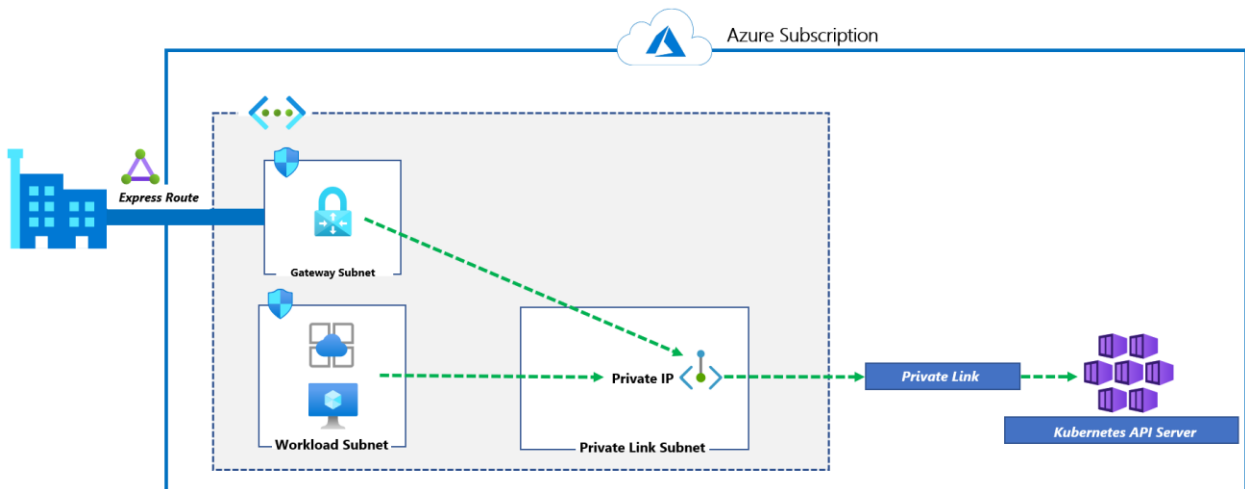
Traffic routing

Load balancer	Standard
Enable HTTP application routing ⓘ	<input type="checkbox"/>

ⓘ HTTP application routing is only recommended for dev/test clusters

Security

Private cluster	Not enabled
Set authorized IP ranges ⓘ	2 <input checked="" type="checkbox"/>
Specify IP ranges * ⓘ	3 1.1.1.1



```

kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: business-app-full-access-role
  namespace: business-app
rules:
- apiGroups: [""]
  resources: ["*"]
  verbs: ["*"]

```

Role

Scoped to a namespace

```

kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: cluster-full-access-role
rules:
- apiGroups: [""]
  resources: ["*"]
  verbs: ["*"]

```

ClusterRole

No namespace definition needed for a ClusterRole as it defines cluster-wide permission

```

kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: business-app-full-access-role-binding
  namespace: business-app
subjects:
- kind: User
  name: developer@contoso.com
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: business-app-full-access-role
  apiGroup: rbac.authorization.k8s.io

```

Users or groups that we are assigning the role or cluster role to. We can specify our Azure AD identities here

The role or cluster role that we are assigning

```

kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: cluster-full-access-role-binding
subjects:
- kind: User
  name: clusteroperator@contoso.com
roleRef:
  kind: ClusterRole
  name: cluster-full-access-role
  apiGroup: rbac.authorization.k8s.io

```

azsec-aks | Cluster configuration ...

Kubernetes service

Search (Ctrl+/) << Save Discard

Services and ingresses

Storage

Configuration

Settings

Node pools

Cluster configuration

Scale

Networking

Dev Spaces

Deployment center (preview)

Policies

Properties

Locks

Upgrade

You can upgrade your cluster to a newer version of Kubernetes. This will upgrade the control cluster.

The upgrade will roll out safely in stages so your container applications can continue to run

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

[View the Kubernetes changelog](#)

Kubernetes version: 1.19.7 (current)

1.20.2 (preview)

1.19.7 (current)

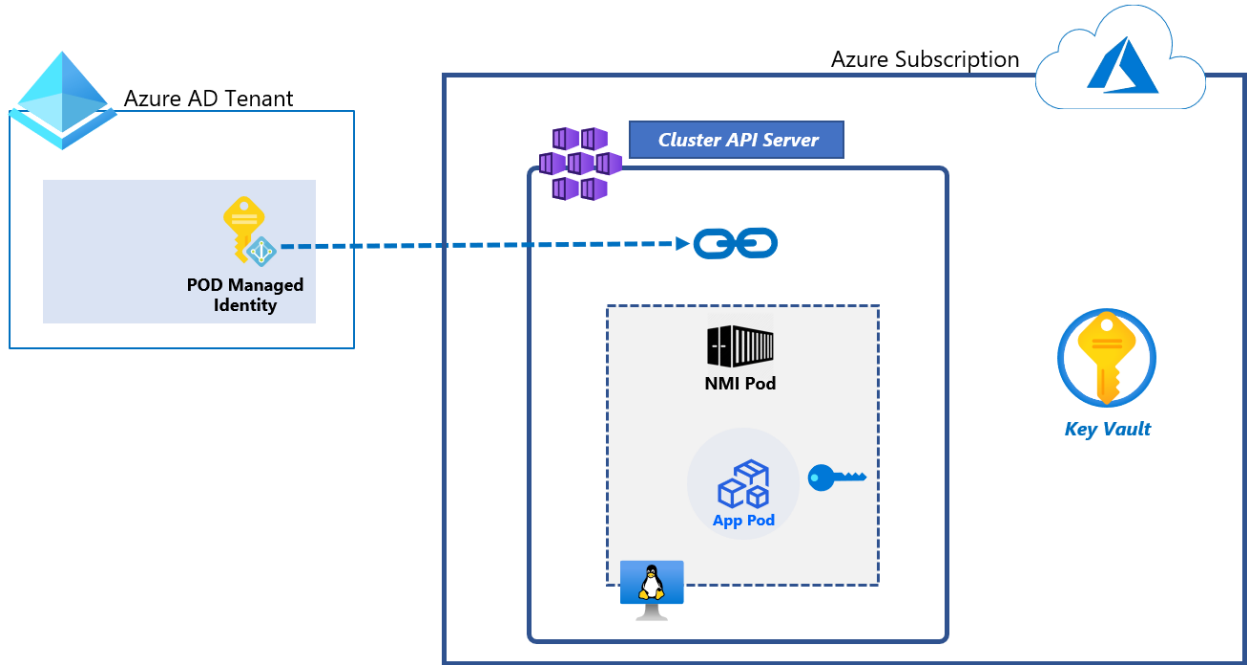
Kubernetes authentication and authorization

Authentication and authorization are used

Role-based access control (RBAC): Disabled

AKS-managed Azure Active Directory: Disabled

AKS-managed Azure Active Directory requires user access



Create Kubernetes cluster ...

Subscription * ⓘ

Resource group * ⓘ **1**

Cluster details

Kubernetes cluster name * ⓘ **2** ✓

Region * ⓘ **3** ✓

Availability zones ⓘ **4** ✓

Kubernetes version * ⓘ

Primary node pool

The number and size of nodes in the primary node pool in your cluster. For production workloads, at least 3 nodes are recommended for resiliency. For development or test workloads, only one node is required. If you would like to add additional node pools or to see additional configuration options for this node pool, go to the 'Node pools' tab above. You will be able to add additional node pools after creating your cluster. [Learn more about node pools in Azure Kubernetes Service](#)

Node size * ⓘ [Change size](#)

Node count * ⓘ **5**

6

Create Kubernetes cluster ...

Basics Node pools Authentication Networking Integrations Tags Review + create

Cluster infrastructure

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

Authentication method Service principal System-assigned managed identity

Kubernetes authentication and authorization

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

Role-based access control (RBAC) Enabled Disabled

AKS-managed Azure Active Directory Enabled Disabled

Admin Azure AD groups

Node pool OS disk encryption

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

Encryption type (Default) Encryption at-rest with a platform-managed key

Review + create

< Previous

Next : Networking >



```
Bash david@Azure:~$ az aks get-credentials --resource-group azuresec-c9-rg --name azsec-c9-aks --admin
Merged "azsec-aks-admin" as current context in /home/david/.kube/config
david@Azure:~$
```



```
david@Azure:~$  
david@Azure:~$ kubectl create namespace development  
namespace/development created  
david@Azure:~$
```

```
role-development-namespace.yaml ●  
1 kind: Role  
2 apiVersion: rbac.authorization.k8s.io/v1  
3 metadata:  
4   name: development-user-full-access  
5   namespace: development  
6 rules:  
7 - apiGroups: [ "", "extensions", "apps" ]  
8   resources: [ "*" ]  
9   verbs: [ "*" ]  
10 - apiGroups: [ "batch" ]  
11   resources:  
12     - jobs  
13     - cronjobs  
14   verbs: [ "*" ]  
15  
david@Azure:~$  
david@Azure:~$ code role-development-namespace.yaml  
david@Azure:~$
```

```
david@Azure:~$  
david@Azure:~$ kubectl apply -f role-development-namespace.yaml  
role.rbac.authorization.k8s.io/development-user-full-access created  
david@Azure:~$
```

```
david@Azure:~$  
david@Azure:~$ az ad group show --group cloud-architects --query objectId -o tsv  
3ed92323-3235-4102-8a6c-260794ec871a  
david@Azure:~$
```

```
rolebinding-development-namespace.yaml
1  kind: RoleBinding
2  apiVersion: rbac.authorization.k8s.io/v1
3  metadata:
4    name: development-user-access
5    namespace: development
6  roleRef:
7    apiGroup: rbac.authorization.k8s.io
8    kind: Role
9    name: development-user-full-access
10 subjects:
11 - kind: Group
12   namespace: cloud-architects
13   name: 3ed92323-3235-4102-8a6c-260794ec871a
14
```

Object ID of the "cloud-architects" Azure AD group

```
david@Azure:~$
david@Azure:~$ code rolebinding-development-namespace.yaml
david@Azure:~$
```

```
david@Azure:~$
david@Azure:~$ kubectl apply -f rolebinding-development-namespace.yaml
rolebinding.rbac.authorization.k8s.io/development-user-access created
david@Azure:~$
```

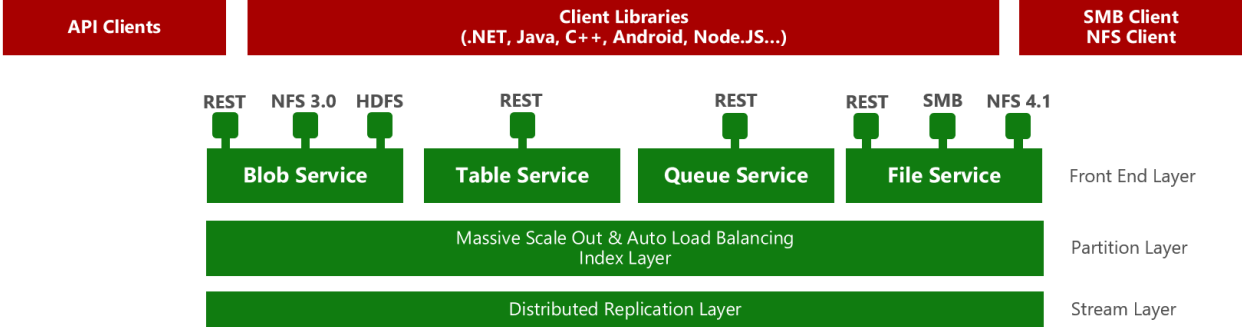
```
david@Azure:~$ kubectl run nginx-dev --image=mcr.microsoft.com/oss/nginx/nginx:1.15.
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and
pod/nginx-dev created
```

```
david@Azure:~$ kubectl get pods --namespace development
```

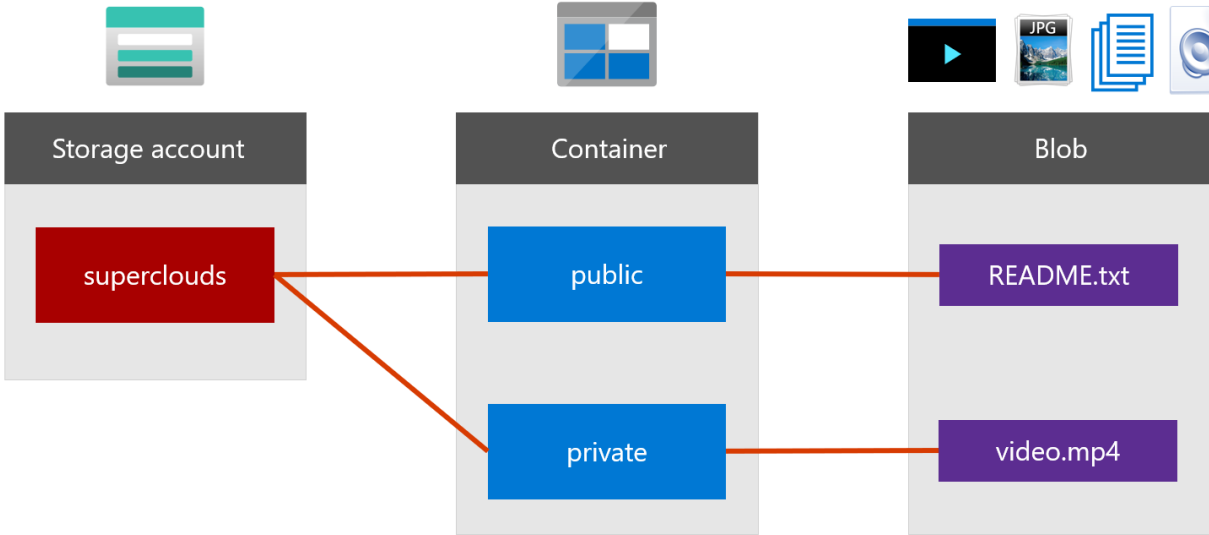
NAME	READY	STATUS	RESTARTS	AGE
nginx-dev	1/1	Running	0	4m14s

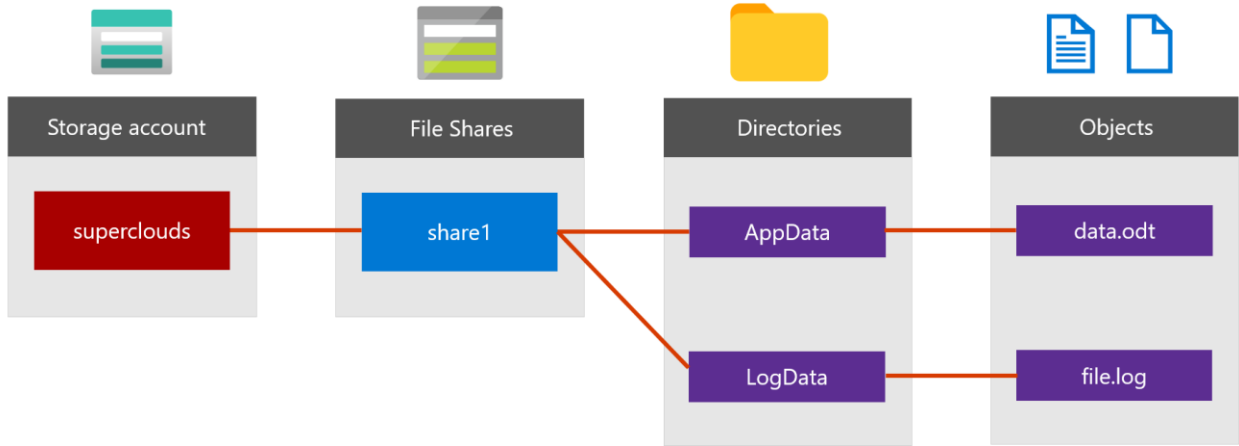
```
david@Azure:~$ kubectl get pods --all-namespaces
Error from server (Forbidden): pods is forbidden: User "brenda@azureblueteam.io" can
```

Chapter 10: Implementing Storage Security



https://<STORAGE_ACCOUNT_NAME>.blob.core.windows.net/<CONTAINER_NAME>/<BLOB_NAME>





dostore9879 | Encryption ...
Storage account

Search (Ctrl+/) << **Encryption** Encryption scopes

Settings

- Access keys
- Geo-replication
- CORS
- Configuration
- Encryption**
- Shared access signature
- Networking
- Security
- Advisor recommendations

Storage service encryption protects your data at rest. Azure Storage encrypts you decrypts it for you as you access it.

Please note that after enabling Storage Service Encryption, only new data will be will retroactively get encrypted by a background encryption process. [Learn more](#)

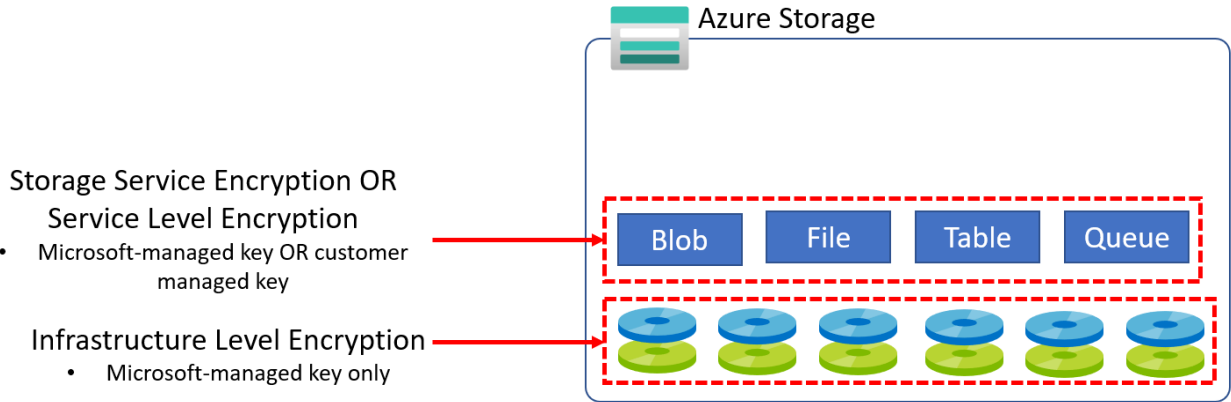
Encryption selection

Support for customer-managed keys ⓘ Blobs and files only

Infrastructure encryption ⓘ Disabled

Encryption type

- Microsoft-managed keys
- Customer-managed keys



Create a storage account ...

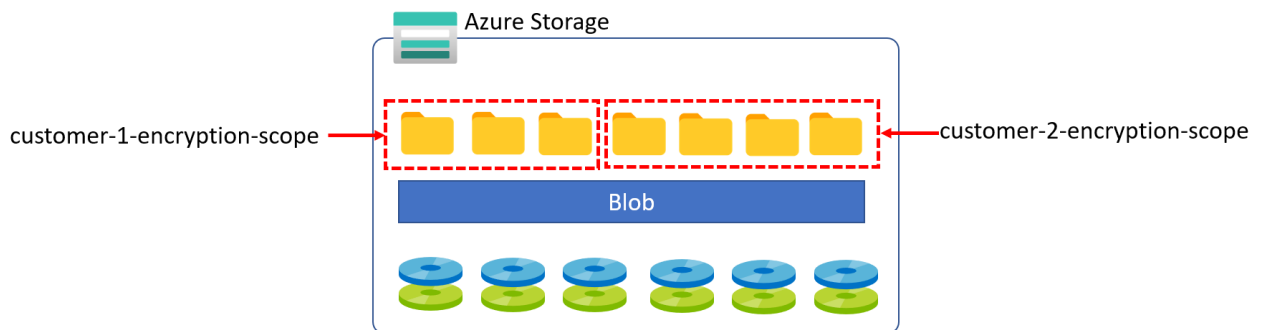
Basics Advanced Networking Data protection Tags Review + create


i Certain options have been disabled by default due to the combination of storage account

Security




Configure security settings that impact your storage account.









- Enable secure transfer *i*
- Enable infrastructure encryption *i* ←
- Enable blob public access *i*




 Search (Ctrl+/)




 Save  Discard  Refresh


-  Access keys
-  Geo-replication
-  CORS
-  **Configuration**
-  Encryption
-  Shared access signature
-  Networking
-  Security

1


 This setting cannot be changed after the :

Secure transfer required 


Disabled **Enabled** 2

Allow Blob public access 

Disabled Enabled

Allow storage account key access 

Disabled Enabled

Minimum TLS version 

3

Azure services



New ...

Storage account

Storage account

Microsoft



Storage account [Add to Favorites](#)

Microsoft
★★★★☆ 4.2 (1732 ratings)

[Create](#)


Create a storage account



Basics [Advanced](#) [Networking](#) [Data protection](#) [Tags](#) [Review + create](#)

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.


Subscription * **1** 

 Resource group * **2** 
[Create new](#)


Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ * **3**

Region ⓘ * **4** 

Performance ⓘ * **5** **Standard: Recommended for most scenarios (general-purpose v2 account)**
 Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ * **6** 

[Review + create](#)

[< Previous](#)

[Next : Advanced >](#)

7

Security

Configure security settings that impact your storage account.

Enable secure transfer ⓘ

Enable infrastructure encryption ⓘ

Enable blob public access ⓘ

Enable storage account key access ⓘ

Minimum TLS version ⓘ

Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). [Learn more](#)

Enable hierarchical namespace

Review + create

< Previous

Next : Networking >

✓ Validation passed

Basics

Advanced

Networking

Data protection

Tags

Review + create

Basics

Subscription	AzureBlueTeam-PROD
Resource Group	azuresec-c10-rg
Location	uksouth
Storage account name	azsecstor2204
Deployment model	Resource manager
Performance	Standard
Replication	Locally-redundant storage (LRS)

Advanced

Secure transfer	Enabled
Allow storage account key access	Enabled
Infrastructure encryption	Disabled
Blob public access	Enabled

Create

< Previous

Next >

[Download a template for](#)



azsecstor2204_1619093627841 | Overview

Deployment

Search (Ctrl+ /)

Delete Cancel Redeploy Refresh

Overview

Inputs

Outputs

Template

We'd love your feedback! →


✓ Your deployment is complete

Deployment name: azsecstor2204_1619093627841
Subscription: AzureBlueTeam-PROD (1c63ad39-68ee-444a-90a8-a2...)
Resource group: azuresec-c10-rg

Deployment details (Download)


Next steps


Go to resource

 Search (Ctrl+J)

<< 2


 Container


 Change access level

 Locks

Blob service

 Containers ¹

 Data protection

 Object replication

Search containers by prefix

Name


\$logs


New container

Name *

public 

Public access level ⓘ

Blob (anonymous read access for blobs only) 

 Blobs within the container can be read by anonymous request, but container data is not available. Anonymous clients cannot enumerate the blobs within the container.

Advanced

Create

Discard

public Container

Search (Ctrl+)

Upload Change access level Refresh Delete

- Overview
- Diagnose and solve problems
- Access Control (IAM)
- Settings
 - Shared access signature
 - Access policy

Authentication method: Access key (Switch to Azure AD User Account)
Location: public

Search blobs by prefix (case-sensitive)

Name
No results

Upload blob

public/

Files ¹
"sampletemplate.json"

Overwrite if files already exist

Advanced

Upload ²

public Container

Search (Ctrl+)

Upload Change access level

- Overview
- Diagnose and solve problems
- Access Control (IAM)
- Settings
 - Shared access signature
 - Access policy
 - Properties
 - Metadata

Authentication method: Access key (Switch to Azure AD User Account)
Location: public

Search blobs by prefix (case-...)
 Show deleted blobs

Name
<input type="checkbox"/> sampletemplate.json ...

sampletemplate.json

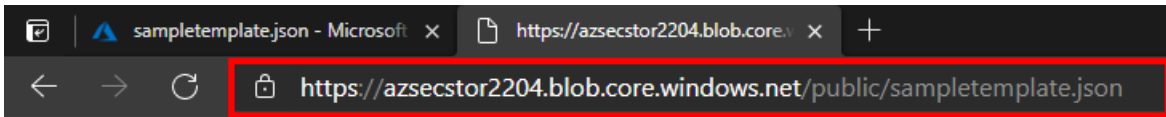
Blob
Save Discard Download Refresh Delete

Overview Versions Snapshots Edit Generate SAS

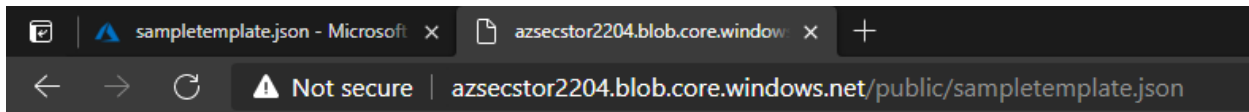
Properties

URL	https://azsecstor2204.bl...
LAST MODIFIED	4/22/2021, 2:21:10 PM
CREATION TIME	4/22/2021, 2:21:10 PM
VERSION ID	-
TYPE	Block blob
SIZE	7.92 KiB
ACCESS TIER	Hot (Inferred)
ACCESS TIER LAST MODIFIED	N/A

Click to copy the URL of the Blob



```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "type": "string",
      "defaultValue": "simpleLinuxVM",
      "metadata": {
        "description": "The name of you Virtual Machine."
      }
    },
    "adminUsername": {
      "type": "string",
      "metadata": {
        "description": "Username for the Virtual Machine."
      }
    }
  }
}
```



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>
  <Code>AccountRequiresHttps</Code>
  <Message>The account being accessed does not support http. RequestId:12fb5079-701e-0045-547b-370ed9000000</Message>
  <AccountName>azsecstor2204</AccountName>
</Error>
```

Azure Storage Service	Storage Account Key	Shared Access Signature (SAS)	Azure Active Directory (Azure AD)	On-premises Active Directory Domain Services	Anonymous public read access
Azure Blobs	Supported	Supported	Supported	Not supported	Supported
Azure Files (SMB)	Supported	Not supported	Supported, only with AAD Domain Services	Supported, credentials must be synced to Azure AD	Not supported
Azure Files (REST)	Supported	Supported	Not supported	Not supported	Not supported

+ Add permissions + Exclude permissions **1**

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. [Learn more](#)
To exclude specific permissions from a wildcard permission, click Exclude permissions. [Learn more](#)

Permission	↑↓	Description	↑↓	Permission type
*		--		Action
Microsoft.Storage/storageAccounts/listkeys/action		Returns the access keys for the specified storage account.		NotAction

Blob File Queue Table

Allowed resource types ⓘ

Service Container Object

Allowed permissions ⓘ

Read Write Delete List Add Create Update Process

Blob versioning permissions ⓘ

Enables deletion of versions

Start and expiry date/time ⓘ

Start

End

Allowed IP addresses ⓘ

Allowed protocols ⓘ

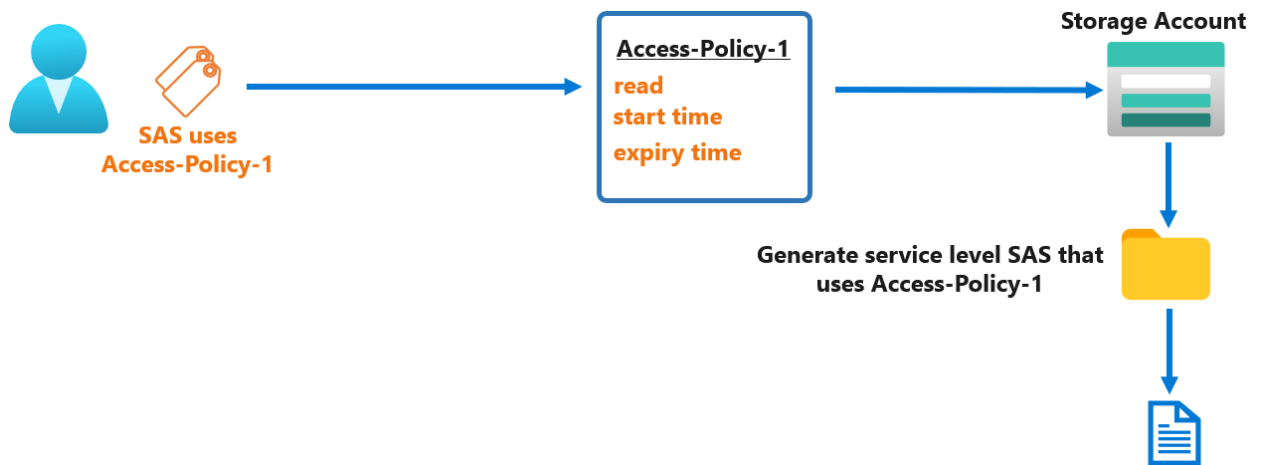
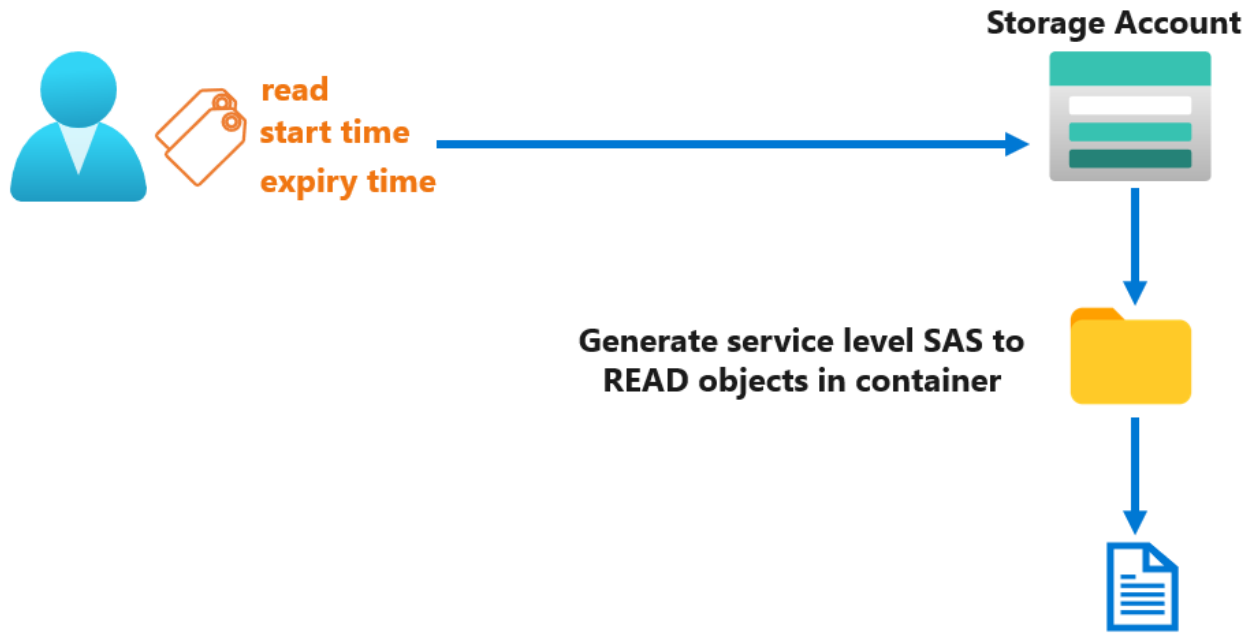
HTTPS only HTTPS and HTTP

Preferred routing tier ⓘ

Basic (default) Microsoft network routing Internet routing

i Some routing options are disabled because the endpoints are not published.

Signing key ⓘ



dostore9879 | Access keys ...

Storage account

Search (Ctrl+)

Storage Explorer (preview)

Settings

- Access keys**
- Geo-replication
- CORS
- Configuration
- Encryption
- Shared access signature
- Networking
- Security
- Advisor recommendations
- Static website
- Properties

Use access keys to authenticate your ap keys so that you can maintain connectio

When you regenerate your access keys,

Storage account name

dostore9879

Hide keys

key1



Regenerate Key1

Key

xUPk0ypXbiTSmqtonTAQv1d1G9dpN

Connection string

DefaultEndpointsProtocol=https;Acco

key2

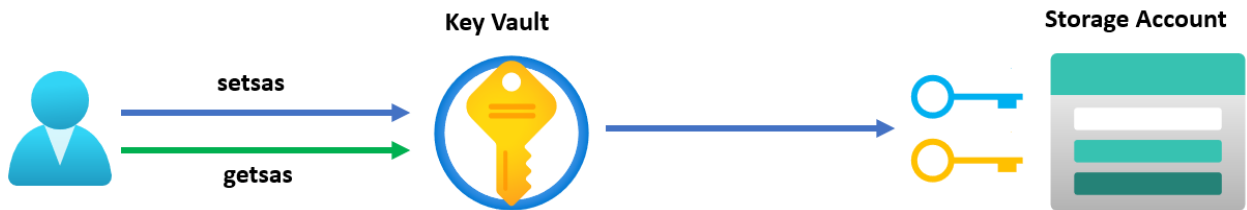


Regenerate Key2

Key

RFZgzeJTaXQWJNKD+r1sZ93zhuCh1te

Connection string



dostore9879 | Configuration 🔗 ⋮
Storage account

Search (Ctrl+/) << **3** **Save** ✕ Discard 🔄 Refresh

Settings

- Access keys
- Geo-replication
- CORS
- Configuration** 1
- Encryption

3 This setting cannot be changed after the

Secure transfer required ⓘ
 Disabled Enabled

Allow Blob public access ⓘ
 Disabled Enabled

2 Allow storage account key access ⓘ
 Disabled Enabled

New container ✕

Name *
private ✓

Public access level ⓘ
Private (no anonymous access) ^

- Private (no anonymous access)
- Blob (anonymous read access for blobs only)
- Container (anonymous read access for containers and blobs)

dostore9879 | Configuration 🔗 ⋮
Storage account

Search (Ctrl+/) << **3** **Save** ✕ Discard 🔄 Refresh

1 **Configuration**

3 This setting cannot be changed after the

Secure transfer required ⓘ
 Disabled Enabled

2 Allow Blob public access ⓘ
 Disabled Enabled

azsecstor 1

Services Marketplace
No results were found.

Resources Documentation
azsecstor2204 2 Storage account

Resource Groups

azsecstor2204 | Configuration

Storage account

Search (Ctrl+/) Save 3 Discard Refresh

Storage Explorer (preview)

Settings

- Access keys
- Geo-replication
- CORS
- Configuration 1**
- Encryption
- Shared access signature
- Networking
- Security

The cost of your storage account depends on the usage and the

Account kind
StorageV2 (general purpose v2)

Performance ⓘ
 Standard Premium

ⓘ This setting cannot be changed after the storage account is

Secure transfer required ⓘ
 Disabled Enabled

2 **Allow Blob public access ⓘ**
 Disabled Enabled

⚠ This will not allow any public access to this storage account,

azsecstor2204 | Containers

Storage account

Search (Ctrl+/) + Container Change access level

Blob service

- Containers 1**
- Data protection
- Object replication

Search containers by prefix

Name

- \$logs
- 2 public

public Container

Search (Ctrl+/) << Upload **Change access level** Refresh Delete Change

Overview

- Diagnose and solve problems
- Access Control (IAM)

Settings

- Shared access signature
- Access policy
- Properties
- Metadata

Change access level

Change the access level of container 'public'.

Public access level ⓘ

Blob (anonymous read access for blobs only) ▾

i Public access to this container is being blocked because public access is disabled on this storage account.

2 **OK** Cancel

Review message

sampletemplate.json Blob

Upload Change access level ...

Authentication method: Access key (Switch to Azure AD User Account)

Location: public

Search blobs by prefix (case-...)

Show deleted blobs

Name
<input type="checkbox"/> sampletemplate.json ...

Overview Versions Snapshots Edit Generate SAS

Properties

URL	https://azsecstor2204.bl... Copy
LAST MODIFIED	4/22/2021, 2:21:10 PM
CREATION TIME	4/22/2021, 2:21:10 PM
VERSION ID	-
TYPE	Block blob
SIZE	7.92 KiB
ACCESS TIER	Hot (Inferred)

Click to copy the URL of the object

sampletemplate.json - Microsoft x https://azsecstor2204.blob.core.w... x +

https://azsecstor2204.blob.core.windows.net/public/sampletemplate.json

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<Error>
  <Code>PublicAccessNotPermitted</Code>
  <Message>Public access is not permitted on this storage account. RequestId:a01fcaa0-101e-000e-3089-37f2</Message>
</Error>
```

sampletemplate.json ...

Blob

Save Discard Download Refresh Delete

Overview Versions Snapshots Edit **Generate SAS** 1

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage blob. [Learn more](#)

Signing method 2

Account key User delegation key

Signing key ⓘ

Key 1 3

Permissions * ⓘ

Read 4

Start and expiry date/time ⓘ

Start 5

04/22/2021 4:16:39 PM

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Expiry 6

04/23/2021 12:16:39 AM

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Allowed IP addresses ⓘ


for example, 168.1.5.65 or 168.1.5.65-168.1....

Allowed protocols ⓘ 7

HTTPS only HTTPS and HTTP

Generate SAS token and URL 8

Blob SAS token ⓘ

sp=r&st=2021-04-22T15:16:39Z&se=2021-04-22T23:16:39Z&spr=https&sv=2020-02-10&sr=b&sig=219LYqRPB... 

Blob SAS URL

<https://azsecstor2204.blob.core.windows.net/public/sampletemplate.json?sp=r&st=2021-04-22T15:16:39Z&se=2021-04-22T23:16:39Z&spr=https&sv=2020-02-10&sr=b&sig=219LYqRPB...> 

Click to copy the URL with the generated SAS token 

sampletemplate.json - Microsoft | https://azsecstor2204.blob.core... | +
https://azsecstor2204.blob.core.windows.net/public/sampletemplate.json?sp=r&st=2021-04-22T15

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
  "contentVersion": "1.0.0.0",  
  "parameters": {  
    "vmName": {  
      "type": "string",  
      "defaultValue": "simpleLinuxVM",  
      "metadata": {  
        "description": "The name of you Virtual Machine."  
      }  
    }  
  },  
}
```

sampletemplate.json ... ✕

Blob

Save Discard Download Refresh Delete

- Overview
- Versions
- Snapshots
- Edit
- Generate SAS**

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage blob. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. [Learn more](#)

public ...

Container

Search (Ctrl+/) << Upload Change access level Refresh Delete

- Overview**
- Diagnose and solve problems
- Access Control (IAM)

- Settings**
- Shared access signature
- Access policy

Authentication method: Access key **Switch to Azure AD User Account**
Location: public

Search blobs by prefix (case-sensitive)

Name
<input type="checkbox"/> sampletemplate.json

↑ Upload | 🔒 Change access level | ↻ Refresh | 🗑 Delete | ⋮

✖ You do not have permissions to list the data using your user account with Azure AD. Click to learn more about authenticating with Azure AD.
This request is not authorized to perform this operation using this permission.
RequestId:44b6ed13-601e-0014-3f8e-379355000000
Time:2021-04-22T15:43:43.0609503Z →

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

Show deleted blobs

public ⋮
Container

- Overview
- Diagnose and solve problems
- Access Control (IAM)**
- Settings

↑ Upload | 🔒 Change access level

✖ You do not have permissions to list
This request is not authorized to per
RequestId:4212bf9b-401e-002c-408e
Time:2021-04-22T15:48:36.1311977Z

Authentication method: Azure AD User
Location: public

public | Access Control (IAM) ⋮

+ Add | ↓ Download role assignments | ≡ Edit columns | ↻ Refresh | ✕ Remove | ❤ Got feedback?

Check access | Role assignments | Roles | Roles (Preview) | Deny assignments | ⋮

My access
View my level of access to this resource.
[View my access](#)

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource.
[Learn more](#)

Find ⓘ

Grant access to this resource
Grant access to resources by assigning a role.

[Add role assignments](#) [Learn more](#)

Add role assignment ×

Role ¹

Assign access to ²

Select ³

Brenda Tao
brenda@azureblueteam.io
cloud-architects

Selected members:
David Okeyode
david-packt-az500_outlook.com#EXT... [Remove](#)

⁴

public Container

Search (Ctrl+ /) << Upload Change access level Refresh Delete


Overview ¹ **Authentication method:** Azure AD User Account [\(Switch to Access key\)](#)
Location: public

Diagnose and solve problems
Access Control (IAM)

Settings

Shared access signature
Access policy
Properties
Metadata

Search blobs by prefix (case-sensitive)

Name
<input type="checkbox"/>  sampletemplate.json



Search (Ctrl+)

Upload Change access level Refresh Delete

Overview

Diagnose and solve problems

Access Control (IAM)

Authentication method: Azure AD User Account (Switch to Access key)

Location: public

Search blobs by prefix (case-sensitive)

Show deleted blobs

Search (Ctrl+)

Save Discard Refresh

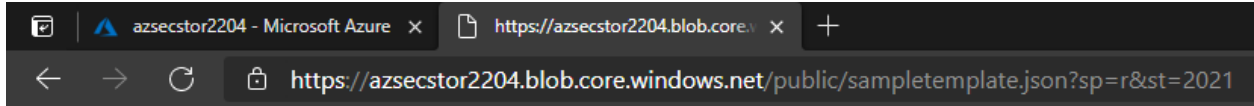
CORS
Configuration
Encryption
Shared access signature
Networking
Security
Advisor recommendations

Secure transfer required
 Disabled Enabled

Allow Blob public access
 Disabled Enabled

Allow storage account key access
 Disabled Enabled

When Allow storage account key access is disabled, any
[Learn more about Allow storage account key access](#)



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>  
  <Code>KeyBasedAuthenticationNotPermitted</Code>  
  <Message>Key based authentication is not permitted on this storage account</Message> RequestId:be01c90f-401e-0071-2b94-  
</Error>
```

Search (Ctrl+*/*)

Save

Settings

Azure Defender plans

- Auto provisioning
- Email notifications
- Threat detection
- Workflow automation
- Continuous export
- Cloud connectors

Azure Defender plan will apply to: 3 resources in this subscription

Select Azure Defender plan by resource type **Enable all**

Azure Defender for	Resource Quantity	Pricing		Plan
Servers	0 servers	\$15/Server/Month	ⓘ	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
App Service	0 instances	\$15/Instance/Month	ⓘ	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Azure SQL Database	0 servers	\$15/Server/Month	ⓘ	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
SQL servers on machines	0 servers	\$15/Server/Month \$0.015/Core/Hour	ⓘ	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Storage	3 storage accounts	\$0.02/10k transactions	ⓘ	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Kubernetes	0 kubernetes cores	\$2/VM core/Month	ⓘ	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Container registries	0 container registries	\$0.29/Image		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Key Vault	0 key vaults	\$0.02/10k transactions		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
Resource Manager (Preview)		FREE during preview	ⓘ	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
DNS (Preview)		FREE during preview	ⓘ	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off

Chapter 11: Implementing Database Security

	Relational Data	Unstructured Data	Semi-Structured Data	Large Data Sets	Small Data Sets	In Memory Database
Azure SQL	✓				✓	
Azure Database for MySQL	✓				✓	
Azure Database for PostgreSQL	✓				✓	
Azure Database for MariaDB	✓				✓	
Azure Cosmos DB		✓	✓	✓	✓	
Azure Table Storage			✓		✓	
Azure Synapse Analytics	✓			✓	✓	
Azure Cache for Redis					✓	✓

IaaS

SQL Virtual Machine

Best for migrations and applications requiring OS-level access



SQL virtual machine

PaaS

Azure SQL Managed Instance

Best for most lift-and-shift migrations to the cloud



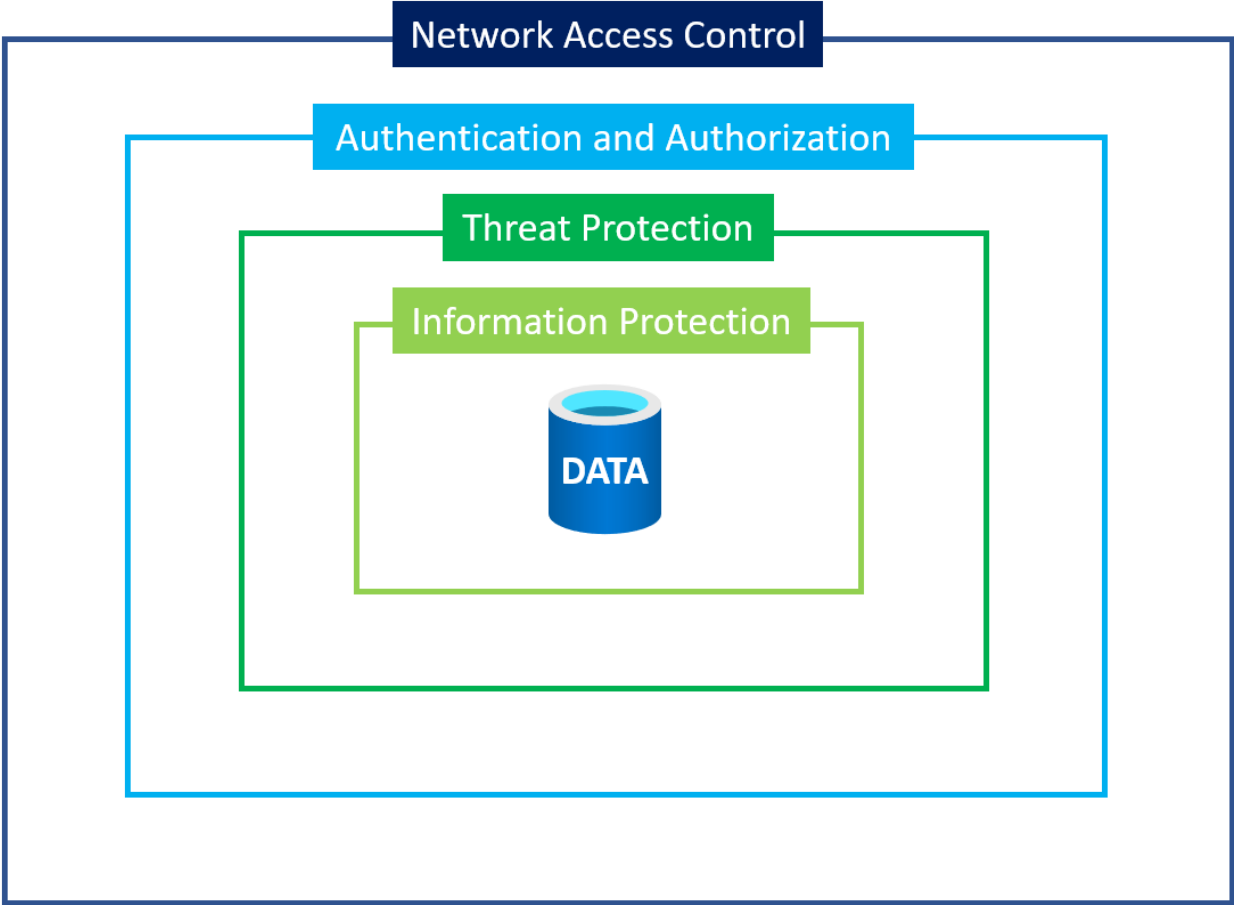
Single instance

Azure SQL Database

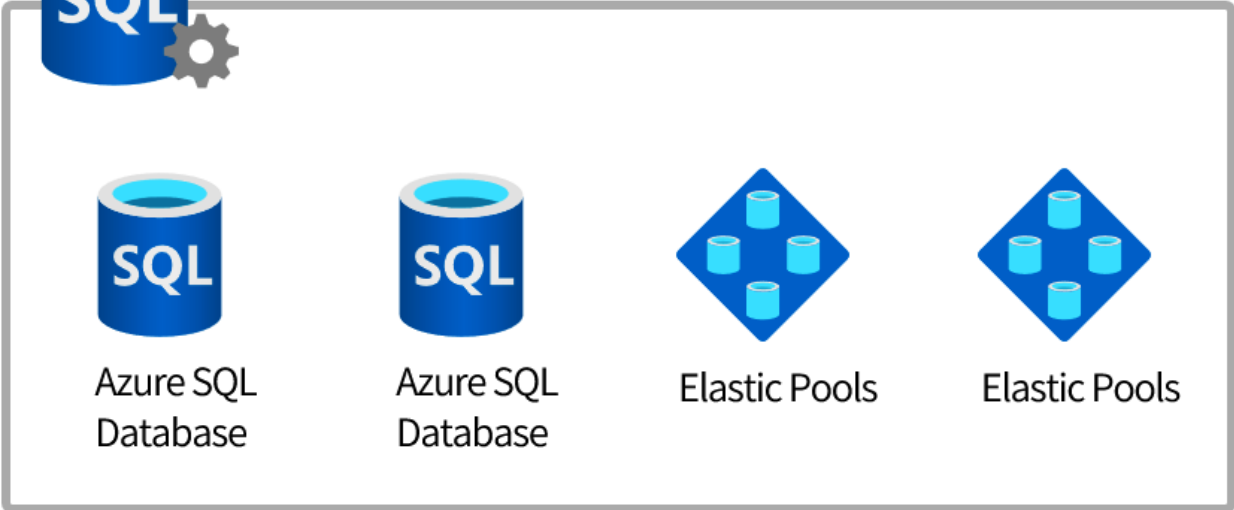
Best for modern cloud applications

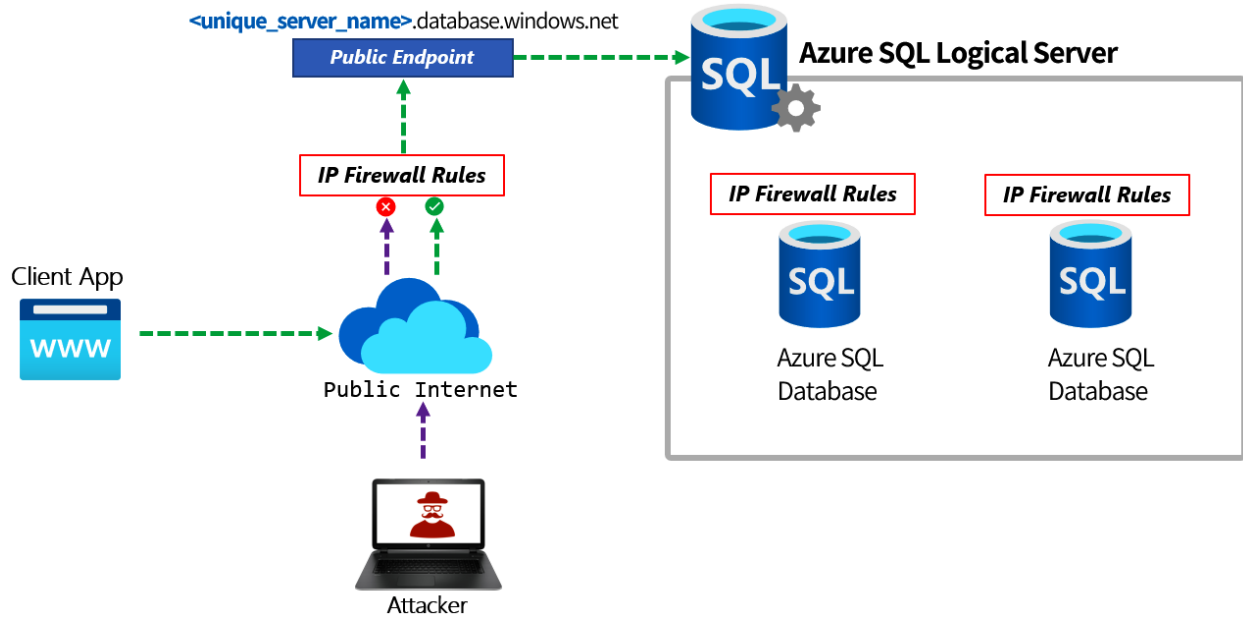


Single database



Azure SQL Logical Server





dosqlsrv01 | Firewalls and virtual networks ...
SQL server

Search (Ctrl+/) << Save Discard + Add client IP

Security

- Auditing
- Firewalls and virtual networks**
- Private endpoint connections
- Security Center
- Transparent data encryption

Intelligent Performance

- Automatic tuning
- Recommendations

Monitoring

- Logs

Minimum TLS Version ⓘ
1.0 1.1 1.2

Connection Policy ⓘ
Default Proxy Redirect

Allow Azure services and resources to access this server ⓘ
Yes No

Client IP address 86.147.112.228

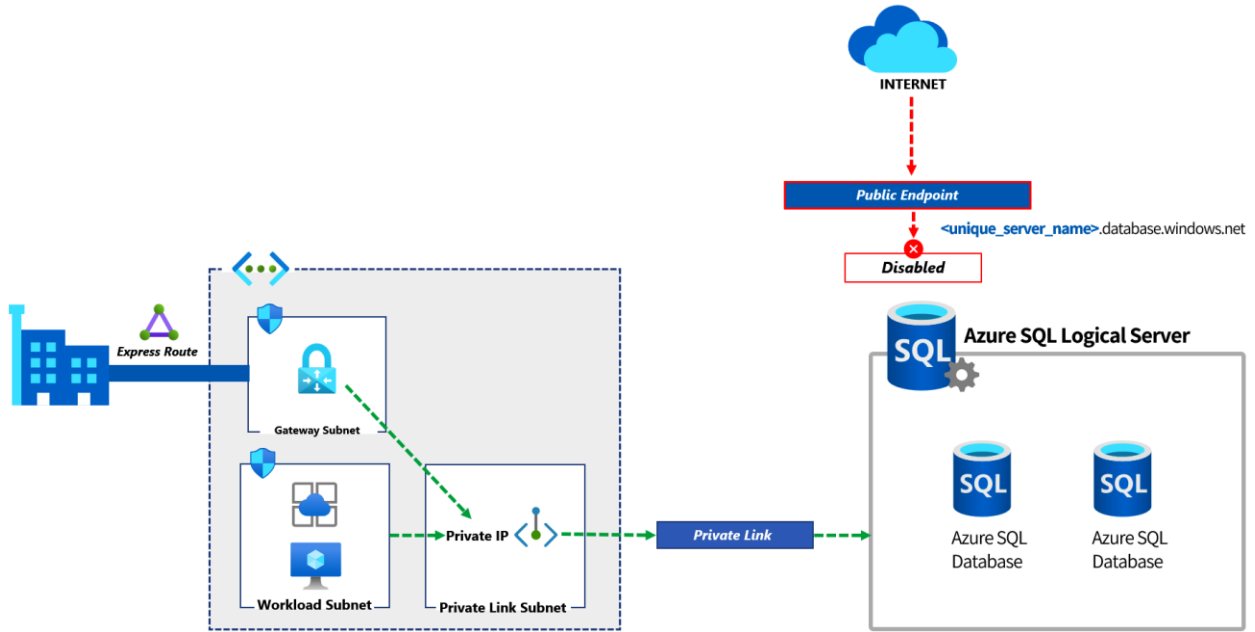
IP Address Rules

Rule name	Start IP	End IP	
			...
Allow_App_Client	1.1.1.1	1.1.1.1	...

Virtual Network Rules

Virtual networks
+ Add existing virtual network + Create new virtual network

Rule name	Virtual network	Subnet	Address



dosqlsrv01 | Firewalls and virtual networks ...

SQL server

Search (Ctrl+)

<< 3 **Save** Discard + Add client IP

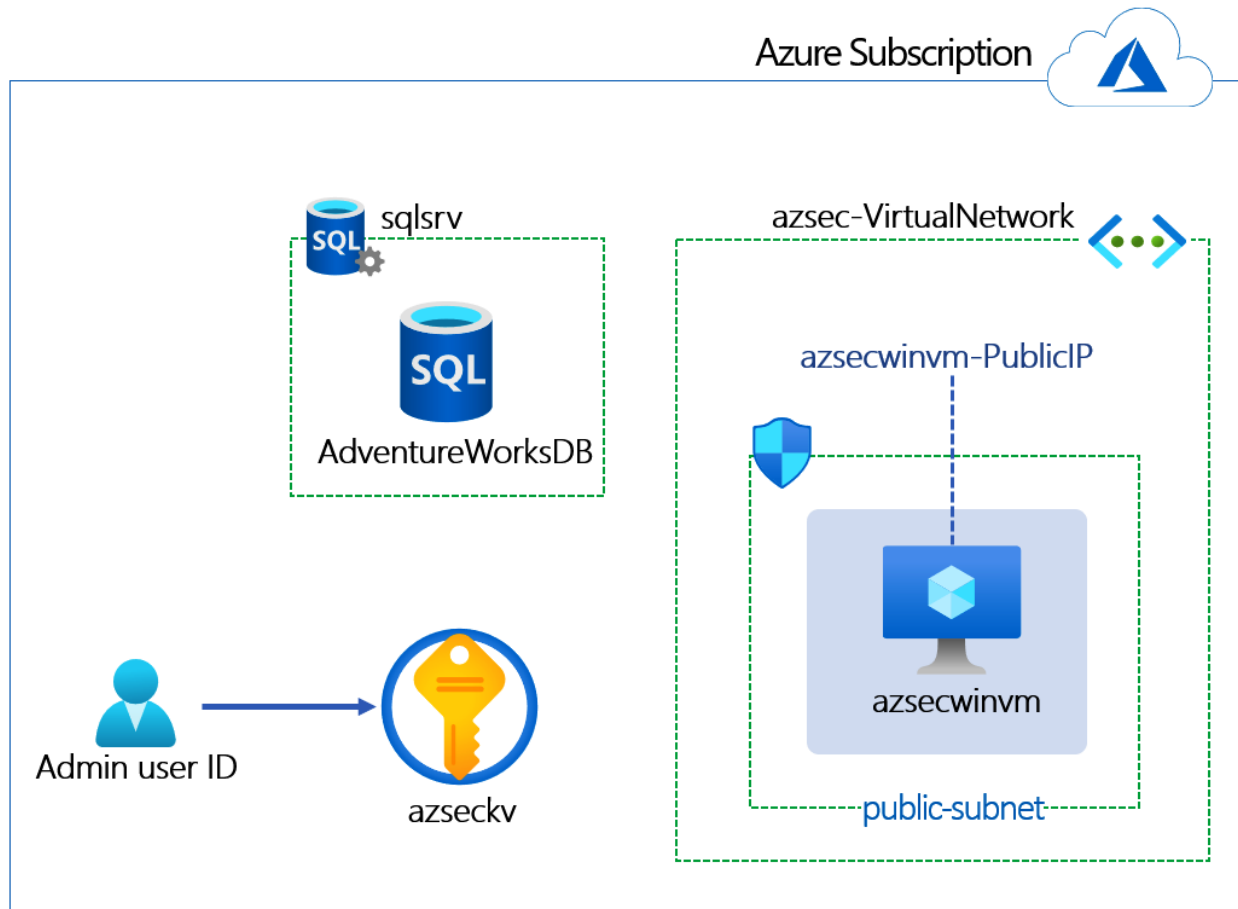
Security

- Auditing
- Firewalls and virtual networks** 1
- Private endpoint connections
- Security Center

Deny public network access ⓘ

2 **Yes** No

Click here to create a new private endpoint. [Create Private Endpoint](#)



```

Bash  ▾ | 🔌 ? ⚙️ 📄 { } 📄
Requesting a Cloud Shell. Succeeded.
Connecting terminal...

david@Azure:~$ az ad signed-in-user show --query objectId --output tsv
43bcb97a-ff4a-484d-989e-6db595fe86b4
david@Azure:~$
  
```

Azure Security Engineer Book - Chapter 11



Deploy to Azure



Visualize

Windows VM

- Windows Server 2019 Datacenter
- SQL Server Management Studio
- Google Chrome



Sign in

to continue to Microsoft Azure

No account? [Create one!](#)

[Can't access your account?](#)



[Sign in with a security key](#) 

Next

Custom deployment ...

Deploy from a custom template

Template



 Customized template 
9 resources



 Edit template

 Edit parameters



Project details


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


Subscription *  **1** AzureBlueTeam-PROD (88b69db8-c0e3-4873-9f9c-bc0cb08e945b) 


Resource group *  **2** (New) azuresec-c11-rg 
[Create new](#)



Instance details


Region *  **3** West Europe 


Storagename  [concat('azsecvmstrg', uniqueString(resourceGroup().id))]



Vm-dns  [concat('azsecwinvm-', uniqueString(resourceGroup().id))]


Admin User  azureadmin


Admin Password *  **4** 

Vmsize *  **1x Standard B2ms**
2 vcpus, 8 GB memory
[Change size](#)

Location  [resourceGroup().location]

Object Id *  **5** 43bcb97a-ff4a-484d-989e-6db595fe86b4 

_artifacts Location  [deployment().properties.templateLink.uri]

_artifacts Location Sas Token 


6 Review + create

< Previous

Next : Review + create >


Custom deployment ...

Deploy from a custom template

✓ Validation Passed 

Basics Review + create

Summary

 Customized template
9 resources

Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal terms

Create

< Previous

Next


Microsoft.Template-20210515133348 | Outputs ...


Deployment

Search (Ctrl+)

 Overview

 Inputs

 **Outputs** 1

 Template


winvmDNS

2

azsecwinvm-5e35jyex5eyrg.westeurope.cloudapp.azure.com 


winvmuser

3

azureadmin 


sqlserverName

4

sqlsrv5e35jyex5eyrg.database.windows.net 

sqladminuser

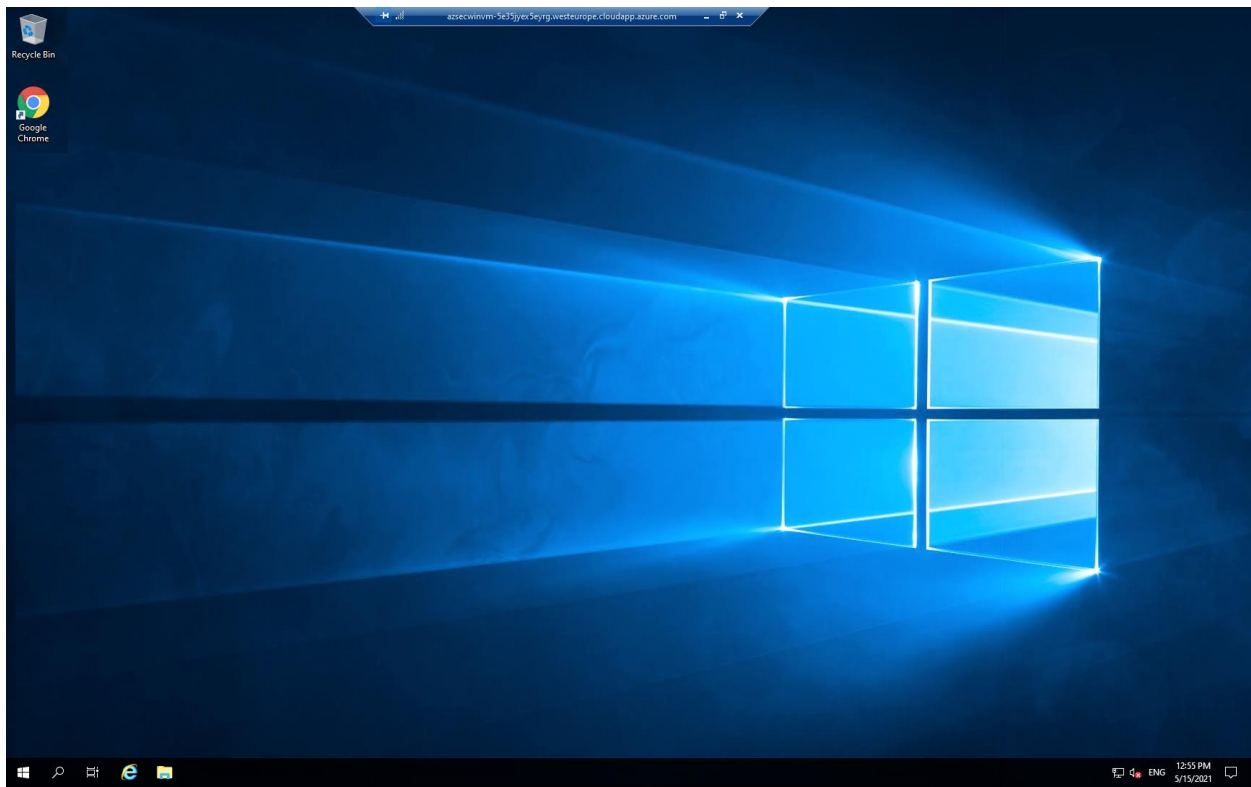
5

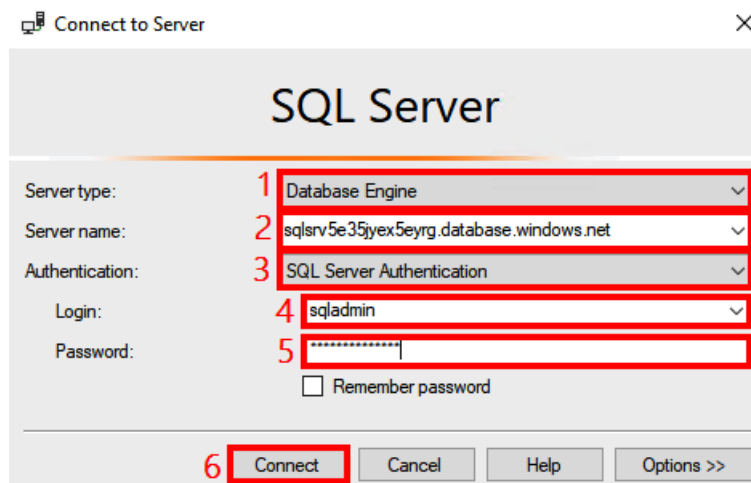
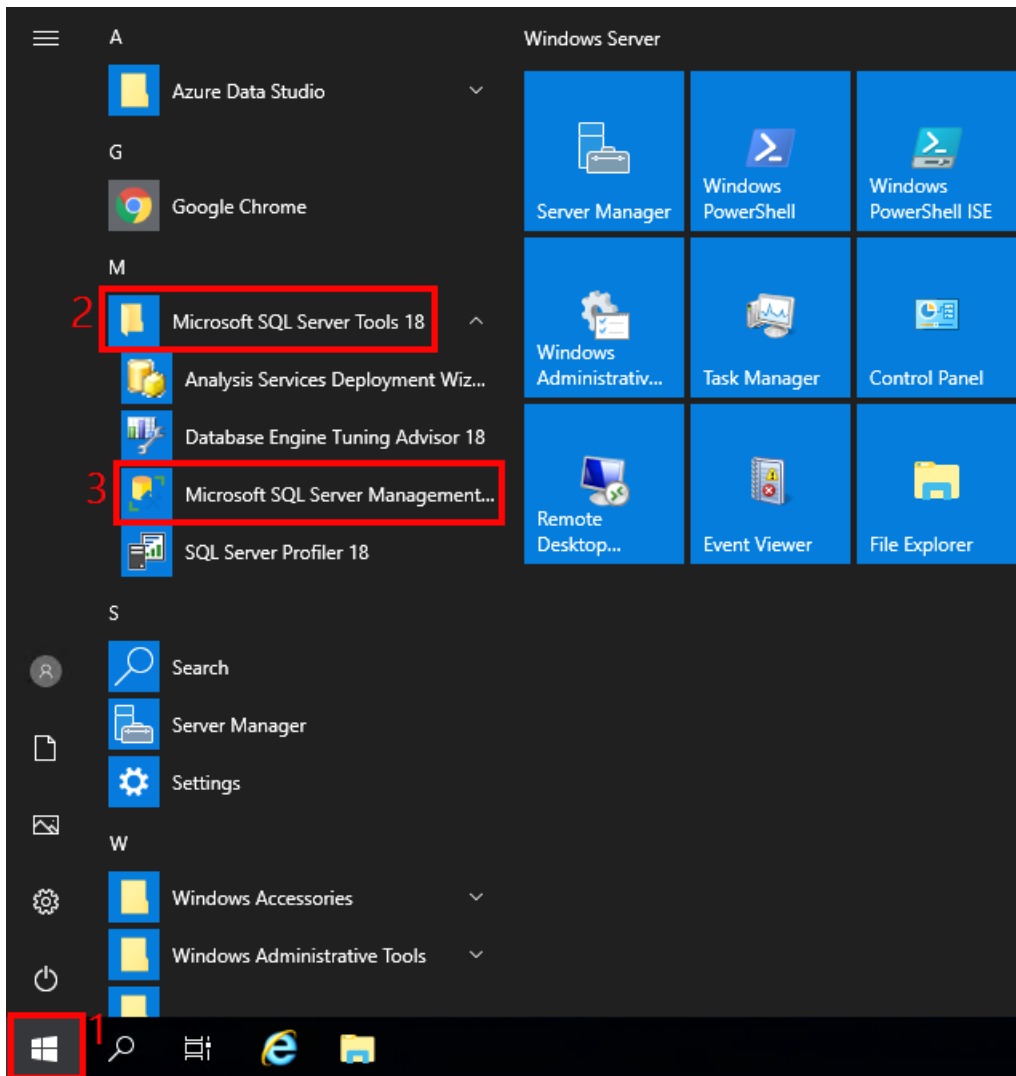
sqladmin 

keyVaultName

6

azseckv5e35jyex5eyrg 





New Firewall Rule

Your client IP address does not have access to the server. Sign in to an Azure account and create a new firewall rule to enable access.

Azure account

You are not signed in to Microsoft Azure

Sign In...

Firewall rule

Name ClientIPAddress_2021-05-15_03:11:46

Add my client IP address

40.114.218.155

Add my subnet IP address range

From 40.114.218.0 To 40.114.218.255

OK Cancel

New Firewall Rule

Your client IP address does not have access to the server. Sign in to an Azure account and create a new firewall rule to enable access.

Azure account

You are signed in as david-packt-az500@outlook.com. [Change user](#)

Firewall rule

Name **Allow-Lab-Windows-VM** 1

Add my client IP address

40.114.218.155

Add my subnet IP address range

From 40.114.218.0 To 40.114.218.255

2 **OK** Cancel


Microsoft Azure 1 →

sqlsrv

Services

No results were found.

Resources

2 →  sqlsrv5e35jyex5eyrg SQL server

sqlsrv5e35jyex5eyrg | Firewalls and virtual networks ...

Search (Ctrl+/)

Save Discard Add client IP

Import/Export history

Security

Auditing

Firewalls and virtual networks

Private endpoint connections

Security Center

Transparent data encryption

Intelligent Performance

Automatic tuning

Recommendations

Monitoring

Logs

Automation

Deny public network access ⓘ

Yes No

Click here to create a new private endpoint.
Create Private Endpoint

Minimum TLS Version ⓘ

1.0 1.1 1.2

Connection Policy ⓘ

Default Proxy Redirect

Allow Azure services and resources to access this server ⓘ

Yes No

Client IP address 86.147.112.228

Rule name	Start IP	End IP	
			...
Allow-Lab-Windows-VM	40.114.218.155	40.114.218.155	...

The firewall rule that was added

Microsoft Azure 1

sqlsrv

Azu

Services

No results were found.

Resources

2

sqlsrv5e35jyex5eyrg

SQL server



Search (Ctrl+ /)



2 **Set admin**



Remove admin



Save

Diagnose and solve problems

Quick start

Settings

1 **Active Directory admin**

SQL databases



Azure Active Directory authentication
your Azure SQL Database V12.

[Learn more](#)

Active Directory admin ⓘ

⊖ No Active Directory admin

Add admin



Active Directory admin

1

Search: Brenda

2

Brenda Tao
brenda@azureblueteam.io
Selected

Selected items



Brenda Tao
brenda@azureblueteam.io

Remove

Select

3



sqlsrv5e35jyex5eyrg | Active Directory admin ...

SQL server

Search (Ctrl+/)

<< Set admin Remove admin Save

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems



Azure Active Directory authentication allows your Azure SQL Database V12.

[Learn more](#)

Active Directory admin ⓘ

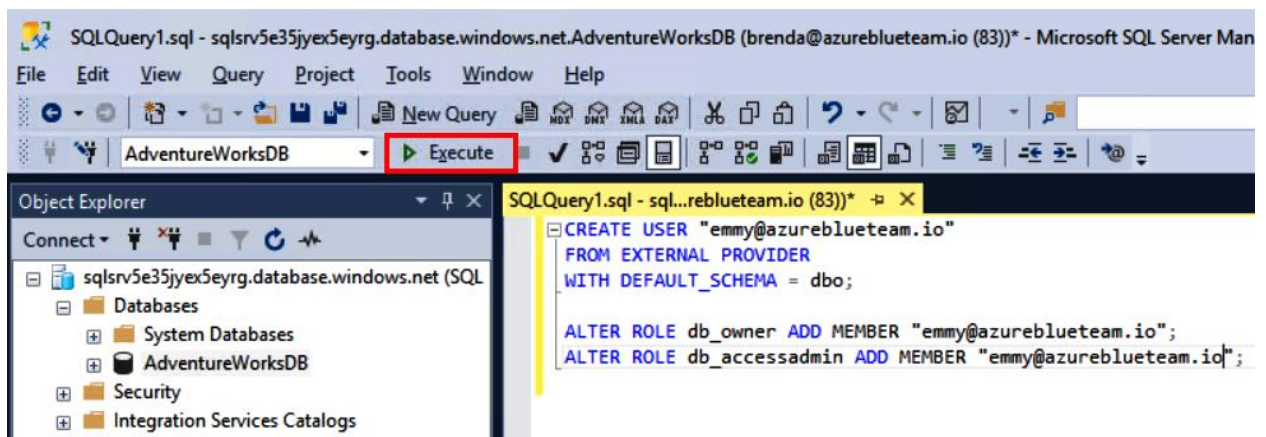
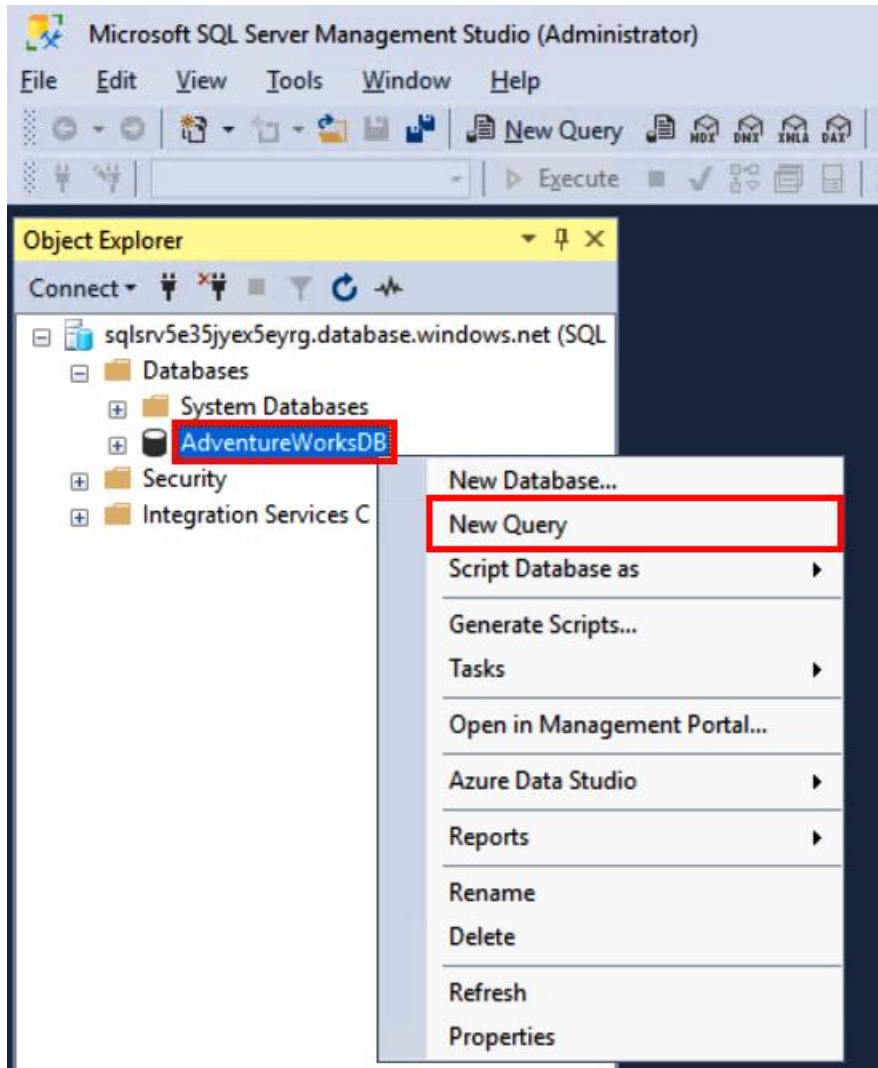
brenda@azureblueteam.io

Connect to Server

SQL Server

Server type:	Database Engine
Server name:	1 sqlsrv5e35jyex5eyrg.database.windows.net
Authentication:	2 Azure Active Directory - Universal with MFA
User name:	3 brenda@azureblueteam.io

4



SQL Server

Server type: Database Engine

Server name: 1 sqlsrv5e35jyex5eyrg.database.windows.net

Authentication: Azure Active Directory - Password

User name: 2 emmy@azureblueteam.io

Password: 3 [REDACTED]

Remember password

4

Connect Cancel Help Options >>

SQL Server

Login Connection Properties Always Encrypted Additional Connection Parameters

Type or select the name of the database for the connection.

Connect to database: 1 AdventureWorksDB

Network

Network protocol: <default>

Network packet size: 4096 bytes

Connection

Connection time-out: 30 seconds

Execution time-out: 0 seconds

Encrypt connection

Trust server certificate

Use custom color: [REDACTED] Select...

Reset All

2 Connect Cancel Help Options <<

Search (Ctrl+ /)

Save Discard Feedback

- Backups
- Deleted databases
- Failover groups
- Import/Export history
- Security**
- Auditing** 1
- Firewalls and virtual networks
- Private endpoint connections

Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure account, Log Analytics workspace or Event Hub. [Learn more about Azure SQL Auditing](#)

Enable Azure SQL Auditing ①



Audit log destination (choose at least one):

- Storage
- Log Analytics
- Event Hub

Auditing of Microsoft support operations

Search (Ctrl+ /)

Visit [Security Center](#) to manage security across your virtual net

- Backups
- Deleted databases
- Failover groups
- Import/Export history

Security

- Auditing
- Firewalls and virtual networks
- Private endpoint connections 1
- Security Center**
- Transparent data encryption

Recommendations Security alerts Findings

0 ! 0 ! -- !

Azure Defender for SQL

Azure Defender for SQL helps you strengthen your security posture, ide protect against threats on your SQL servers.

You are invited to a 30-day trial, free of charge. After the trial ends, you

[Enable Azure Defender for SQL](#) 2



AdventureWorksDB (sqlsrv5e35jyex5eyrg/

SQL database

Search (Ctrl+)



Save



Discard



Feedback

Security



Auditing



Data Discovery & Classification



Dynamic Data Masking



Security Center



Transparent data encryption

Intelligent Performance



Performance overview



Transparent data encryption en changes to your application. To

[Learn more](#)

Data encryption

ON

OFF

Encryption status



Encrypted



sqlsrv5e35jyex5eyrg | Transparent data encryption

SQL server

Search (Ctrl+)



Save



Discard



Feedback



Backups



Deleted databases



Failover groups



Import/Export history

Security



Auditing



Firewalls and virtual networks



Private endpoint connections



Security Center



Transparent data encryption

Intelligent Performance

Transparent data encryption

Transparent data encryption encrypts your databases, backups, and logs at rest without . encryption, go to each database. [Learn more](#)

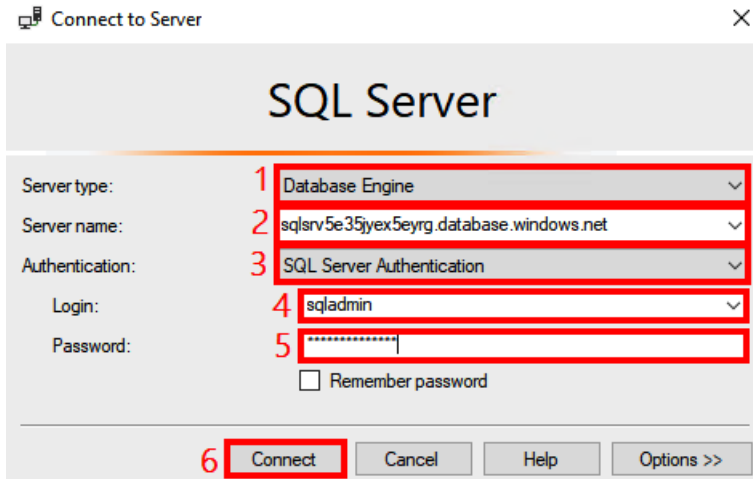
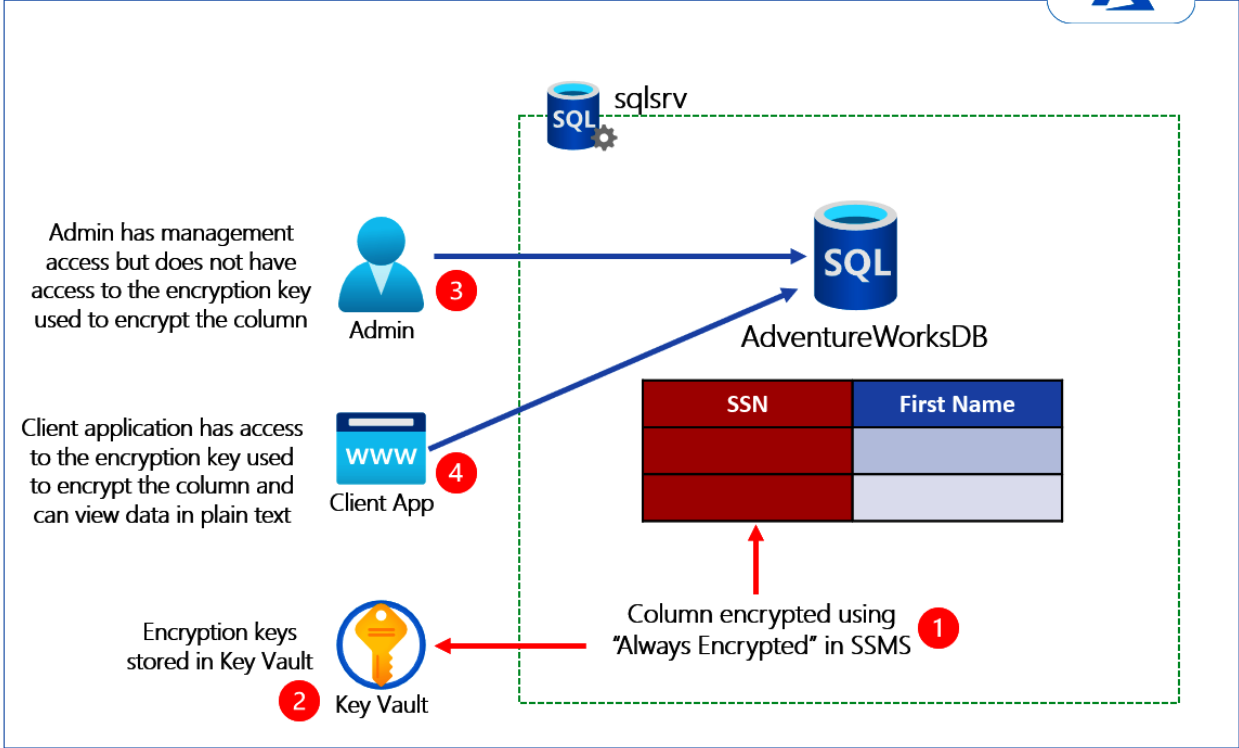
Transparent data encryption ⓘ

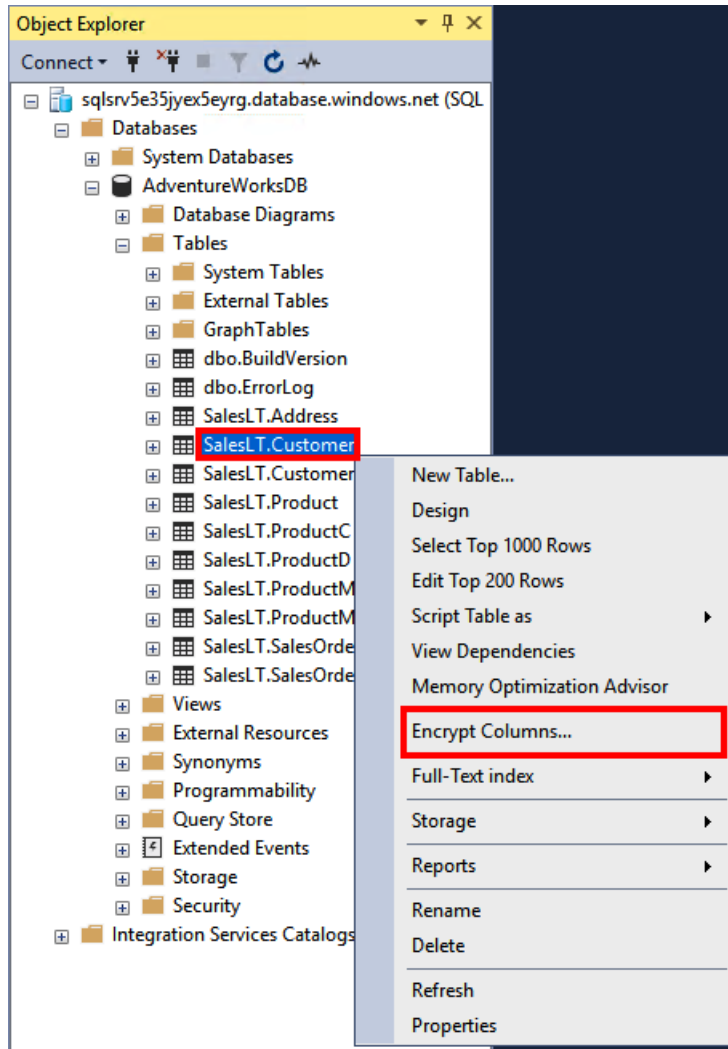
Service-managed key

Customer-managed key



You've chosen to use a service-managed key. Azure will automatically generate a key to







Column Selection

- Introduction
- Column Selection**
- Master Key Configuration
- Run Settings
- Summary
- Results

Help

Search column name...

Apply one key to all checked columns: CEK_Auto1 (New)

Encryption Type Encryption Key

Name	State	Encryption Type	Encryption Key
SalesLT.Customer			
<input type="checkbox"/> CustomerID			
<input type="checkbox"/> NameStyle	⊘		
<input type="checkbox"/> Title			
<input type="checkbox"/> FirstName			
<input type="checkbox"/> MiddleName			
<input type="checkbox"/> LastName			
<input type="checkbox"/> Suffix			
<input type="checkbox"/> CompanyName			
<input type="checkbox"/> SalesPerson			
<input type="checkbox"/> EmailAddress			
<input type="checkbox"/> Phone			
<input checked="" type="checkbox"/> PasswordHash	⚠	Deterministic	CEK_Auto1 (New)
<input checked="" type="checkbox"/> PasswordSalt	⚠	Deterministic	CEK_Auto1 (New)
<input type="checkbox"/> rowguid	⊘		
<input type="checkbox"/> ModifiedDate	⊘		

Show affected columns only

< Previous **Next >** Cancel



Master Key Configuration

Introduction Help

Column Selection

Master Key Configuration

Run Settings

Summary

Results

To generate a new column encryption key, a column master key must be selected to protect it. The column master key is stored outside of the database.

Select column master key:

Auto generate column master key

Select the key store provider:

- Windows certificate store
- 1** Azure Key Vault

2 You are signed in as david-packt-az500@outl
Select a subscription to use:

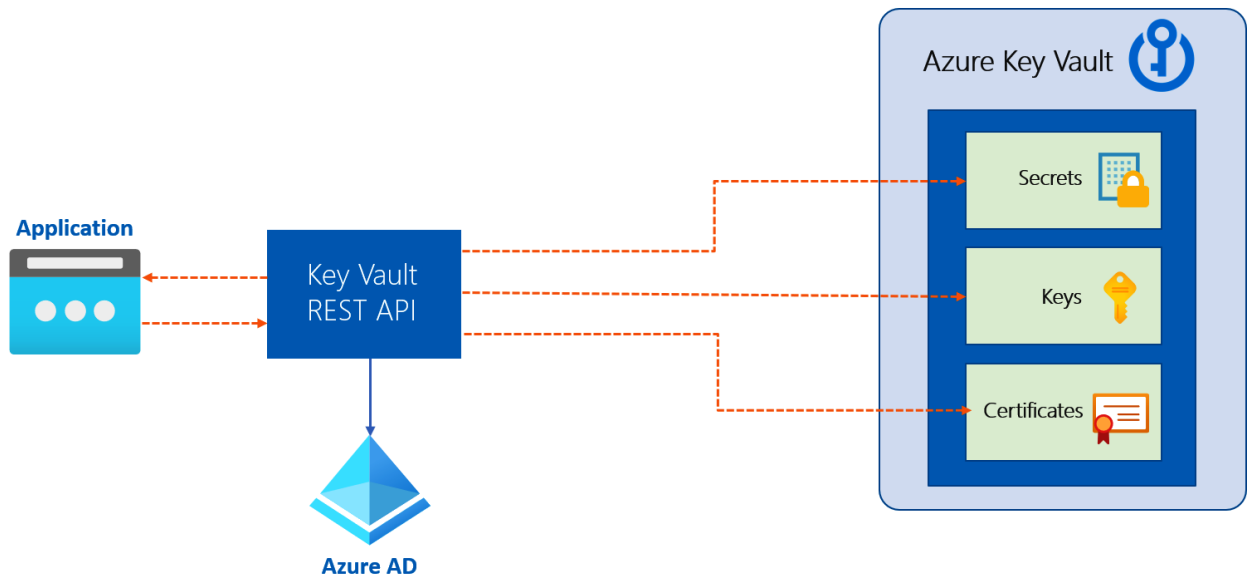
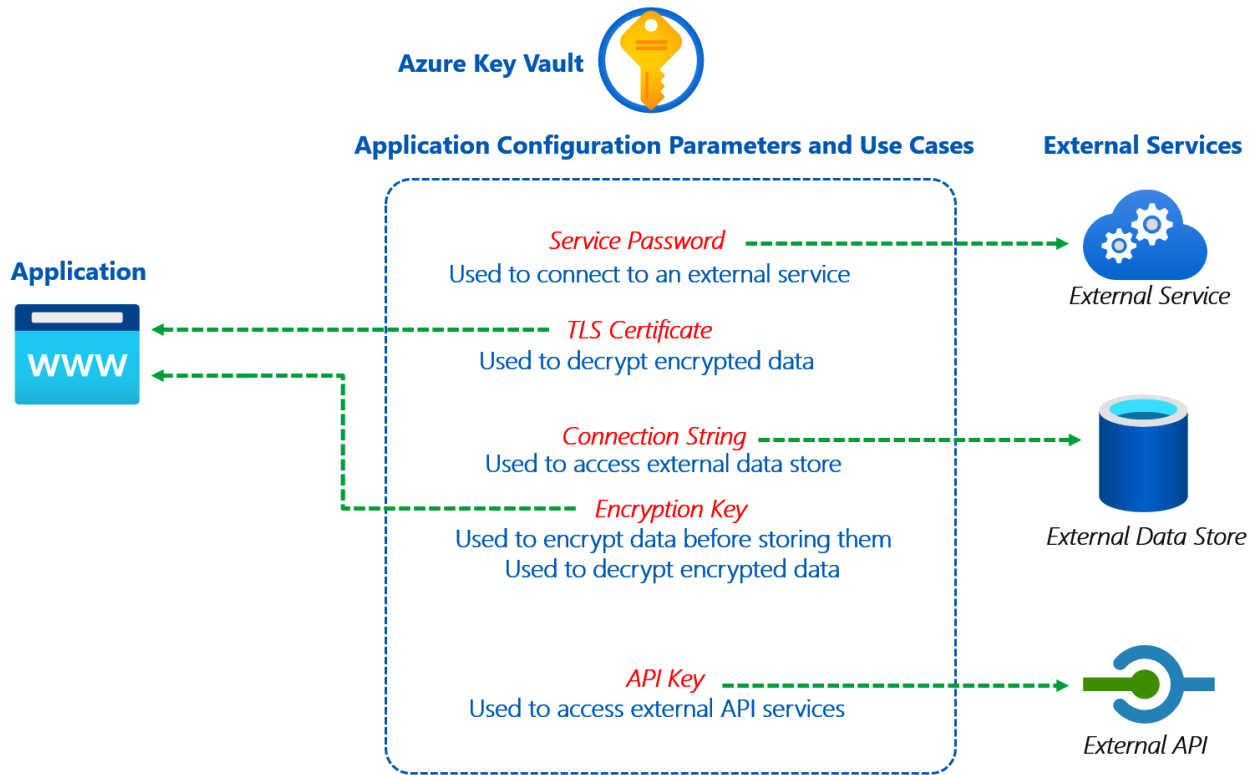
Select an Azure Key Vault:

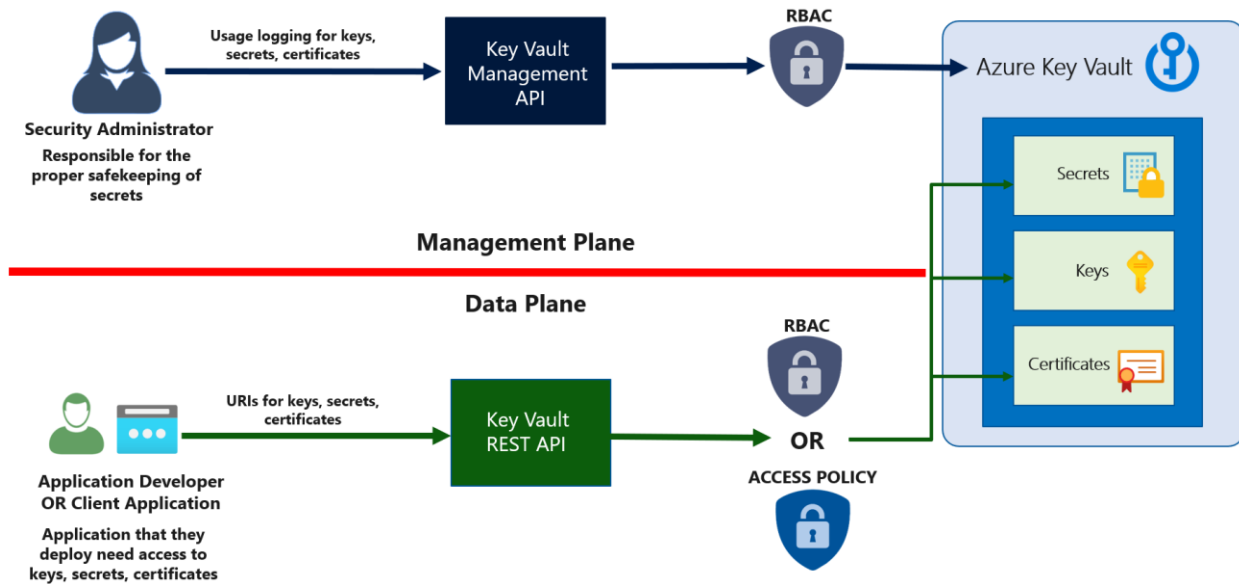
3 azsec-120321

4

< Previous **Next >** Cancel

Chapter 12: Implementing Secrets, Keys, and Certificate Management with Key Vault





Key Vault Built-In Roles	Description
Key Vault Administrator	Can perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets.
Key Vault Reader	Can read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as secret contents or key material.
Key Vault Certificates Officer	Can perform any action on the certificates of a key vault, except manage permissions.
Key Vault Crypto Officer	Can perform any action on the keys of a key vault, except manage permissions.
Key Vault Crypto Service Encryption User	Can read metadata of keys and perform wrap/unwrap operations.
Key Vault Crypto User	Can perform cryptographic operations using keys.
Key Vault Secrets Officer	Can perform any action on the secrets of a key vault, except manage permissions.
Key Vault Secrets User	Can read secret contents.

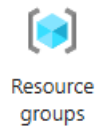
Enable Access to:

- Azure Virtual Machines for deployment ⓘ
- Azure Resource Manager for template deployment ⓘ
- Azure Disk Encryption for volume encryption ⓘ


```
david@Azure:~$ az ad sp create-for-rbac --name app-kv-test --skip-assignment
Changing "app-kv-test" to a valid URI of "http://app-kv-test", which is the req
The output includes credentials that you must protect. Be sure that you do not
more information, see https://aka.ms/azadsp-cli
{
  "appId": "ba79b485-8065-49fc-ab45-0740e85bcc4d",
  "displayName": "app-kv-test",
  "name": "http://app-kv-test",
  "password": "cX-R05AecZ1.ToSuq6Fx5a2M-8z0-~k0JQ",
  "tenant": "7f3"
}
```

Make a note of these

Azure services



Create a resource ...

- Get started
- Recently created
- Categories
 - AI + Machine Learning

1 Key Vault

KoçSistem Azure Key Vault Management

2 Key Vault

Create | Learn more

Create key vault ...

Basics Access policy Networking Tags Review + create

Project details

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

Subscription * 1 AzureBlueTeam-PROD (70bd6846-4c49-4397-8c48-a5e7b5274083) ✓
Resource group * 2 (New) azuresec-c12-rg ✓
[Create new](#)

Instance details

Key vault name * ⓘ 3 azseckv0000 ✓
Region * 4 West Europe ✓

Soft-delete ⓘ Enabled
Days to retain deleted vaults * ⓘ 90
Purge protection ⓘ
5 Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)
 Disable purge protection (allow key vault and objects to be purged during retention period)
ⓘ Once enabled, this option cannot be disabled

[Review + create](#) < Previous **Next : Access policy >** 6

Basics **Access policy** Networking Tags Review + create

Enable Access to:

- Azure Virtual Machines for deployment ⓘ
- Azure Resource Manager for template deployment ⓘ
- Azure Disk Encryption for volume encryption ⓘ

Permission model


- Vault access policy
- 1** **Azure role-based access control**


2 Review + create


< Previous

Next : Networking >

 Delete  Cancel  Redeploy  Refresh

 We'd love your feedback! →

 **Your deployment is complete**

 Deployment name: azseckv0000
Subscription: [AzureBlueTeam-PROD \(70bd6846-4c49-4397-8c48-a5...](#)
Resource group: [azuresec-c12-rg](#)

∨ **Deployment details** ([Download](#))

∧ **Next steps**

Go to resource

Search (Ctrl+/)

+ Generate/Import Refresh Restore Backup

Settings

- Keys
- Secrets**
- Certificates
- Access policies

 The operation is not allowed by RBAC. If role assignments

Name	Type
------	------

You are unauthorized to view these contents.



Search (Ctrl+/)

<< 2 + Add Download role assignments

- Overview
- Activity log
- Access control (IAM) 1**
- Tags
- Diagnose and solve problems

- Add role assignment 3**
- Add role assignment (Preview)
- Add co-administrator

View my level of access to this resource.

[View my access](#)

Add role assignment



Role ⓘ


Key Vault Administrator ⓘ 1

Assign access to ⓘ

User, group, or service principal 2

Select ⓘ

Search by name or email address

 AAD DC Administrators

Selected members:

 David Okeyode
david-packt-az500_outlook.com#EXT... [Remove](#) 3

4

Upload options

Manual

Name * ⓘ

1 Api-Key ✓

Value * ⓘ

2 ✓

Content type (optional)

Set activation date ⓘ

Set expiration date ⓘ

Enabled

Yes No

Create 3



Api-Key | Access control (IAM) ...

Versions

Search (Ctrl+)

<< 2

+ Add



Download role assignments



Overview



Access control (IAM)

1

Add role assignment 3

Add role assignment (Preview)

Add co-administrator

View my level of access to this resource.

View my access

ts Roles


Role ⓘ
Key Vault Secrets User ⓘ 1

Assign access to ⓘ
User, group, or service principal


Select ⓘ
app-kv-test 2

No users, groups, or service principals found.


Selected members:


 app-kv-test 3 [Remove](#)

[Save](#) 4 [Discard](#)

 **Api-Key** ...
Versions

<< [+ New Version](#) [Refresh](#) [Delete](#)

 Overview 1

 Access control (IAM)

Version

CURRENT VERSION

2



378ff3dbb0de4f3f824d713e57feadc4

Secret Version



Save



Discard

Properties

Created 6/6/2021, 10:13:48 AM

Updated 6/6/2021, 10:13:48 AM

Secret Identifier

<https://azseckv0000.vault.azure.net/secrets/Api-Key/378ff3dbb...>

Settings

Set activation date ⓘ

```
Bash | v | ⏻ | ? | ⚙️ | 📄 | 📄 | {} | 📄 | 📄
david@Azure:~$
david@Azure:~$ az login --service-principal --username "ba79b485-8065-49fc-ab45-0740e85bcc4d" --password "cX-R05AecZl.ToSuq6Fx5a2M-8z0-~k0JQ" --tenant "7f3-8065-49fc-ab45-0740e85bcc4d"
Cloud Shell is automatically authenticated under the initial account signed-in with.
Run 'az login' only if you need to use a different account
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "7f3-8065-49fc-ab45-0740e85bcc4d",
    "id": "70bd6846-4c49-4397-8c48-a5e7b5274083",
    "isDefault": true,
    "managedByTenants": [],
    "name": "AzureBlueTeam-PROD",
```

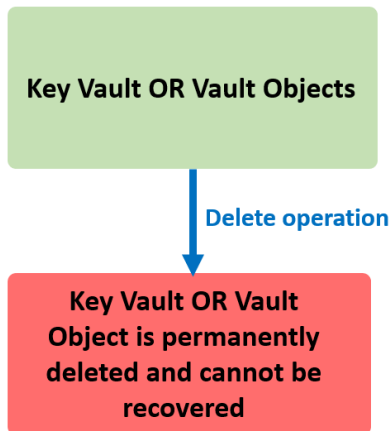


```

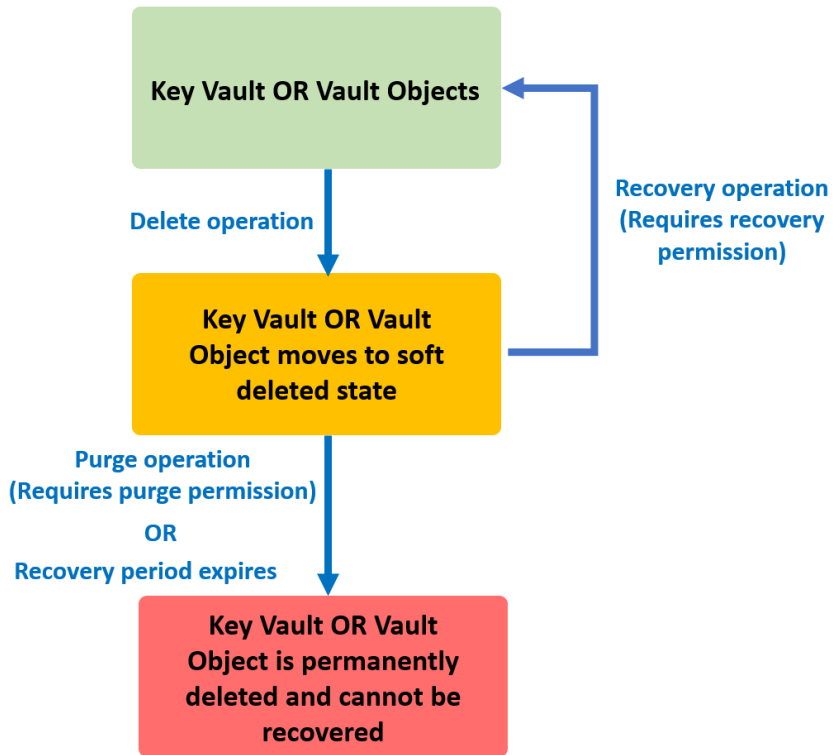
david@Azure:~$ curl https://azseckv0000.vault.azure.net/secrets/Api-Key/378ff3dbb0de4f3f824d713e57feadc4?api-version=2016-10-01 -H "Authorization: Bearer $token" | jq
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left  Speed
100    215    100    215     0     0    589     0   -:--:--  -:--:--  -:--:--   587
{
  "value": "123456789",
  "id": "https://azseckv0000.vault.azure.net/secrets/Api-Key/378ff3dbb0de4f3f824d713e57feadc4",
  "attributes": {
    "enabled": true,
    "created": 1622970828,
    "updated": 1622970828,
    "recoveryLevel": "Recoverable"
  }
}

```

Without soft delete protection



With soft delete and/or purge protection



Microsoft Azure

azseckv 1

Services

No results were found.

Resources

azseckv0000 2 Key vault

azseckv0000 | Secrets ...

Key vault

Search (Ctrl+/) << + Generate/Import Refresh

Settings

- Keys
- Secrets 1
- Certificates

Name

Api-Key 2

Api-Key ...

Versions

Search (Ctrl+/) << + New Version Refresh Delete 1 Download Backup

Overview

Access control (IAM)

Are you sure that you want to delete this resource?
Soft delete is enabled for this key vault. You can restore your deleted secret

2 Yes No

Search (Ctrl+/)

Generate/Import Refresh Restore Backup **Manage deleted secrets**

Settings

Keys

Secrets

Name	Type
There are no secrets available.	

Manage deleted secrets

i Purge protection is enabled for all items within this key vault.

Recover or purge deleted secrets.

Secrets

Refresh

<input type="checkbox"/>	Name ↑	Deleted date	Scheduled purge date
1 <input checked="" type="checkbox"/>	Api-Key	June 6, 2021	September 4, 2021

Greyed out because purge protection is enabled
All items have loaded

3 **Recover** Purge Cancel

Generate/Import **Refresh** Restore Backup Manage deleted secrets

Name	Type
Api-Key	← Recovered secret



Api-Key ...

Versions

Search (Ctrl+/) <<

Overview

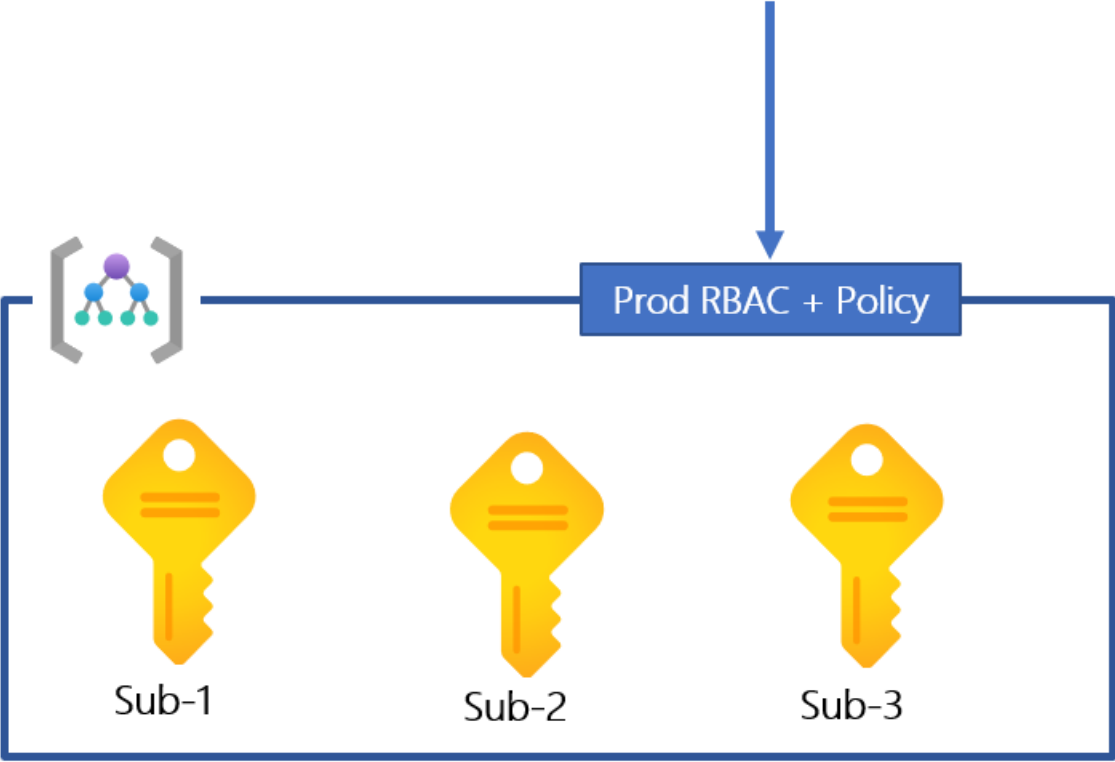
Access control (IAM)

+ New Version ↻ Refresh 🗑 Delete **↓ Download Backup**

Version	Status
CURRENT VERSION	
378ff3dbb0de4f3f824d713e57feadc4	✓ Enabled

Chapter 13: Azure Cloud Governance and Security Operations

Governance Controls applied ONCE for multiple subscriptions





Management groups

Default Directory



Overview

Get started

Settings



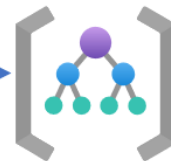
No management groups to display

Organize your subscriptions into groups called "management groups" to help you manage access, policy and compliance across your subscriptions. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have. [Learn more](#)



Start using management groups

Global Governance Controls



ROOT MANAGEMENT GROUP



PRODUCTION



ENGINEERING



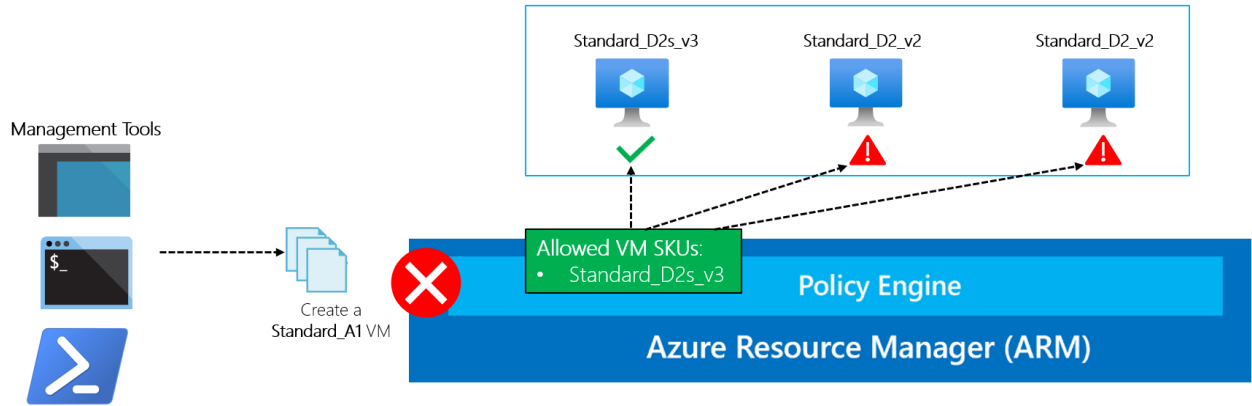
DEVELOPMENT



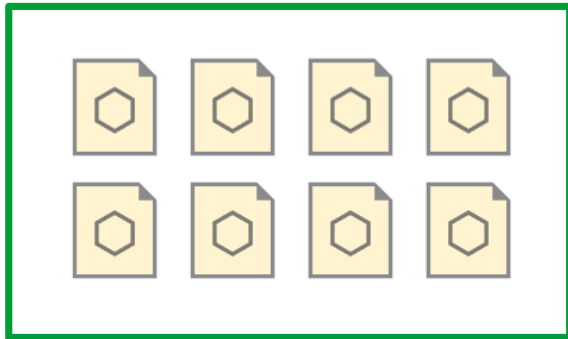
SRE-TEAM-SUB



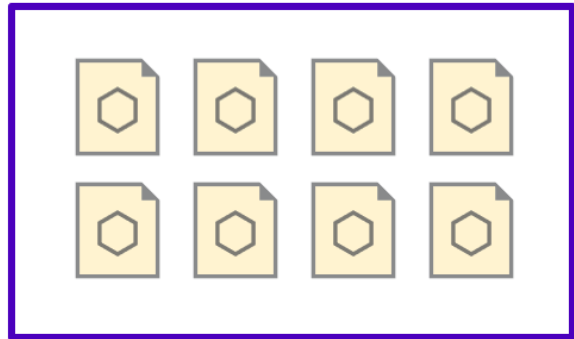
BILLING-SUB

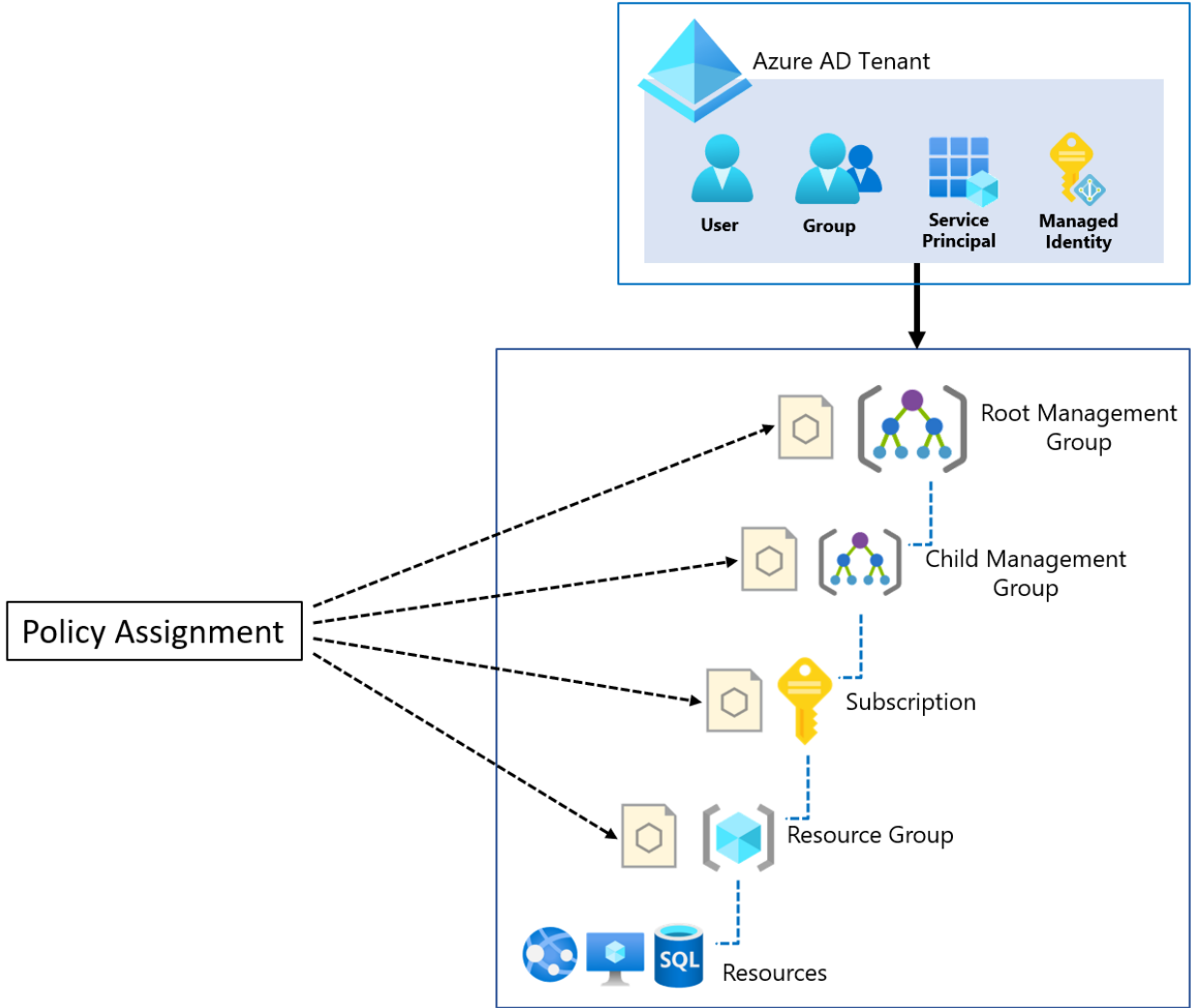


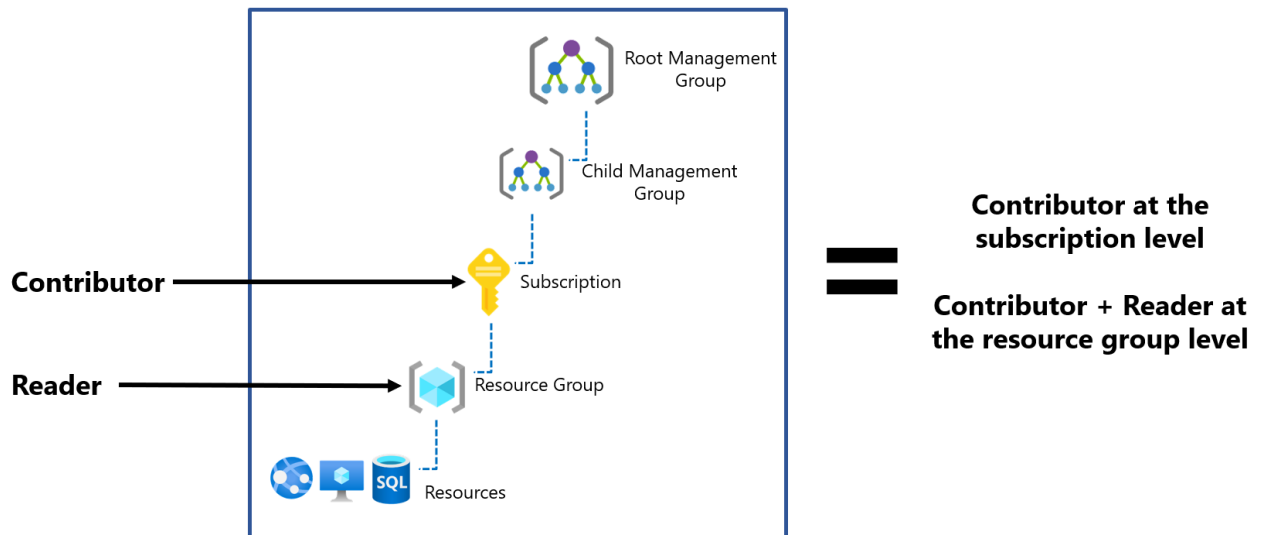
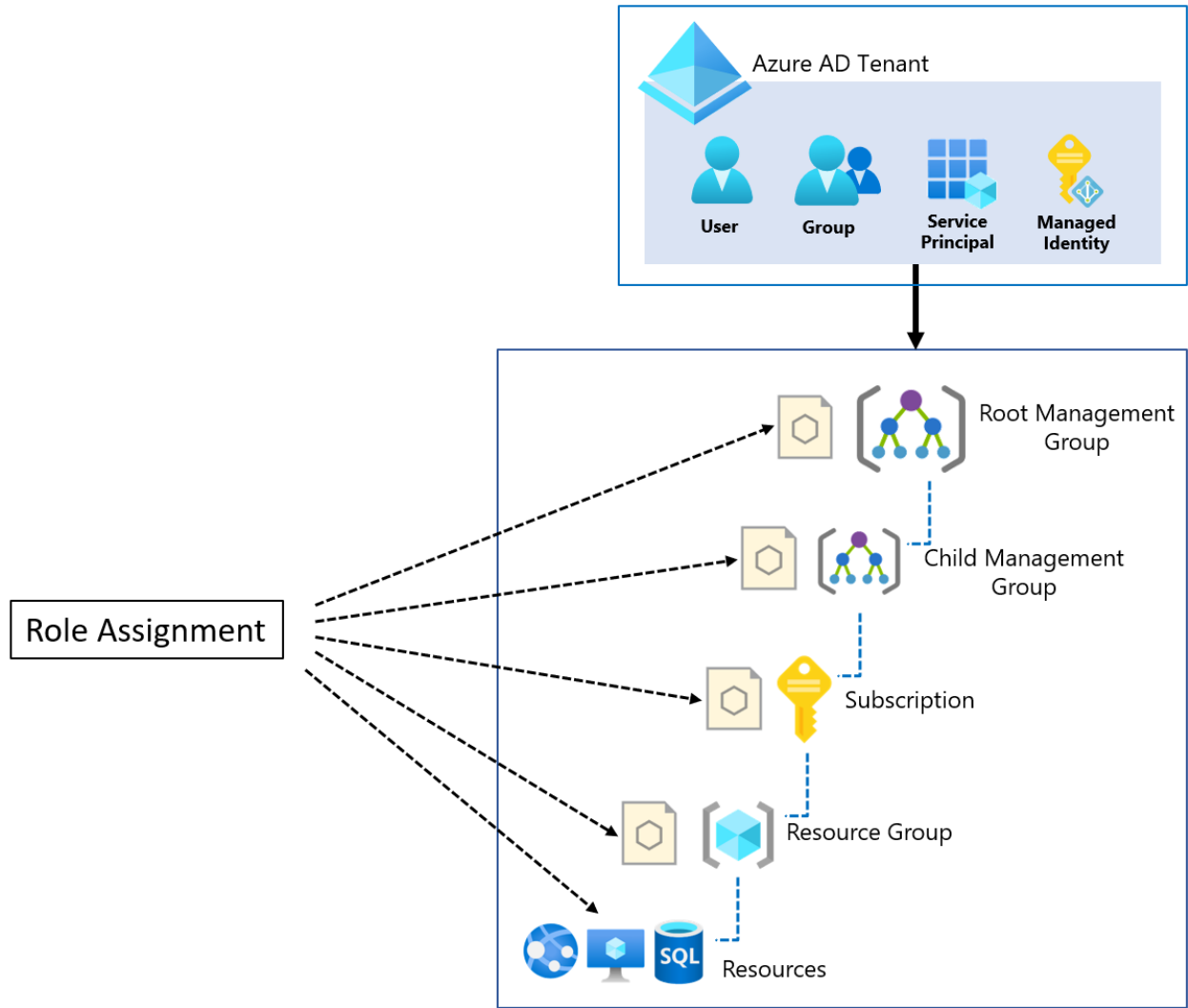
Security Initiative Security related policies

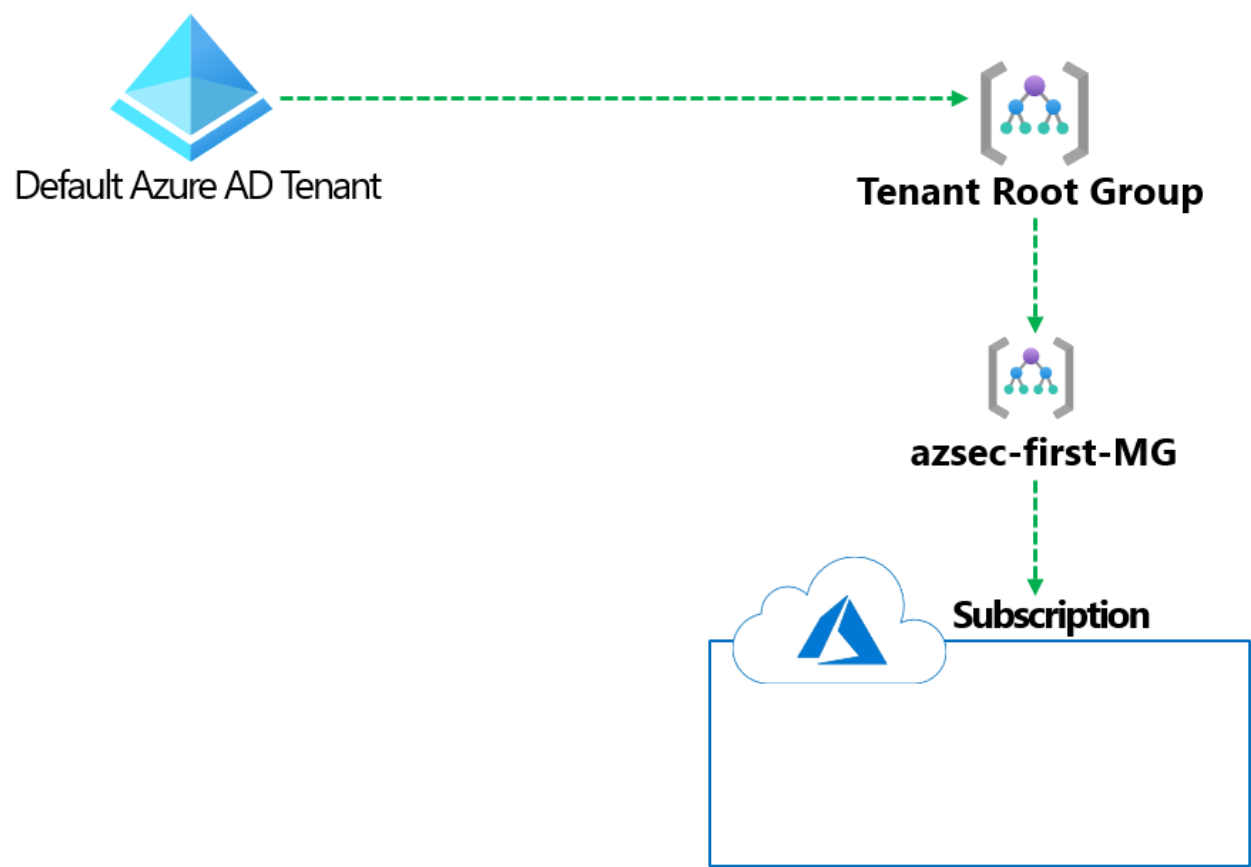
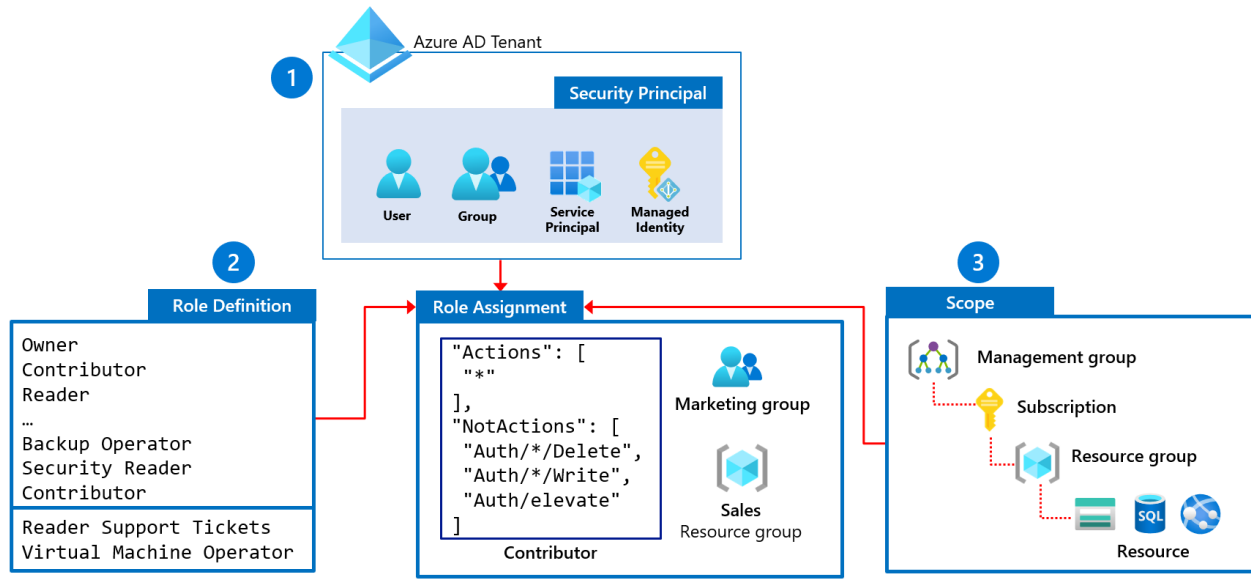


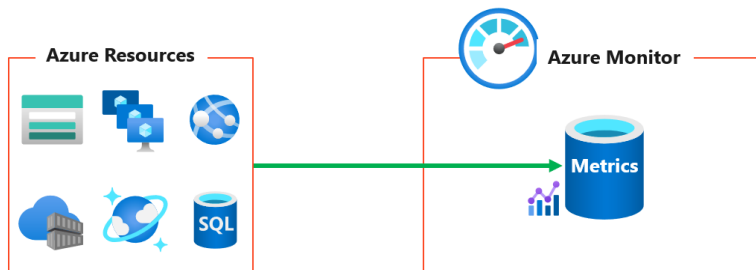
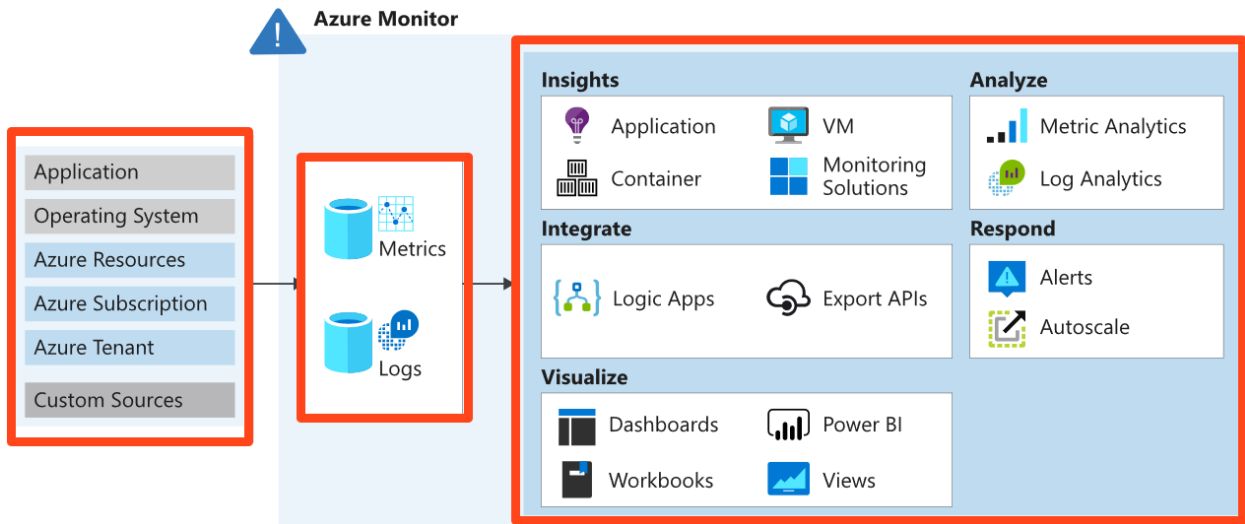
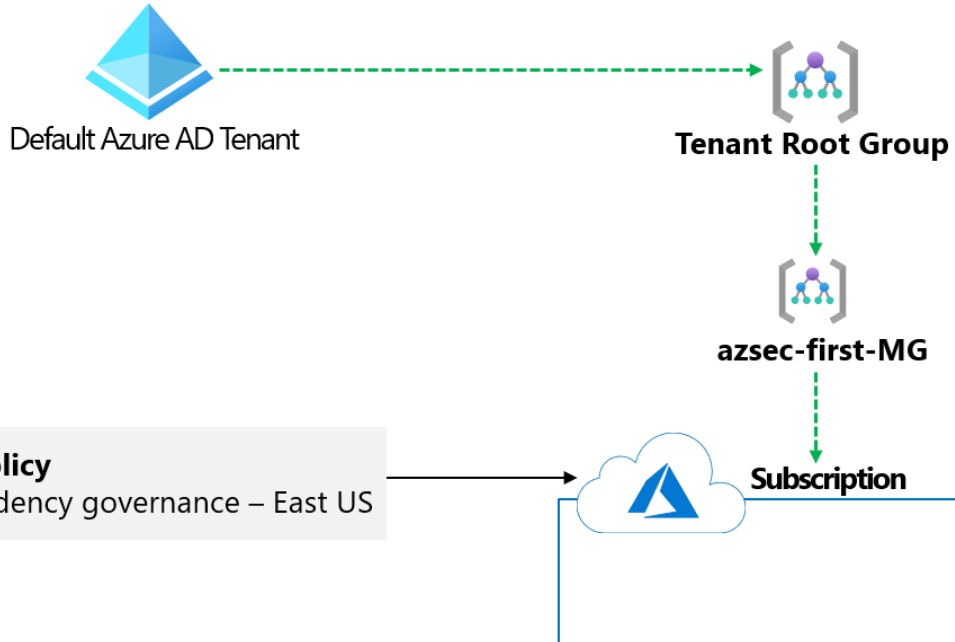
PCI-DSS Initiative Compliance related policies



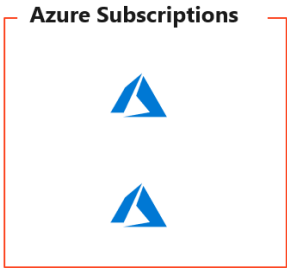








Analyse and Visualize using Metrics Explorer
Visualize using Azure Monitor Workbooks
Alert using a metrics alert rule
 Used as a **trigger** for autoscale events
Export to a Log Analytics workspace for event correlation and further analysis



View, Query and Filter using the Activity log menu
Alert using an activity log alert rule
Used as a **trigger** for automated events
Export to a Log Analytics workspace for event correlation and further analysis



azseckv0000 | Diagnostic settings

Search (Ctrl+ /)

Refresh Feedback

Networking

Security

Properties

Locks

Monitoring

Insights

Alerts

Metrics

Diagnostic settings 1

Logs

Workbooks

Diagnostic settings are used to configure streaming export of platform and metrics to independent destinations. [Learn more about diagnostic](#)

Diagnostic settings

Name	Storage account
------	-----------------

No diagnostic settings defined

2 [+ Add diagnostic setting](#)

Click 'Add Diagnostic setting' above to configure the collection of the

- AuditEvent
- AllMetrics

pentestvm | Diagnostic settings

Virtual machine

Search (Ctrl+/) Save Discard

Policies

Run command

Monitoring

- Insights
- Alerts
- Metrics
- Diagnostic settings 1**
- Logs
- Connection monitor (classic)
- Workbooks

Automation

- Tasks (preview)
- Export template

Overview Performance counters Logs Crash dumps Sinks Agent

Azure Monitoring collects host-level metrics - like CPU utilization, disk and network usage - for all virtual machines without any additional software. For more insight into this virtual machine, you can collect guest-level metrics, logs, and other diagnostic data using the Azure Diagnostics agent. You can also send diagnostic data to other services like Application Insights. [Learn more](#)

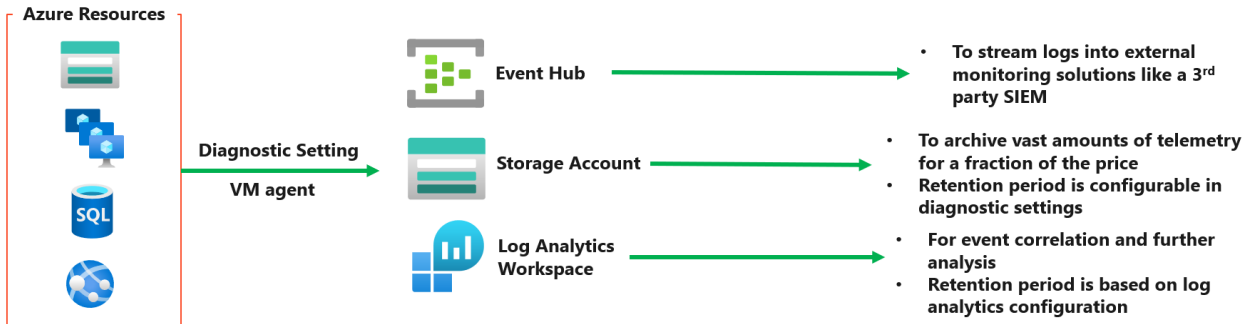
To get started now, choose a storage account below where diagnostic data will be sent and then click the button labeled 'Enable guest-level diagnostics'.

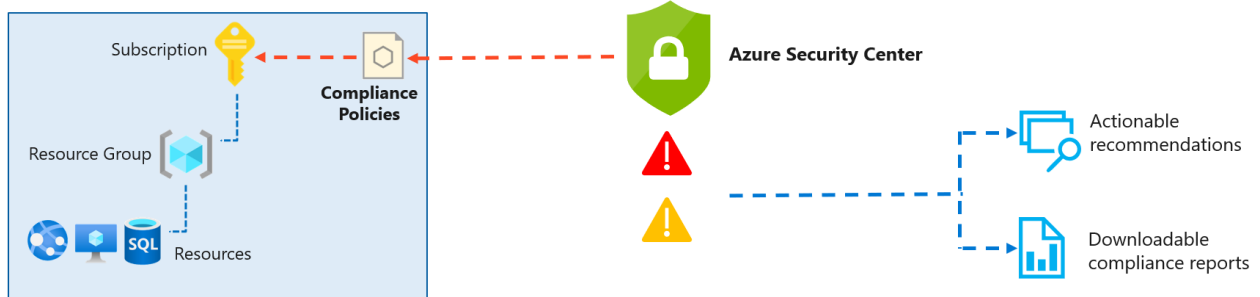
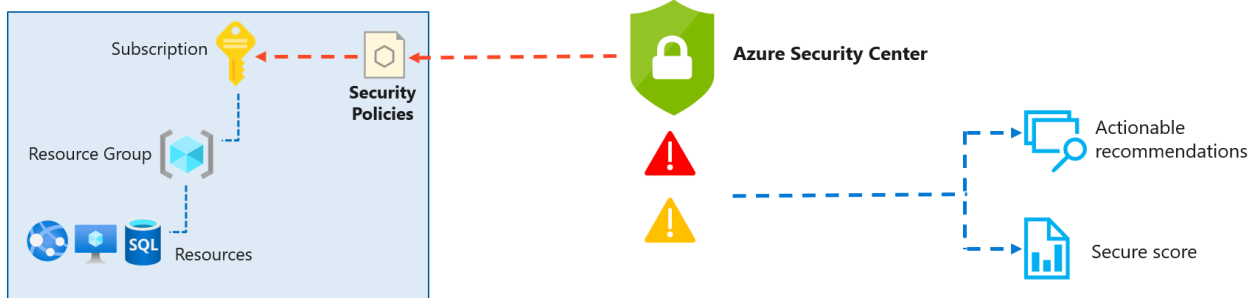
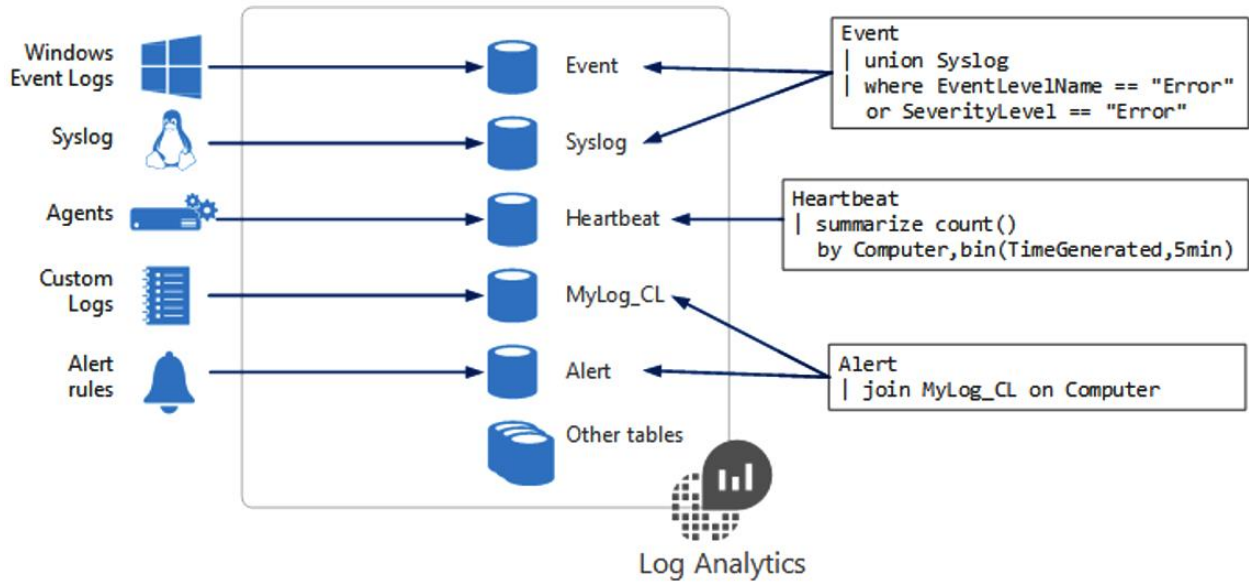
Diagnostics storage account *

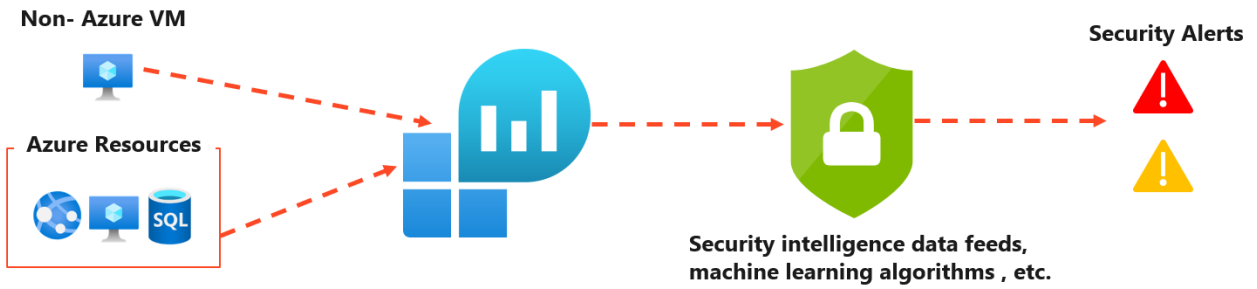
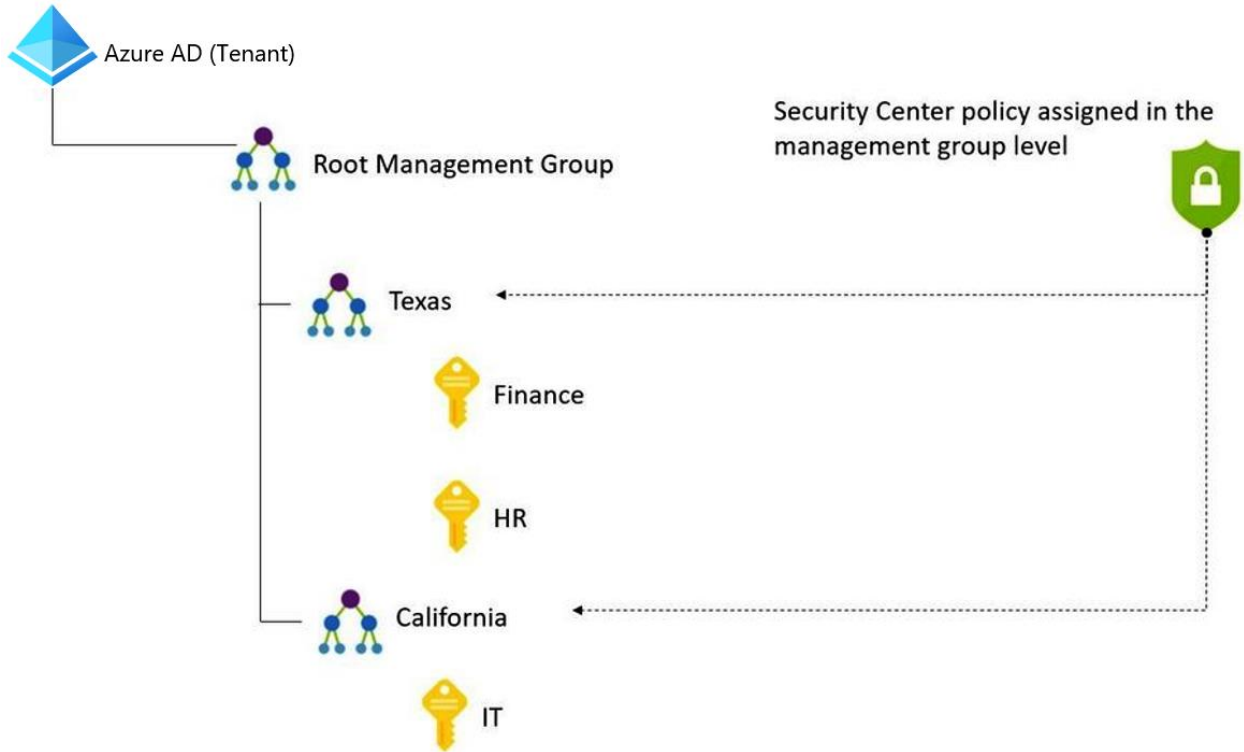
ptvmstrghuxrda64ba3qe

[Create new](#)

2 Enable guest-level monitoring









Collect

Security data across
your enterprise



Respond

Rapidly and
automate protection



Detect

Threats with vast
threat intelligence &
AI



Investigate

Critical incidents
guided by AI



**Log Analytics
Workspace**



Azure Sentinel

