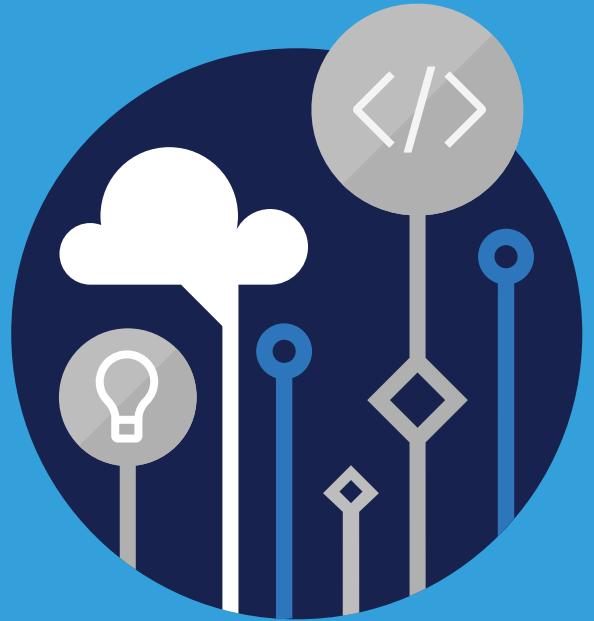


Microsoft
Official
Course



AZ-104T00

Microsoft Azure
Administrator

AZ-104T00

Microsoft Azure Administrator

II Disclaimer

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2019 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <http://www.microsoft.com/trademarks>¹ are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

¹ <http://www.microsoft.com/trademarks>

MICROSOFT LICENSE TERMS

MICROSOFT INSTRUCTOR-LED COURSEWARE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

**BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS.
IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.**

If you comply with these license terms, you have the rights below for each license you acquire.

1. DEFINITIONS.

1. "Authorized Learning Center" means a Microsoft Imagine Academy (MSIA) Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
2. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.
3. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
4. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of an MPN Member (defined below), or (iii) a Microsoft full-time employee, a Microsoft Imagine Academy (MSIA) Program Member, or a Microsoft Learn for Educators – Validated Educator.
5. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
6. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.
7. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics, or Microsoft Business Group courseware.
8. "Microsoft Imagine Academy (MSIA) Program Member" means an active member of the Microsoft Imagine Academy Program.
9. "Microsoft Learn for Educators – Validated Educator" means an educator who has been validated through the Microsoft Learn for Educators program as an active educator at a college, university, community college, polytechnic or K-12 institution.
10. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
11. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies.
12. "MPN Member" means an active Microsoft Partner Network program member in good standing.

13. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
 14. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.
 15. "Trainer" means (i) an academically accredited educator engaged by a Microsoft Imagine Academy Program Member to teach an Authorized Training Session, (ii) an academically accredited educator validated as a Microsoft Learn for Educators – Validated Educator, and/or (iii) a MCT.
 16. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.
2. **USE RIGHTS.** The Licensed Content is licensed, not sold. The Licensed Content is licensed on a **one copy per user basis**, such that you must acquire a license for each individual that accesses or uses the Licensed Content.
- 2.1 Below are five separate sets of use rights. Only one set of rights apply to you.
 1. **If you are a Microsoft Imagine Academy (MSIA) Program Member:**
 1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
 2. For each license you acquire on behalf of an End User or Trainer, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
 2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content.
 3. For each license you acquire, you must comply with the following:
 1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 2. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
 3. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End

User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

4. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
6. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
7. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

2. If you are a Microsoft Learning Competency Member:

1. Each license acquire may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
2. For each license you acquire on behalf of an End User or MCT, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
 2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. you will provide one (1) MCT with the unique redemption code and instructions on how they can access one (1) Trainer Content.
3. For each license you acquire, you must comply with the following:
 1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 2. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
 3. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

4. you will ensure that each MCT teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
6. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
7. you will only provide access to the Trainer Content to MCTs.

3. If you are a MPN Member:

1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
2. For each license you acquire on behalf of an End User or Trainer, you may either:
 1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
 2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
 3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content.
3. For each license you acquire, you must comply with the following:
 1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 2. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
 3. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
 4. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,

5. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
6. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
7. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
8. you will only provide access to the Trainer Content to Trainers.

4. If you are an End User:

For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

5. If you are a Trainer.

1. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.

2. If you are an MCT, you may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement.
3. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "customize" refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

- 2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.
- 2.3 **Redistribution of Licensed Content.** Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.
- 2.4 **Third Party Notices.** The Licensed Content may include third party code that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code are included for your information only.
- 2.5 **Additional Terms.** Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. **LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY.** If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("Pre-release"), then in addition to the other provisions in this agreement, these terms also apply:
 1. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.
 2. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.
 3. **Pre-release Term.** If you are an Microsoft Imagine Academy Program Member, Microsoft Learning Competency Member, MPN Member, Microsoft Learn for Educators – Validated Educator, or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("Pre-release term"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.
4. **SCOPE OF LICENSE.** The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
 - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
 - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
 - modify or create a derivative work of any Licensed Content,
 - publicly display, or make the Licensed Content available for others to access or use,
 - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
 - work around any technical limitations in the Licensed Content, or
 - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.
5. **RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property

laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.

6. **EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
7. **SUPPORT SERVICES.** Because the Licensed Content is provided "as is", we are not obligated to provide support services for it.
8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
9. **LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
11. **APPLICABLE LAW.**
 1. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
 2. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.
12. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
13. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
14. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US\$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

This limitation applies to

- anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential, or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 \$ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised April 2019



Contents

■	Module 0 Start Here	1
	Start Here	1
■	Module 1 Administer Identity	7
	Configure Azure Active Directory	7
	Configure User and Group Accounts	16
	Module 01 Lab	23
■	Module 2 Administer Governance and Compliance	27
	Configure Subscriptions	27
	Configure Azure Policy	38
	Configure Role-Based Access Control	47
	Module 02 Lab	56
■	Module 3 Administer Azure Resources	63
	Configure Azure Resources with Tools	63
	Use Azure Resource Manager	74
	Configure Resources ARM Templates	83
	Module 03 Lab	92
■	Module 4 Administer Virtual Networking	101
	Configure Virtual Networks	101
	Configure Network Security Groups	111
	Configure Azure Firewall	117
	Configure Azure DNS	123
	Module 04 Lab	135
■	Module 5 Administer Intersite Connectivity	141
	Configure VNet Peering	141
	Configure VPN Gateway	147
	ExpressRoute and Virtual WAN	158
	Module 05 Lab	166
■	Module 6 Administer Network Traffic	171
	Configure Network Routing and Endpoints	171
	Configure Azure Load Balancer	182
	Configure Azure Application Gateway	191
	Module 06 Lab	198

■	Module 7 Administer Azure Storage	203
	Configure Storage Accounts	203
	Configure Blob Storage	214
	Configure Storage Security	224
	Configure Azure Files and File Sync	234
	Configure Storage with Tools	246
	Module 07 Lab	256
■	Module 8 Administer Azure Virtual Machines	267
	Configure Virtual Machines	267
	Configure Virtual Machine Availability	283
	Configure Virtual Machine Extensions	295
	Module 08 Lab	301
■	Module 9 Administer PaaS Compute Options	307
	Configure Azure App Service Plans	307
	Configure Azure App Services	315
	Configure Azure Container Instances	330
	Configure Azure Kubernetes Service	338
	Module 09 Lab	350
■	Module 10 Administer Data Protection	357
	Configure File and Folder Backups	357
	Configure Virtual Machine Backups	369
	Module 10 Lab	381
■	Module 11 Administer Monitoring	387
	Configure Azure Monitor	387
	Configure Azure Alerts	395
	Configure Log Analytics	402
	Configure Network Watcher	410
	Module 11 Lab	416

Module 0 Start Here

Start Here

About this Course

Course Description

This course teaches IT Professionals how to manage their Azure subscriptions, secure identities, administer the infrastructure, configure virtual networking, connect Azure and on-premises sites, manage network traffic, implement storage solutions, create and scale virtual machines, implement web apps and containers, back up and share data, and monitor your solution.

Level: Intermediate

Audience

This course is for Azure Administrators. Azure Administrators manage the cloud services that span storage, networking, and compute cloud capabilities, with a deep understanding of each service across the full IT lifecycle. They take end-user requests for new cloud applications and make recommendations on services to use for optimal performance and scale, as well as provision, size, monitor and adjust as appropriate. This role requires communicating and coordinating with vendors. Azure Administrators use the Azure Portal and as they become more proficient they use PowerShell and the Command Line Interface.

Prerequisites

Successful Azure Administrators start this role with experience in virtualization, networking, identity, and storage.

- Understanding on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.
- Understanding network configurations, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- Understanding Active Directory concepts, including users, groups, and role-based access control.
- Understanding resilience and disaster recovery, including backup and restore operations.

You can gain the prerequisites and a better understanding of Azure by taking **AZ-104: Prerequisites for Azure Administrators¹**. This free online training will give you the experience you need to be successful in this course.

Expected learning

- Secure identities with Azure Active Directory and users and groups.
- Manage subscriptions, accounts, Azure policies, and Role-Based Access Control.
- Administer Azure using the Resource Manager, Azure portal, Cloud Shell, Azure PowerShell, CLI, and ARM templates.
- Configure virtual networks including planning, IP addressing, Azure DNS, Network Security Groups, and Azure Firewall.
- Configure intersite connectivity solutions like VNet Peering, virtual network gateways, and Site-to-Site VPN connections.
- Manage network traffic using network routing and service endpoints, Azure load balancer, and Azure Application Gateway.
- Implement, manage and secure Azure storage accounts, blob storage, and Azure files with File Sync.
- Plan, create, and scale virtual machines.
- Administer Azure App Service, Azure Container Instances, and Kubernetes.
- Backup files, folders, and virtual machines.
- Monitor the Azure infrastructure with Azure Monitor, Azure alerts, Log Analytics, and Network Watcher.

Syllabus

The course content includes a mix of content, demonstrations, hands-on labs, reference links, and knowledge check questions.

Module 01 - Administer Identity

In this module, you will learn how to secure identities with Azure Active Directory, and implement users and groups. This module includes:

- Configure Azure Active Directory
- Configure User and Group Accounts
- Lab 01 - Manage Azure Active Directory Identities

Module 02 – Administer Governance and Compliance

In this module, you will learn about managing your subscriptions and accounts, implementing Azure policies, and using Role-Based Access Control. This module includes:

- Configure Subscriptions and Accounts
- Configure Azure Policy
- Configure Role-Based Access Control (RBAC)
- Lab 02a - Manage Subscriptions and RBAC
- Lab 02b - Manage Governance via Azure Policy

¹ <https://docs.microsoft.com/learn/paths/az-104-administrator-prerequisites/>

Module 03 – Administer Azure Resources

In this module, you will learn about the tools an Azure Administrator uses to manage their infrastructure. This includes the Azure Portal, Cloud Shell, Azure PowerShell, CLI, and Resource Manager Templates. This module includes:

- Configure Resources with Tools
- Use Azure Resource Manager
- Configure Resources with ARM Templates
- Lab 03a - Manage Azure resources by Using the Azure Portal
- Lab 03b - Manage Azure resources by Using ARM Templates
- Lab 03c - Manage Azure resources by Using Azure PowerShell (optional)
- Lab 03d - Manage Azure resources by Using Azure CLI (optional)

Module 04 – Administer Virtual Networking

In this module, you will learn about basic virtual networking concepts like virtual networks and subnetting, IP addressing, Azure DNS, network security groups, and Azure Firewall. This module includes:

- Configure Virtual Networks
- Configure Network Security Groups
- Configure Azure Firewall
- Configure Azure DNS
- Lab 04 - Implement Virtual Networking

Module 05 – Administer Intersite Connectivity

In this module, you will learn about intersite connectivity features including VNet Peering, Virtual Network Gateways, and VPN Gateway Connections. This module includes:

- Configure VNet Peering
- Configure VPN Gateway Connections
- Configure ExpressRoute and Virtual WAN
- Lab 05 - Implement Intersite Connectivity

Module 06 – Administer Network Traffic Management

In this module, you will learn about network traffic strategies including network routing and service endpoints, Azure Load Balancer, and Azure Application Gateway. This module includes:

- Configure Network Routing and Endpoints
- Configure Azure Load Balancer
- Configure Azure Application Gateway
- Lab 06 - Implement Traffic Management

Module 07 – Administer Azure Storage

In this module, you will learn about basic storage features including storage accounts, blob storage, Azure files and File Sync, storage security, and storage tools. This module includes:

- Configure Storage Accounts
- Configure Blob Storage

- Configure Storage Security
- Configure Azure Files and File Sync
- Configure Storage with Tools
- Lab 07 - Manage Azure storage

Module 08 – Administer Azure Virtual Machines

In this module, you will learn about Azure virtual machines including creating, availability and extensions. This module includes:

- Configure Virtual Machines
- Configure Virtual Machine Availability
- Configure Virtual Machine Extensions
- Lab 08 - Manage Virtual Machines

Module 09 - Administer PaaS Compute Options

In this module, you will learn administer computing features like Azure App Service, Azure Container Instances, and Kubernetes. This module includes:

- Configure Azure App Service Plans
- Configure Azure App Services
- Configure Azure Container Instances
- Configure Azure Kubernetes Services
- Lab 09a - Implement Web Apps
- Lab 09b - Implement Azure Container Instances
- Lab 09c - Implement Azure Kubernetes Service

Module 10 – Administer Data Protection

In this module, you will learn about backing up files and folders, and virtual machine backups. This module includes:

- Configure File and Folder Backups
- Configure Virtual Machine Backups
- Lab 10 - Implement Data Protection

Module 11 – Administer Monitoring

In this module, you will learn about monitoring your Azure infrastructure including Azure Monitor, alerting, and log analytics. This module includes:

- Configure Azure Monitor
- Configure Azure Alerts
- Configure Log Analytics
- Configure Network Watcher
- Lab 11 - Implement Monitoring

AZ-104 Certification Exam

The AZ-104, **Microsoft Azure Administrator²**, certification exam is geared towards Azure Administrator candidates who manage cloud services that span compute, networking, storage, security, and other cloud capabilities within Microsoft Azure. These candidates should have a deep understanding of each service across the full IT lifecycle; including infrastructure services, applications, and environments. They will also be able to make recommendations on services to us for optimal performance and scale, including provision, size, monitor, and adjust Azure resources.

The exam includes five study areas. The percentages indicate the relative weight of each area on the exam. The higher the percentage, the more questions the exam will contain.

AZ-104 Study Areas	Weights
Manage Azure identities and governance	15-20%
Implement and manage storage	15-20%
Deploy and manage Azure compute resources	20-25%
Configure and manage virtual networking	25-30%
Monitor and backup Azure resources	10-15%

Additional Study Resources

There are a lot of additional resources to help you learn about Azure. We recommend you bookmark these pages.

- **Learn - AZ-104: Prerequisites for Azure administrators³**
- **Learn - AZ-104: Manage identities and governance in Azure⁴**
- **Learn - AZ-104: Implement and manage storage⁵**
- **Learn - AZ-104: Deploy and manage Azure compute resources⁶**
- **Learn - AZ-104: Configure and manage virtual networks for Azure administrators⁷**
- **Learn - AZ-104: Monitor and backup Azure resources⁸**
- **Azure Community Support⁹**
- **Azure Documentation¹⁰**
- **Microsoft Azure Blog¹¹**
- **Microsoft Learn Blog¹²**

² <https://docs.microsoft.com/learn/certifications/exams/az-104>

³ <https://docs.microsoft.com/learn/paths/az-104-administrator-prerequisites/>

⁴ <https://docs.microsoft.com/learn/paths/az-104-manage-identities-governance/>

⁵ <https://docs.microsoft.com/learn/paths/az-104-manage-storage/>

⁶ <https://docs.microsoft.com/learn/paths/az-104-manage-compute-resources/>

⁷ <https://docs.microsoft.com/learn/paths/az-104-manage-virtual-networks/>

⁸ <https://docs.microsoft.com/learn/paths/az-104-monitor-backup-resources/>

⁹ <https://azure.microsoft.com/support/community/>

¹⁰ <https://docs.microsoft.com/azure/>

¹¹ <https://azure.microsoft.com/blog/>

¹² <https://techcommunity.microsoft.com/t5/microsoft-learn-blog/bg-p/MicrosoftLearnBlog>

Obtaining and Redeeming Your Azure Pass

To launch and complete the Online labs for this course you will first need to create an Azure subscription:

1. To be assigned an Azure Pass, click on the "Obtain Azure Pass" button below.
2. This will open a new window in your browser that looks like this:

The following is your Azure Pass

If this is the first time you have received this pass then you will need to navigate to the following site to create an Azure Subscription using this pass.

<http://www.microsoftazurepass.com/>

Once you have created your subscription it will remain active until expiration. So if you have already created your subscription using the Azure Pass above and it is still active, you may now move directly to completing the lab steps in the Azure Portal. (<https://portal.azure.com/>)

Please do not use any other Azure Subscriptions that you may already have.

[Close](#)

3. Copy down your Azure Pass and follow the directions for redeeming it.
4. Once you have created your trial Azure Subscription, you will need to follow the directions in each of the Lab module in this course to launch the lab environment.

Note: You only need to click the "Obtain Azure Pass" button once. If you click the button again after already being assigned an Azure Pass, our platform will recognize this and will present you with the same Azure Pass number.**

Module 1 Administer Identity

Configure Azure Active Directory

Introduction

Scenario

Transitioning workloads to the cloud involves more than just moving servers, websites, and data. Companies need to think about how to secure those resources and identify authorized users. Your company plans to implement Azure Active Directory and features like Azure AD Join and Self-Service Password Reset.

You need to select an Azure Active Directory edition and implement the required features.

Skills measured

Managing Azure Active Directory features is a part of **Exam AZ-104: Microsoft Azure Administrator¹**.

Manage Azure identities and governance (15-20%)

Manage Azure AD objects

- Configure Azure AD Join.
- Configure Self-Service Password Reset.

Learning objectives

In this module, you will learn how to:

- Identify the features and uses of Azure Active Directory.
- Define the main Azure Active Directory components such as identity, account and tenant.
- Compare Azure Active Directory to Azure Directory Domain Services.

¹ <https://docs.microsoft.com/learn/certifications/exams/az-104>

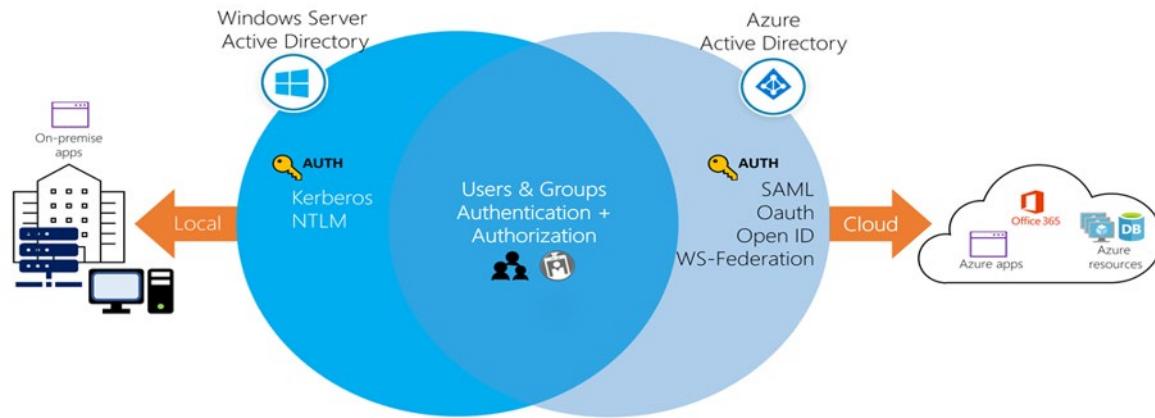
- Identify features of Azure Active Directory editions.
- Identify features and usage cases for Azure AD Join.
- Identify features and usage cases for Self-Service Password Reset.

Prerequisites

None

Describe Azure Active Directory Benefits and Features

Azure Active Directory (Azure AD) is Microsoft's multi-tenant cloud-based directory and identity management service.



Benefits and features

- **Single sign-on to any cloud or on-premises web app.** Azure Active Directory provides secure single sign-on to cloud and on-premises applications. SSO includes Microsoft 365 and thousands of SaaS applications such as Salesforce, Workday, DocuSign, ServiceNow, and Box.
- **Works with iOS, macOS, Android, and Windows devices.** Users can launch applications from a personalized web-based access panel, mobile app, Microsoft 365, or custom company portals using their existing work credentials. The experience is the same on iOS, macOS, Android, and Windows devices.
- **Protect on-premises web applications with secure remote access.** Access your on-premises web applications from everywhere and protect with multi-factor authentication, conditional access policies, and group-based access management. Users can access SaaS and on-premises web apps from the same portal.
- **Easily extend Active Directory to the cloud.** You can connect Active Directory and other on-premises directories to Azure Active Directory in just a few steps. This connection means a consistent set of users, groups, passwords, and devices across both environments.

- **Protect sensitive data and applications.** You can enhance application access security with unique identity protection capabilities. This includes a consolidated view into suspicious sign-in activities and potential vulnerabilities. You can also take advantage of advanced security reports, notifications, remediation recommendations, and risk-based policies.
- **Reduce costs and enhance security with self-service capabilities.** Delegate important tasks such as resetting passwords and the creation and management of groups to your employees. Providing self-service application access and password management through verification steps can reduce helpdesk calls and enhance security.

Note: If you are a Microsoft 365, Azure, or Dynamics CRM Online customer, you might not realize that you are already using Azure AD. Every Microsoft 365, Azure and Dynamics CRM tenant is already an Azure AD tenant. Whenever you want you can start using that tenant to manage access to thousands of other cloud applications Azure AD integrates with.

Describe Azure AD Concepts

It is important to understand these Azure AD concepts.

- **Identity.** An object that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authentication through secret keys or certificates.
- **Account.** An identity that has data associated with it. You can't have an account without an identity.
- **Azure AD Account.** An identity created through Azure AD or another Microsoft cloud service, such as Microsoft 365. Identities are stored in Azure AD and accessible to your organization's cloud service subscriptions. This account is also sometimes called a Work or school account.
- **Azure subscription.** Used to pay for Azure cloud services. You can have many subscriptions and they're linked to a credit card.
- **Azure tenant/directory.** A dedicated and trusted instance of Azure AD, a Tenant is automatically created when your organization signs up for a Microsoft cloud service subscription.
 - More instances of Azure AD can be created.
 - Azure AD is the underlying product providing the identity service.
 - The term Tenant means a single instance of Azure AD representing a single organization.
 - The terms Tenant and Directory are often used interchangeably.

Compare AD DS to Azure Active Directory

AD DS is the traditional deployment of Windows Server-based Active Directory on a physical or virtual server. Although AD DS is commonly considered to be primarily a directory service, it is only one component of the Windows Active Directory suite of technologies, which also includes Active Directory Certificate Services (AD CS), Active Directory Lightweight Directory Services (AD LDS), Active Directory Federation Services (AD FS), and Active Directory Rights Management Services (AD RMS). Although you can deploy and manage AD DS in Azure virtual machines it's recommended you use Azure AD instead, unless you are targeting IaaS workloads that depend on AD DS specifically.

Azure AD is different from AD DS

Although Azure AD has many similarities to AD DS, there are also many differences. It is important to realize that using Azure AD is different from deploying an Active Directory domain controller on an Azure

virtual machine and adding it to your on-premises domain. Here are some characteristics of Azure AD that make it different.

- **Identity solution.** Azure AD is primarily an identity solution, and it is designed for Internet-based applications by using HTTP and HTTPS communications.
- **REST API Querying.** Because Azure AD is HTTP/HTTPS based, it cannot be queried through LDAP. Instead, Azure AD uses the REST API over HTTP and HTTPS.
- **Communication Protocols.** Because Azure AD is HTTP/HTTPS based, it does not use Kerberos authentication. Instead, it uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization).
- **Federation Services.** Azure AD includes federation services, and many third-party services (such as Facebook).
- **Flat structure.** Azure AD users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs).

Note: Azure AD is a managed service. You only manage the users, groups, and policies. Deploying AD DS with virtual machines using Azure means that you manage the deployment, configuration, virtual machines, patching, and other backend tasks.

Select Azure Active Directory Editions

Azure Active Directory comes in four editions—**Free**, **Microsoft 365 Apps**, **Premium P1**, and **Premium P2**. The Free edition is included with an Azure subscription. The Premium editions are available through a Microsoft Enterprise Agreement, the Open Volume License Program, and the Cloud Solution Providers program. Azure and Microsoft 365 subscribers can also buy Azure Active Directory Premium P1 and P2 online.

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	500,000	Unlimited	Unlimited	Unlimited
Single Sign-On	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access Management	X	X	X	X
Business to Business Collaboration	X	X	X	X
Identity & Access Management for Microsoft 365 apps		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access Management			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

Azure Active Directory Free. Provides user and group management, on-premises directory synchronization, basic reports, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.

Azure Active Directory Microsoft 365 Apps. This edition is included with O365. In addition to the Free features, this edition provides Identity & Access Management for Microsoft 365 apps including branding, MFA, group access management, and self-service password reset for cloud users.

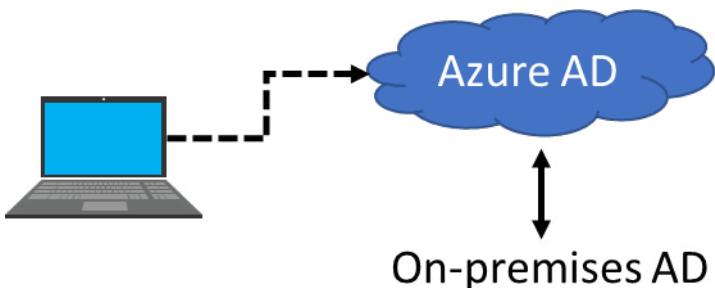
Azure Active Directory Premium P1. In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.

Azure Active Directory Premium P2. In addition to the Free and P1 features, P2 also offers Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data. Privileged Identity Management is included to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.

Note: The [Azure Active Directory Pricing²](#) page has detailed information on what is included in each of the editions. Based on the feature list which edition does your organization need?

Implement Azure AD Join

Azure Active Directory (Azure AD) enables single sign-on to devices, apps, and services from anywhere. IT administrators must ensure corporate assets are protected and that devices meet standards for security and compliance.



Azure AD Join is designed to provide access to organizational apps and resources and to simplify Windows deployments of work-owned devices. AD Join has these benefits.

- **Single-Sign-On (SSO)** to your Azure-managed SaaS apps and services. Your users won't have additional authentication prompts when accessing work resources. The SSO functionality is available even when users are not connected to the domain network.
- **Enterprise compliant roaming** of user settings across joined devices. Users don't need to connect to a Microsoft account (for example, Hotmail) to observe settings across devices.
- **Access to Microsoft Store for Business** using an Azure AD account. Your users can choose from an inventory of applications pre-selected by the organization.
- **Windows Hello** support for secure and convenient access to work resources.
- **Restriction of access** to apps from only devices that meet compliance policy.

² <https://azure.microsoft.com/pricing/details/active-directory>

- **Seamless access to on-premise resources** when the device has line of sight to the on-premises domain controller.

Connection options

To get a device under the control of Azure AD, you have two options:

- **Registering** a device to Azure AD enables you to manage a device's identity. Azure AD device registration provides the device with an identity that is used to authenticate the device when a user signs-in to Azure AD. You can use the identity to enable or disable a device.
- **Joining** a device is an extension to registering a device. Joining provides the benefits of registering and changes the local state of a device. Changing the local state enables your users to sign-in to a device using an organizational work or school account instead of a personal account.

Note: Registration combined with a mobile device management (MDM) solution such as Microsoft Intune, provides additional device attributes in Azure AD. You can create conditional access rules that enforce access from devices to meet your standards for security and compliance.

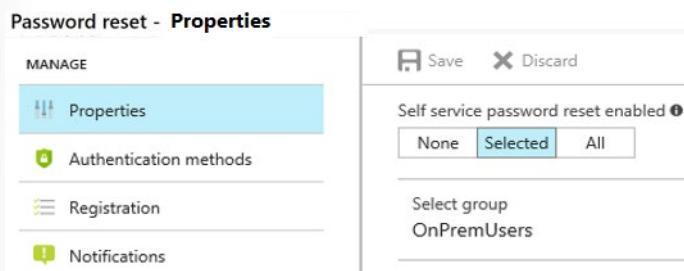
Note: Although AD Join is intended for organizations that do not have on-premises Windows Server Active Directory infrastructure it can be used for other scenarios like branch offices.

Implement Self-Service Password Reset

Many helpdesk calls are requests to reset passwords for users. Enabling **Self-service password reset** (SSPR) gives the users the ability to bypass the helpdesk and reset their own passwords.

To configure Self-Service Password Reset, you first determine who will be enabled to use self-service password reset. From your existing Azure AD tenant, on the Azure Portal under **Azure Active Directory** select **Password reset**.

In the Password reset properties there are three options: **None**, **Selected**, and **All**.



The **Selected** option is useful for creating specific groups who have self-service password reset enabled. You can create group for testing or proof of concept before deploying to a larger group. Once you are ready to deploy this functionality to all users with accounts in your AD Tenant, you can change the setting to **All**.

Authentication methods

After enabling password reset for user and groups, you pick the number of authentication methods required to reset a password and the number of authentication methods available to users.

At least one authentication method is required to reset a password. It is a good idea to have other methods available. You can choose from email notification, a text, or code sent to user's mobile or office phone, or a set of security questions.

Password reset - Authentication methods

mitaric (Default Directory) - Azure Active Directory

Save Discard

Number of methods required to reset ①

1 2

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

Number of questions required to register ①

3 4 5

Number of questions required to reset ①

3 4 5

Select security questions
5 security questions selected

You can require a security questions to be registered for the users in your AD tenant. You can also configure how many correctly answered security questions are required for a successful password reset. Security questions can be less secure than other methods because some people might know the answers to another user's questions.

Note: Azure Administrator accounts can always reset their passwords no matter what options are configured.

Knowledge check

Choose the best response for each question.

Multiple choice

Your users want to sign-in to devices, apps, and services from anywhere. They want to sign-in using an organizational work or school account instead of a personal account. You must ensure corporate assets are protected and that devices meet standards for security and compliance. Specifically, you need to be able to enable or disable a device. What should you do? Select one.

- Enable the device in Azure AD.
- Join the device to Azure AD.
- Register the device with Azure AD.

Multiple choice

A dedicated and trusted instance of Azure AD is referred to as:

- An Azure tenant
- An Azure identity
- An Azure account

Multiple choice

You are configuring Self-service Password Reset. Which of the following is not a validation method? Select one.

- An email notification.
- A text or code sent to a user's mobile or office phone.
- A paging service.
- A set of security questions

Summary and Resources

Summary

Azure Administrators must be familiar with Azure Active Directory and its features.

You should now be able to:

- Understand the features and uses of Azure Active Directory.
- Define the main Azure Active Directory components such as identity, account and tenant.
- Compare Azure Active Directory to Azure Directory Domain Services.
- Identify features of Azure Active Directory editions.
- Identify features and usage cases for Azure AD Join.
- Identify features and usage cases for Self-Service Password Reset.

Learn more

You can learn more by reviewing the following.

- **Azure Active Directory Documentation³**
- **Azure AD device identity documentation⁴**
- **Azure AD self-service password reset⁵**
- **Learn - Allow users to reset their password with Azure Active Directory self-service password reset⁶**

³ <https://docs.microsoft.com/azure/active-directory/>

⁴ <https://docs.microsoft.com/azure/active-directory/devices/>

⁵ <https://docs.microsoft.com/azure/active-directory/authentication/concept-sspr-howitworks>

⁶ <https://docs.microsoft.com/learn/modules/allow-users-reset-their-password/>

- Learn - Manage device identity with Azure AD join and Enterprise State Roaming⁷

⁷ <https://docs.microsoft.com/learn/modules/manage-device-identity-ad-join/>

Configure User and Group Accounts

Introduction

Scenario

Every user who needs access to Azure resources needs an Azure user account. A user account contains all the information needed to authenticate the user during the sign-on process. Group accounts lets you organize user accounts so administration is easier.

You need to create and manage user and group accounts.

Skills measured

Managing user and groups accounts is part of **Exam AZ-104: Microsoft Azure Administrator⁸**.

Manage Azure identities and governance (15-20%)

Manage Azure AD objects

- Create users and groups.
- Manage user and group properties.
- Manage device settings.
- Perform bulk user updates.
- Manage guest accounts.

Learning objectives

In this module, you will learn how to:

- Configure users accounts and user account properties.
- Create new user accounts.
- Import bulk user accounts with a template.
- Configure group accounts and assignment types.

Prerequisites

None

Create User Accounts

To view the Azure AD users, access the All users page.

⁸ <https://docs.microsoft.com/learn/certifications/exams/az-104>

Name	User principal name	User type	Directory synced
Retail Crisis Notifications	@microsoft.com	Member	Yes
Rumon Sinha	@microsoft.onmicrosoft.com	Guest	No
Momir Radojkovic	@microsoft.onmicrosoft.com	Guest	No
Mika Robertson	@microsoft.onmicrosoft.com	Member	No

Typically, Azure AD defines users in three ways:

- **Cloud identities.** These users exist only in Azure AD. Examples are administrator accounts and users that you manage yourself. Cloud identities can be in Azure Active Directory or an external Azure Active Directory, if the user is defined in another Azure AD instance. When these accounts are removed from the primary directory, they are deleted.
- **Directory-synchronized identities.** These users exist in an on-premises Active Directory. A synchronization activity that occurs via Azure AD Connect brings these users in to Azure. Their source is Windows Server AD.
- **Guest users.** These users exist outside Azure. Examples are accounts from other cloud providers and Microsoft accounts such as an Xbox LIVE account. Their source is Invited user. This type of account is useful when external vendors or contractors need access to your Azure resources. Once their help is no longer necessary, you can remove the account and all of their access.

Note: Have you thought about the type of users you will need?

Manage User Accounts

There are multiple ways to add cloud identities to Azure AD.

Azure Portal

You can add new users through the Azure Portal. In addition to Name and User name, there is profile information like Job Title and Department.

Things to consider when managing users:

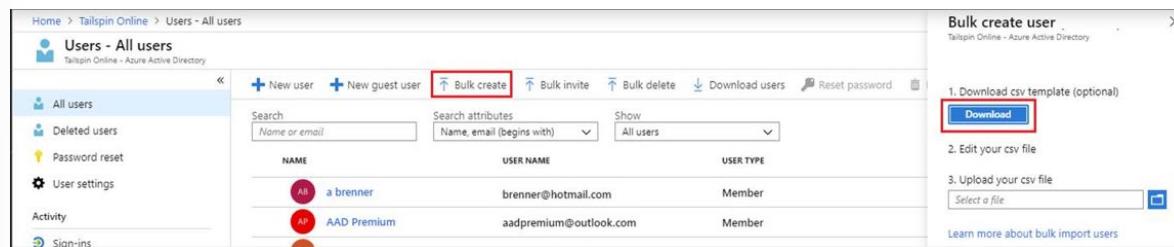
- Must be Global Administrator to manage users.
- User profile (picture, job, contact info) is optional.
- Deleted users can be restored for 30 days.

- Sign in and audit log information is available.

Note: Users can also be added to Azure AD through Microsoft 365 Admin Center, Microsoft Intune admin console, and the CLI. How do you plan to add users?

Create Bulk User Accounts

Azure Active Directory (Azure AD) supports bulk user create and delete operations and supports downloading lists of users. Just fill out the comma-separated values (CSV) template. You can download the template from the Azure AD portal. To create users in the Azure Portal, you must be signed in as a Global administrator or User administrator.



Things to consider when using the template

- **Naming conventions.** Establish or implement a naming convention for usernames, display names, and aliases. For example, a user name could consist of last name, period, first name: 'Smith.John@contoso.com'.
- **Passwords.** Implement a convention for the initial password of the newly created user. Figure out a way for the new users to receive their password in a secure way. Methods commonly used include generating a random password and emailing it to the new user or their manager.

Note: PowerShell is also available for bulk user uploads.

Create Group Accounts

Azure AD allows you to define two different types of groups.

- **Security groups.** Security groups are used to manage member and computer access to shared resources for a group of users. For example, you can create a security group for a specific security policy. By doing it this way, you can give a set of permissions to all the members at once, instead of having to add permissions to each member individually. This option requires an Azure AD administrator.
- **Microsoft 365 groups.** Microsoft 365 groups provide collaboration opportunities by giving members access to a shared mailbox, calendar, files, SharePoint site, and more. You can give people outside of your organization access to the group. Both users and admins can use Microsoft 365 groups.

Name	Group Type	Membership Type
<input type="checkbox"/> MA Managers	Security	Assigned
<input type="checkbox"/> VM Virtual Machine Administrators	Security	Assigned
<input type="checkbox"/> VN Virtual Network Administrators	Security	Assigned

Adding Members to Groups

There are different ways you can assign access rights:

- **Assigned.** Lets you add specific users to be members of this group and to have unique permissions.
- **Dynamic User.** Lets you use dynamic membership rules to automatically add and remove members. When a member's attributes change, Azure reviews the dynamic group rules for the directory. If the member meets the rule requirements, they're added. If the member no longer meets the rules requirements, they're removed.
- **Dynamic Device (Security groups only).** Lets you use dynamic group rules to automatically add and remove devices. If a device's attributes change, Azure reviews the dynamic group rules for the directory. If the device meets the rule requirements, they're added. If the device no longer meets the rules requirements, they're removed.

Note: Have you thought about which groups you need to create? Would you use directly assigned or dynamically assigned membership?

Create Administrative Units

It can be useful to restrict administrative scope by using administrative units in organizations that are made up of independent divisions of any kind.

Example

Consider the example of a large university that's made up of many autonomous schools (School of Business, School of Engineering, and so on). Each school has a team of IT admins who control access, manage users, and set policies for their school.

A central administrator could:

- Create a role with administrative permissions over only Azure AD users in the business school administrative unit.
- Create an administrative unit for the School of Business.
- Populate the administrative unit with only the business school students and staff.
- Add the business school IT team to the role, along with its scope.

Considerations

- You can manage administrative units by using the Azure portal, PowerShell cmdlets and scripts, or Microsoft Graph.
- In the portal, you can manage administrative units if you are a Global Administrator or a Privileged Role Administrator.
- Administrative units apply scope only to management permissions. They don't prevent members or administrators from using their default user permissions to browse other users, groups, or resources outside the administrative unit.

Demonstration - Users and Groups

In this demonstration, we will explore Azure Active Directory.

Note: Depending on your subscription not all areas of the Azure Active Directory blade will be available.

Review license and domain information

1. Access the Azure portal and navigate to the **Azure Active Directory** blade.
2. On the Overview blade, review the **Tenant information** including license and primary domain.

Explore user accounts

1. Select the **Users** blade.
2. Explain the choices for **New user** and **New guest user**.
3. Select **New user** and discuss the differences between **Create user** and **Invite user**.
4. Create a **New user** reviewing the **Identity**, **Groups and roles**, **Settings**, and **Job Info** parameters.
5. After the user is created, review **Reset password**, **Delete user**, and **Sign-ins**.

Explore group accounts

1. Return to the **Azure Active Directory** page and select the **Groups** blade.
2. Create a **New group** or select an existing group to review.
3. Review information about a group including **Membership type** and **Type**.

Optional - Explore PowerShell for group management

1. Create a new group called Developers.

```
New-AzADGroup -DisplayName Developers -MailNickname Developers
```

2. Retrieve the Developers group ObjectId.

```
Get-AzADGroup
```

3. Retrieve the user ObjectId for the member to add.

```
Get-AzADUser
```

4. Add the user to the group. Replace groupObjectId and userObjectId.

```
Add-AzADGroupMember -MemberUserPrincipalName ""myemail@domain.com"" -TargetGroupDisplayName ""MyGroupDisplayName""
```

5. Verify the members of the group. Replace groupObjectid.

```
Get-AzADGroupMember -GroupDisplayName "MyGroupDisplayName"
```

Knowledge check

Choose the best response for each question.

Multiple choice

You are assigning Azure AD roles. Which role will allow the user to manage all the groups in your Teams tenants and be able to assign other administrator roles? Select one.

- Password administrator
- Security administrator
- Global administrator

Multiple choice

You would like to add a user who has a Microsoft account to your subscription. Which type of user account is this? Select one.

- Cloud identity
- Directory-Synchronized identity
- Guest User

Multiple choice

If you delete a user account by mistake, can it be restored? Select one.

- When a user account is deleted, it's gone forever and can't be restored.
- The user account can be restored, but only when it's created within the last 30 days.
- The user account can be restored, but only when it's deleted within the last 30 days.

Multiple choice

Which of the following roles has full access to manage all resources but does not allow you to assign roles? Select one.

- Owner
- Contributor
- Reader

Summary and Resources

Summary

Azure AD helps you give access to your organization's resources by providing access rights to a single user or to an entire Azure AD group.

You should now be able to:

- Configure users accounts and user account properties.
- Create new user accounts.
- Import bulk user accounts with a template.
- Configure group accounts and assignment types.
- Manage multiple directories and identify usage cases for multiple directories.

Learn more

You can learn more by reviewing the following.

- **Azure Active Directory fundamentals documentation⁹**
- **Learn - Manage users and groups in Azure Active Directory¹⁰**
- **Learn - Create Azure users and groups in Azure Active Directory¹¹**

⁹ <https://docs.microsoft.com/azure/active-directory/fundamentals/>

¹⁰ <https://docs.microsoft.com/learn/modules/manage-users-and-groups-in-aad/>

¹¹ <https://docs.microsoft.com/learn/modules/create-users-and-groups-in-azure-active-directory/>

Module 01 Lab

Lab 01 - Manage Azure Active Directory Identities

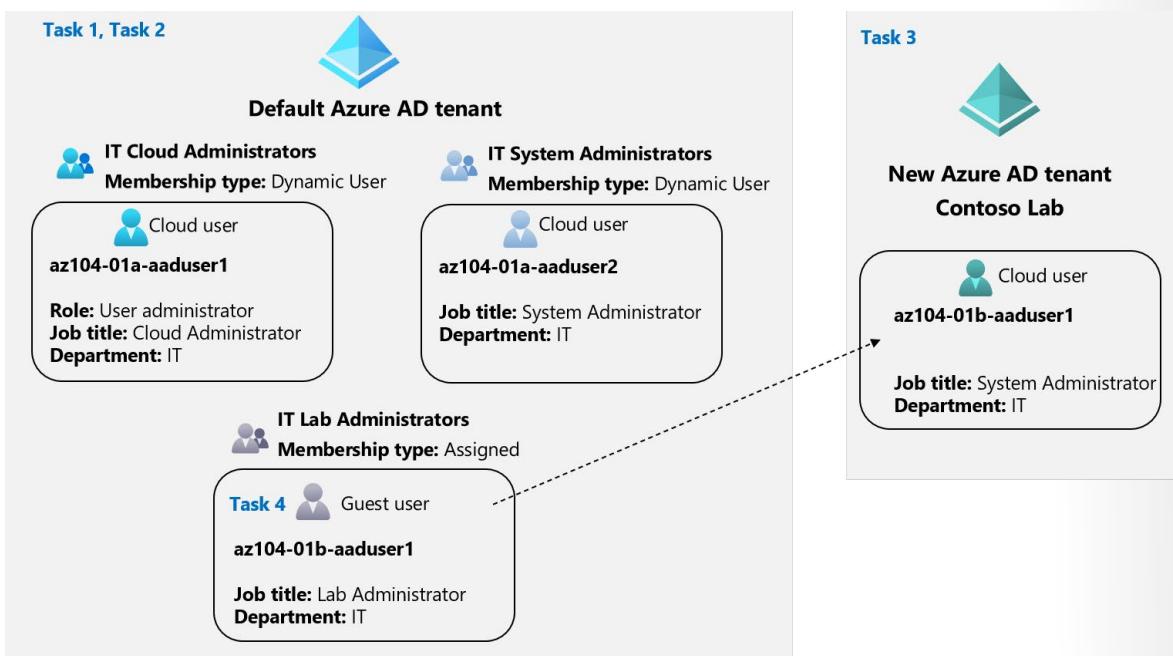
Lab scenario

In order to allow Contoso users to authenticate by using Azure AD, you have been tasked with provisioning users and group accounts. Membership of the groups should be updated automatically based on the user job titles. You also need to create a test Azure AD tenant with a test user account and grant that account limited permissions to resources in the Contoso Azure subscription.

Objectives

In this lab, you will:

- Task 1: Create and configure Azure AD users.
- Task 2: Create Azure AD groups with assigned and dynamic membership.
- Task 3: Create an Azure Active Directory (AD) tenant.
- Task 4: Manage Azure AD guest users.



Note: Consult with your instructor for how to access the lab instructions and lab environment (if provided)

Answers

Multiple choice

Your users want to sign-in to devices, apps, and services from anywhere. They want to sign-in using an organizational work or school account instead of a personal account. You must ensure corporate assets are protected and that devices meet standards for security and compliance. Specifically, you need to be able to enable or disable a device. What should you do? Select one.

- Enable the device in Azure AD.
- Join the device to Azure AD.
- Register the device with Azure AD.

Explanation

Join the device to Azure AD. Joining a device is an extension to registering a device. This means, it provides you with all the benefits of registering a device, like being able to enable or disable the device. In addition, it also changes the local state of a device. Changing the local state enables your users to sign-in to a device using an organizational work or school account instead of a personal account.

Multiple choice

A dedicated and trusted instance of Azure AD is referred to as:

- An Azure tenant
- An Azure identity
- An Azure account

Explanation

A dedicated and trusted instance of Azure AD is referred to as an Azure tenant or directory.

Multiple choice

You are configuring Self-service Password Reset. Which of the following is not a validation method?

Select one.

- An email notification.
- A text or code sent to a user's mobile or office phone.
- A paging service.
- A set of security questions

Explanation

A paging service. At least one authentication method is required to reset a password. Choices include email notification, a text or code sent to user's mobile or office phone, or a set of security questions.

Multiple choice

You are assigning Azure AD roles. Which role will allow the user to manage all the groups in your Teams tenants and be able to assign other administrator roles? Select one.

- Password administrator
- Security administrator
- Global administrator

Explanation

Global administrator. Only the global administrator can manage groups across tenants and assign other administrator roles.

Multiple choice

You would like to add a user who has a Microsoft account to your subscription. Which type of user account is this? Select one.

- Cloud identity
- Directory-Synchronized identity
- Guest User

Explanation

Guest user. Guest users are users added to Azure AD from a third party like Microsoft or Google.

Multiple choice

If you delete a user account by mistake, can it be restored? Select one.

- When a user account is deleted, it's gone forever and can't be restored.
- The user account can be restored, but only when it's created within the last 30 days.
- The user account can be restored, but only when it's deleted within the last 30 days.

Explanation

The user account can be restored, but only when it's deleted within the last 30 days. A user account can be restored when it's deleted within the last 30 days.

Multiple choice

Which of the following roles has full access to manage all resources but does not allow you to assign roles? Select one.

- Owner
- Contributor
- Reader

Explanation

Contributor. Grants full access to manage all resources, but does not allow you to assign roles.

Module 2 Administer Governance and Compliance

Configure Subscriptions

Introduction

Scenario

Your company is moving to Azure. As a first step, they are need to obtain an Azure subscription.

You are responsible for obtaining an Azure subscription for your company. You are also responsible for effective management of costs.

Skills measured

Managing Azure subscriptions is part of **Exam AZ-104: Microsoft Azure Administrator¹**.

Manage Azure identities and governance (15-20%)

Manage subscriptions and governance

- Apply tags.
- Manage subscriptions.
- Configure Cost Management.

Learning objectives

In this module, you will learn how to:

- Determine the correct region to locate Azure services.
- Identify features and usage cases for Azure subscriptions.

¹ <https://docs.microsoft.com/learn/certifications/exams/az-104>

- Identify how to obtain an Azure subscription.
 - Understand billing and features for different Azure subscriptions.
 - Use the Cost Management product for cost analysis.
 - Determine when to use resource tagging.
 - Identify ways to reduce costs.

Prerequisites

None

Identify Regions

Microsoft Azure is made up of datacenters located around the globe. These datacenters are organized and made available to end users by region. A **region**² is a geographical area on the planet containing at least one, but potentially multiple datacenters. The datacenters are in close proximity and networked together with a low-latency network.

A few examples of regions are *West US*, *Canada Central*, *West Europe*, *Australia East*, and *Japan West*. Azure is generally available in 60+ regions and available in 140 countries.



Things to know about regions

- Azure has more global regions than any other cloud provider.
 - Regions provide customers the flexibility and scale needed to bring applications closer to their users.
 - Regions preserve data residency and offer comprehensive compliance and resiliency options for customers.
 - For most Azure services, when you deploy a resource in Azure, you choose the region where you want your resource to be deployed.
 - Some services or virtual machine features are only available in certain regions, such as specific virtual machine sizes or storage types.

2 <https://azure.microsoft.com/global-infrastructure/regions>

- Some global Azure services that do not require you to select a region. These services include Azure Active Directory, Microsoft Azure Traffic Manager, and Azure DNS.
- Each Azure region is paired with another region within the same geography, together making a regional pair. The exception is Brazil South, which is paired with a region outside its geography.

Note: View the latest [Azure regions map](#).³

Things to know about regional pairs

- **Physical isolation.** Azure prefers at least 300 miles of separation between datacenters in a regional pair, although this isn't practical or possible in all geographies. Physical datacenter separation reduces the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once.
- **Platform-provided replication.** Some services such as Geo-Redundant Storage provide automatic replication to the paired region.
- **Region recovery order.** During a broad outage, recovery of one region is prioritized out of every pair. Applications that are deployed across paired regions are guaranteed to have one of the regions recovered with priority.
- **Sequential updates.** Planned Azure system updates are rolled out to paired regions sequentially (not at the same time). Rolling updates minimizes downtime, reduces bugs, and logical failures in the rare event of a bad update.
- **Data residency.** A region resides within the same geography as its pair (except for Brazil South) to meet data residency requirements for tax and law enforcement jurisdiction purposes.

Note: View the complete list of [region pairs](#).⁴

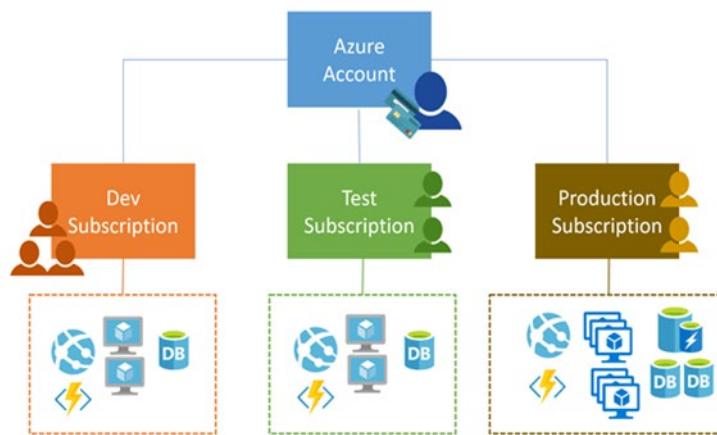
Implement Azure Subscriptions

An Azure subscription is a logical unit of Azure services that is linked to an Azure account. Billing for Azure services is done on a per-subscription basis. If your account is the only account associated with a subscription, then you are responsible for billing.

Subscriptions help you organize access to cloud service resources. They also help you control how resource usage is reported, billed, and paid for. Each subscription can have a different billing and payment setup, so you can have different subscriptions and different plans by department, project, regional office, and so on. Every cloud service belongs to a subscription, and the subscription ID may be required for programmatic operations.

³ <https://azure.microsoft.com/global-infrastructure/regions/>

⁴ <https://docs.microsoft.com/azure/best-practices-availability-paired-regions#what-are-paired-regions>



Azure Accounts

Subscriptions have accounts. An Azure account is simply an identity in Azure Active Directory (Azure AD) or in a directory that is trusted by Azure AD, such as a work or school organization. If you don't belong to one of these organizations, you can sign up for an Azure account by using your Microsoft Account, which is also trusted by Azure AD.

Getting access to resources

Every Azure subscription is associated with an Azure Active Directory. Users and services that access resources of the subscription first need to authenticate with Azure Active Directory.

Note: Do you know how many subscriptions your organization has? Do you know how resources are organized into resource groups?

Obtain a Subscription

There are several ways to get an Azure subscription: Enterprise agreements, Microsoft resellers, Microsoft partners, and a personal free account.



Enterprise



Resellers



Partners



Personal

Enterprise agreements

Any **Enterprise Agreement**⁵ customer can add Azure to their agreement by making an upfront monetary commitment to Azure. That commitment is consumed throughout the year by using any combination of the wide variety of cloud services Azure offers. Enterprise agreements have a 99.95% monthly SLA.

Reseller

Buy Azure through the **Open Licensing program**⁶, which provides a simple, flexible way to purchase cloud services from your Microsoft reseller. If you already purchased an Azure in Open license key, **activate a new subscription or add more credits now**⁷.

Partners

Find a **Microsoft partner**⁸ who can design and implement your Azure cloud solution. These partners have the business and technology expertise to recommend solutions that meet the unique needs of your business.

Personal free account

With a **free trial account**⁹, you can get started using Azure right away and you won't be charged until you choose to upgrade.

Note: Which subscription model are you most interested in?

Identify Subscription Usage

Azure offers free and paid subscription options to suit different needs and requirements. The most commonly used subscriptions are:

- Free
- Pay-As-You-Go
- Enterprise Agreement
- Student

Azure free subscription

An Azure free subscription includes a \$200 credit to spend on any service for the first 30 days, free access to the most popular Azure products for 12 months, and access to more than 25 products that are always free. An Azure free subscription is an excellent way for new users to get started. To set up a free subscription, you need a phone number, a credit card, and a Microsoft account.

Note: Credit card information is used for identity verification only. You won't be charged for any services until you upgrade.

⁵ <https://azure.microsoft.com/pricing/enterprise-agreement/>

⁶ <https://www.microsoft.com/licensing/licensing-programs/open-license.aspx>

⁷ <https://azure.microsoft.com/offers/ms-azr-0111p/>

⁸ <https://azure.microsoft.com/partners/directory/>

⁹ <https://azure.microsoft.com/free/>

Azure Pay-As-You-Go subscription

A Pay-As-You-Go (PAYG) subscription charges you monthly for the services you used in that billing period. This subscription type is appropriate for a wide range of users, from individuals to small businesses, and many large organizations as well.

Azure Enterprise Agreement

An Enterprise Agreement provides flexibility to buy cloud services and software licenses under one agreement, with discounts for new licenses and Software Assurance. It's targeted at enterprise-scale organizations.

Azure for Students subscription

An Azure for Students subscription includes \$100 in Azure credits to be used within the first 12 months plus select free services without requiring a credit card at sign-up. You must verify your student status through your organizational email address.

Implement Cost Management

With Azure products and services, you only pay for what you use. As you create and use Azure resources, you are charged for the resources. You use Azure Cost Management and Billing features to conduct billing administrative tasks and manage billing access to costs. You also its features to monitor and control Azure spending and to optimize Azure resource use.



Cost Management shows organizational cost and usage patterns with advanced analytics. Reports in Cost Management show the usage-based costs consumed by Azure services and third-party Marketplace offerings. Costs are based on negotiated prices and factor in reservation and Azure Hybrid Benefit discounts. Collectively, the reports show your internal and external costs for usage and Azure Market-

place charges. Other charges, such as reservation purchases, support, and taxes are not yet shown in reports. The reports help you understand your spending and resource use and can help find spending anomalies. Predictive analytics are also available. Cost Management uses Azure management groups, budgets, and recommendations to show clearly how your expenses are organized and how you might reduce costs.

You can use the Azure portal or various APIs for export automation to integrate cost data with external systems and processes. Automated billing data export and scheduled reports are also available.

Plan and control expenses

The ways that Cost Management help you plan for and control your costs include: Cost analysis, budgets, recommendations, and exporting cost management data.

- **Cost analysis.** You use cost analysis to explore and analyze your organizational costs. You can view aggregated costs by organization to understand where costs are accrued and to identify spending trends. And you can see accumulated costs over time to estimate monthly, quarterly, or even yearly cost trends against a budget.
- **Budgets.** Budgets help you plan for and meet financial accountability in your organization. They help prevent cost thresholds or limits from being surpassed. Budgets can also help you inform others about their spending to proactively manage costs. And with them, you can see how spending progresses over time.
- **Recommendations.** Recommendations show how you can optimize and improve efficiency by identifying idle and underutilized resources. Or, they can show less expensive resource options. When you act on the recommendations, you change the way you use your resources to save money. To act, you first view cost optimization recommendations to view potential usage inefficiencies. Next, you act on a recommendation to modify your Azure resource use to a more cost-effective option. Then you verify the action to make sure that the change you make is successful.
- **Exporting cost management data.** If you use external systems to access or review cost management data, you can easily export the data from Azure. And you can set a daily scheduled export in CSV format and store the data files in Azure storage. Then, you can access the data from your external system.

Apply Resource Tagging

You can apply tags to your Azure resources to logically organize them by categories. Each tag consists of a name and a value. For example, you can apply the name *Environment* and the value *Production* or *Development* to your resources. After creating your tags, you associate them with the appropriate resources.

With tags in place, you can retrieve all the resources in your subscription with that tag name and value. This means, you can retrieve related resources from different resource groups.

The screenshot shows the 'RG-Backup | Tags' page in the Azure portal. On the left, there's a sidebar with links: Home, Overview, Activity log, Access control (IAM), Tags (which is selected and highlighted in grey), and Events. The main area has a search bar at the top. Below it, there are buttons for Save, Delete all, and Revert changes. A descriptive text block explains what tags are: "Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case-insensitive and tag values are case-sensitive." It includes a link to "Learn more about tags". Below this, there's a table header with columns for Name and Value, and a text input field where a tag can be added.

Perhaps one of the best uses of tags is to group billing data. When you download the usage CSV for services, the tags appear in the Tags column. You could then group virtual machines by cost center and production environment.

Considerations

There are a few things to remember about tagging:

- Each resource or resource group can have a maximum of 50 tag name/value pairs.
- Tags applied to the resource group are not inherited by the resources in that resource group.

Note: When you need to create a lot of resource tags you will want to do that programmatically. You can use PowerShell or the CLI.

Apply Cost Savings

Reservations help you save money by paying ahead. You can pay for one-year or three-years of virtual machine, SQL Database compute capacity, Azure Cosmos DB throughput, or other Azure resources.

Pre-paying allows you to get a discount on the resources you use. Reservations can significantly reduce your virtual machine, SQL database compute, Azure Cosmos DB, or other resource costs up to 72% on pay-as-you-go prices. Reservations provide a billing discount and don't affect the runtime state of your resources.

Azure Hybrid Benefits is a pricing benefit for customers who have licenses with Software Assurance. Azure Hybrid Benefits helps maximize the value of existing on-premises Windows Server or SQL Server license investments when migrating to Azure. There's an Azure Hybrid Benefit Savings Calculator to help you determine your savings.

Azure Credits is monthly credit benefit that allows you to experiment with, develop, and test new solutions on Azure. For example, as a Visual Studio subscriber, you can use Microsoft Azure at no extra charge. With your monthly Azure credit, Azure is your personal sandbox for dev/test.

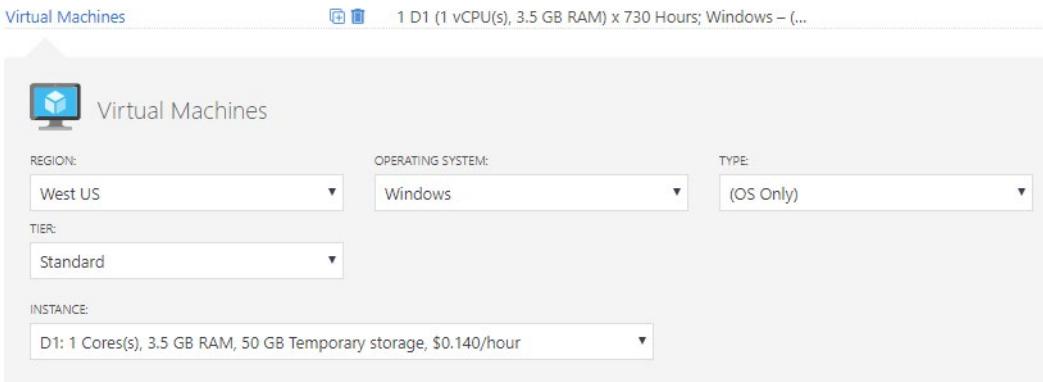
Azure regions pricing can vary from one region to another, even in the US. Double check the pricing in various regions to see if you can save a little.

Budgets help you plan for and drive organizational accountability. With budgets, you can account for the Azure services you consume or subscribe to during a specific period. They help you inform others about their spending to proactively manage costs, and to monitor how spending progresses over time. When the budget thresholds you've created are exceeded, only notifications are triggered. None of your resources are affected and your consumption isn't stopped. You can use budgets to compare and track spending as you analyze costs.

Pricing Calculator:

The **Pricing Calculator**¹⁰ provides estimates in all areas of Azure including compute, networking, storage, web, and databases.

Your Estimate



The screenshot shows the Azure Pricing Calculator interface. At the top, it says "Virtual Machines" and "1 D1 (1 vCPU(s), 3.5 GB RAM) x 730 Hours; Windows – (...". Below this is a search bar with a magnifying glass icon. The main area is titled "Virtual Machines" and contains the following fields:

- REGION:** West US
- OPERATING SYSTEM:** Windows
- TYPE:** (OS Only)
- TIER:** Standard
- INSTANCE:** D1: 1 Cores(s), 3.5 GB RAM, 50 GB Temporary storage, \$0.140/hour

Knowledge check

Choose the best response for each question.

Multiple choice

Your company financial comptroller wants to be notified whenever the company is half-way to spending the money allocated for cloud services. What should you do? Select one.

- Create an Azure reservation.
- Create a budget and a spending threshold.
- Create a management group.
- Enter workloads in the Total Cost of Ownership calculator.

Multiple choice

What tool can you use to gain greater visibility into your spending patterns? Select one.

- Cost Insights
- Cost Analysis
- Your invoice

¹⁰ <https://azure.microsoft.com/pricing/calculator/>

Multiple choice

Your company is concerned about cost and provisioning too many virtual machines at once. What's the best way to control resource provisioning? Select one.

- Change your subscription to pay as you go.
- Apply spending limits to the development team's Azure subscription.
- Verbally give the managers a budget and hold them accountable for overages.

Multiple choice

The leadership team wants information on resource costs by departments. What's the best way to categorize costs by department? Select one.

- Apply a tag to each resource that identifies the appropriate billing department.
- Split the cost evenly between departments.
- Keep a spreadsheet that lists each team's resources.

Multiple choice

An Azure subscription ... Select one.

- is a logical container used to provision resources in Azure
- is associated with a single department or organization
- represents a single domain

Summary and Resources

Summary

Obtaining and managing Azure subscriptions is a common Administrator task. Effectively identifying and managing costs is also important.

You should now be able to:

- Determine the correct region to locate Azure services.
- Identify features and usage cases for Azure subscriptions.
- Identify how to obtain an Azure subscription.
- Understand billing and features for different Azure subscriptions.
- Use the Cost Management product for cost analysis.
- Determine when to use resource tagging.
- Identify ways to reduce costs.

Learn more

You can learn more by reviewing the following.

- **What is Azure Cost Management + Billing?**¹¹
- **Create an additional Azure subscription**¹²
- **Learn - Analyze costs and create budgets with Azure Cost Management**¹³
- **Learn - Predict costs and optimize spending for Azure**¹⁴

11 <https://docs.microsoft.com/azure/cost-management-billing/cost-management-billing-overview>

12 <https://docs.microsoft.com/azure/cost-management-billing/manage/create-subscription>

13 <https://docs.microsoft.com/learn/modules/analyze-costs-create-budgets-azure-cost-management/>

14 <https://docs.microsoft.com/learn/modules/predict-costs-and-optimize-spending/>

Configure Azure Policy

Introduction

Scenario

Your company is subject to many regulations and compliance rules. They want to ensure each department implements and deploys resources correctly.

You decide to use Azure policy to implement compliance measures.

Skills measured

Azure policies is part of **Exam AZ-104: Microsoft Azure Administrator¹⁵**.

Manage Azure identities and governance (15–20%)

Manage subscriptions and governance

- Configure Azure policies.
- Configure management groups.

Learning objectives

In this module, you will learn how to:

- Create management groups to target policies and spend budgets.
- Implement Azure policy with policy and initiative definitions.
- Scope Azure policies and determine compliance.

Prerequisites

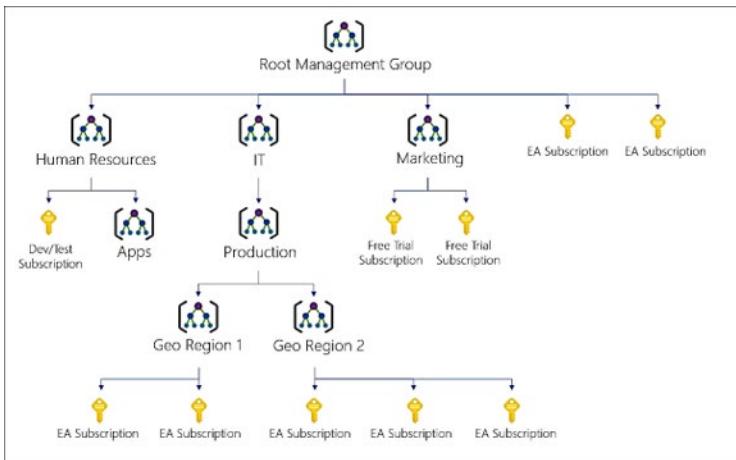
None

Create Management Groups

If your organization has several subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called *management groups* and apply your governance conditions to the management groups. Management group enable:

- Organizational alignment for your Azure subscriptions through custom hierarchies and grouping.
- Targeting of policies and spend budgets across subscriptions and inheritance down the hierarchies.
- Compliance and cost reporting by organization (business/teams).

¹⁵ <https://docs.microsoft.com/learn/certifications/exams/az-104>



All subscriptions within a management group automatically inherit the conditions applied to the management group. For example, you can apply policies to a management group that limits the regions available for virtual machine (VM) creation. This policy would be applied to all management groups, subscriptions, and resources under that management group by only allowing VMs to be created in that region.

Adding management groups

You can create the management group by using the portal, PowerShell, or Azure CLI. Currently, you can't use Resource Manager templates to create management groups.

NAME	ID	TYPE	MY ROLE
Azure Policy	<MG ID>	Management Group	Owner
Contoso IT	<MG ID>	Management Group	Owner
Contoso Marketing	<MG ID>	Management Group	Owner

- The **Management Group ID** is the directory unique identifier that is used to submit commands on this management group. This identifier is not editable after creation as it is used throughout the Azure system to identify this group.
- The **Display Name** field is the name that is displayed within the Azure portal. A separate display name is an optional field when creating the management group and can be changed at any time.

Note: Do you think you will use Management Groups? If so, how do you plan to implement them?

Implement Azure Policies

Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules over your resources, so those resources stay compliant with your corporate standards and service level agreements. Azure Policy runs evaluations and scans for resources that are not compliant.

The main advantages of Azure policy are in the areas of enforcement and compliance, scaling, and remediation.

- **Enforcement and compliance.** Turn on built-in policies or build custom ones for all resource types. Real-time policy evaluation and enforcement. Periodic and on-demand compliance evaluation.
- **Apply policies at scale.** Apply policies to a Management Group with control across your entire organization. Apply multiple policies and aggregate policy states with policy initiative. Define an exclusion scope.
- **Remediation.** Real-time remediation, and remediation on existing resources.

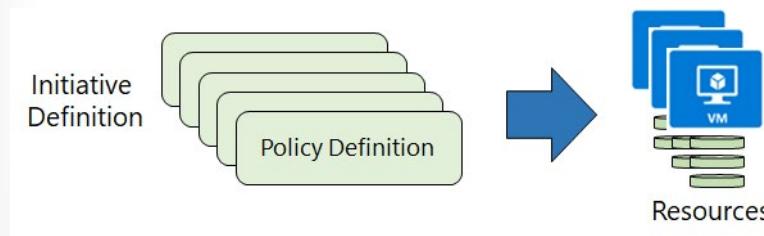
Azure Policy will be important to you if your team runs an environment where you need to govern:

- Multiple engineering teams (deploying to and operating in the environment)
- Multiple subscriptions
- Need to standardize/enforce how cloud resources are configured
- Manage regulatory compliance, cost control, security, or design consistency

Use Cases

- Specify the resource types that your organization can deploy.
- Specify a set of virtual machine SKUs that your organization can deploy.
- Restrict the locations your organization can specify when deploying resources.
- Enforce a required tag and its value.
- Audit if Azure Backup service is enabled for all Virtual machines.

Create Azure Policies



To implement Azure Policies, you can follow these steps.

1. **Browse Policy Definitions.** A Policy Definition expresses what to evaluate and what actions to take. Every policy definition has conditions under which it is enforced. And, it has an accompanying effect that takes place if the conditions are met. For example, you could prevent VMs from being deployed if they are exposed to a public IP address.
2. **Create Initiative Definitions.** An initiative definition is a set of Policy Definitions to help track your compliance state for a larger goal. For example, ensuring a branch office is compliant.
3. **Scope the Initiative Definition.** You can limit the scope of the Initiative Definition to Management Groups, Subscriptions, or Resource Groups.
4. **View Policy Evaluation results.** Once an Initiative Definition is assigned, you can evaluate the state of compliance for all your resources. Individual resources, resource groups, and subscriptions within a

scope can be exempted from having policy rules affect it. Exclusions are handled individually for each assignment.

Note: Even if you have only a few Policy Definitions, we recommend creating an Initiative Definition.

Create Policy Definitions

There are many Built-in Policy Definitions for you to choose from. Sorting by Category will help you locate what you need. For example,

- The Allowed Virtual Machine SKUs enables you to specify a set of virtual machine SKUs that your organization can deploy.
- The Allowed Locations policy enables you to restrict the locations that your organization can specify when deploying resources. The Allowed Locations policy can be used to enforce your geo-compliance requirements.

Name	Type	Definition type	Category
Not allowed resource types	Built-in	Policy	General
Allowed storage account SKUs	Built-in	Policy	Storage
Allowed resource types	Built-in	Policy	General
Allowed virtual machine SKUs	Built-in	Policy	Compute
Allowed locations	Built-in	Policy	General
Allowed locations for resource groups	Built-in	Policy	General

when there isn't an applicable policy you can add a new Policy Definition. You can import a policy definitions from [GitHub](#)¹⁶. New Policy Definitions are added almost every day.

Policy definition
New Policy definition

BASICS

Definition location *

Name * ⓘ

Description

Category ⓘ
 Create new Use existing

POLICY RULE

¹⁶ <https://github.com/Azure/azure-policy/tree/master/samples>

Note: Policy Definitions have a specific JSON format.

Create Initiative Definitions

Once you have determined which Policy Definitions you need, you create an Initiative Definition. This definition will include one or more policies. There is a pick list on the right side of the New Initiative definition page (not shown) to make your selection.

Initiative definition
New Initiative definition

BASICS

Definition location *

Visual Studio Enterprise

Name *

East Region

Description

East Region Initiative Definition

Category

Create new Use existing

General

namingPolicyDefinition	Policy to specify allowed naming convention	Custom	Delete
regionPolicyDefinition	Policy to allow resource creation only in certain regions	Custom	Delete

Note: How do you plan to organize your policy definitions?

Scope the Initiative Definition

Once our Initiative Definition is created, you can assign the definition to establish its scope. A scope determines what resources or grouping of resources the policy assignment gets enforced on.

Policy - Assignments

Search (Ctrl+ /)

Assign initiative Assign policy Refresh

Overview Getting started Join Preview Compliance Remediation

Authoring Assignments Definitions

Scope: Visual Studio Enterprise

Definition type: All definition types

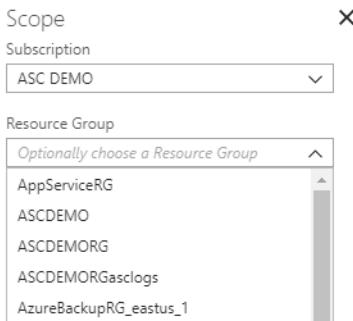
Total Assignments: 2

Initiative Assignments: 2

Policy Assignments: 0

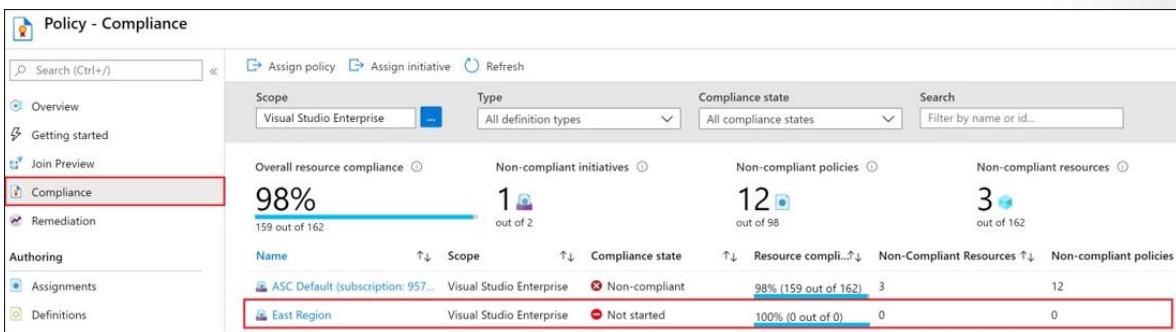
name	Scope	Type	Policies	Category
East Region	Visual Studio Enterprise	Initiative	2	General
ASC Default (subscription)	Visual Studio Enterprise	Initiative	96	Security Center

You can select the Subscription, and then optionally a Resource Group.



Determine Compliance

Once your policy is in place, you can use the Compliance blade to review non-compliant initiatives, non-compliant policies, and non-compliant resources.



Policy conditions are evaluated against your existing resources. When the condition is met, those resources are marked as non-compliant. Although the portal does not show the evaluation logic, the compliance state results are shown. The compliance state result is either compliant or non-compliant.

Note: Policy evaluation occurs about once an hour.

Demonstration - Azure Policy

In this demonstration, we will work with Azure policies.

Assign a policy

1. Access the Azure portal.
2. Search for and select **Policy**.
3. Select **Assignments** on the left side of the Azure Policy page.
4. Select **Assign Policy** from the top of the Policy - Assignments page.
5. Notice the **Scope** which determines what resources or grouping of resources the policy assignment gets enforced on.
6. Select the **Policy definition ellipsis** to open the list of available definitions. Take some time to review the built-in policy definitions.
7. Search for and select **Allowed locations**. This policy enables you to restrict the locations your organization can specify when deploying resources.
8. Move the **Parameters** tab and using the drop-down select one or more allowed locations.

9. Click **Review + create** and then **Create** to create the policy.

Create and assign an initiative definition

1. Return to the Azure Policy page and select **Definitions** under Authoring.
2. Select **Initiative Definition** at the top of the page.
3. Provide a **Name** and **Description**.
4. **Create new** Category.
5. From the right panel **Add** the **Allowed locations** policy.
6. Add one additional policy of your choosing.
7. **Save** your changes and then **Assign** your initiative definition to your subscription.

Check for compliance

1. Return to the Azure Policy service page.
2. Select **Compliance**.
3. Review the status of your policy and your definition.

Check for remediation tasks

1. Return to the Azure Policy service page.
2. Select **Remediation**.
3. Review any remediation tasks that are listed.

Remove your policy and initiative

1. Return to the Azure Policy service page.
2. Select **Assignments**.
3. Select your **Allowed locations** policy.
4. Click **Delete assignment**.
5. Return to the Azure Policy service page.
6. Select **Initiatives**.
7. Select your new initiative.
8. Click **Delete initiative**.

Knowledge check

Choose the best response for each question.

Multiple choice

Your organization has several Azure policies that they would like to create and enforce for a new branch office. What should you do? Select one.

- Create a policy initiative
- Create a management group
- Create a new subscriptions

Multiple choice

You would like to categorize resources and billing for different departments like IT and HR. The billing needs to be consolidated across multiple resource groups and you need to ensure everyone complies with the solution. You have created tags for each department, like department:HR. What should you do next?

- Create a billing group for each department
- Create an Azure policy
- Create a subscription account rule

Multiple choice

Your company wants to ensure that only cost-effective virtual machine SKU sizes are deployed. What should you do? Select one.

- Periodically inspect the deployment to see which SKU sizes are used
- Create an Azure RBAC role that defines the allowed virtual machine SKU sizes
- Create a policy in Azure Policy that specifies the allowed SKU sizes

Multiple choice

Which of the following can be used to manage governance across multiple Azure subscriptions?

- Azure initiatives
- Resource groups
- Management groups

Summary and Resources

Summary

Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. Azure Policy helps you define and implement your governance strategy.

You should now be able to:

- Create management groups to target policies and spend budgets.
- Implement Azure policy with policy and initiative definitions.
- Scope Azure policies and determine compliance.

Learn more

You can learn more by reviewing the following.

- **Azure Policy Documentation¹⁷**
- **Learn - Apply and monitor infrastructure standards with Azure Policy¹⁸**
- **Learn - Build a cloud governance strategy on Azure¹⁹**

¹⁷ <https://docs.microsoft.com/azure/azure-policy/>

¹⁸ <https://docs.microsoft.com/learn/modules/intro-to-governance/>

¹⁹ <https://docs.microsoft.com/learn/modules/analyze-costs-create-budgets-azure-cost-management/>

Configure Role-Based Access Control

Introduction

Scenario

Securing your Azure resources, such as virtual machines, websites, networks, and storage, is a critical function for any organization using the cloud. Your company wants to ensure that your data and assets are protected, but still grant your employees and partners the access they need to perform their jobs.

You decide to use role-based access control. You need to ensure assets are protected, but users can still access the resources they need.

Skills measured

Role-based access control is part of **Exam AZ-104: Microsoft Azure Administrator²⁰**.

Manage Azure identities and governance (15-20%)

Manage role-based access control (RBAC)

- Create a custom role.
- Provide access to Azure resources by assigning roles at different scopes.
- Interpret access assignments.

Learning objectives

In this module, you will learn how to:

- Identify the features and usage cases for role-based access control.
- List and create role definitions.
- Create role assignments.
- Identify the differences between Azure role-based access control and Azure Active Directory roles.
- Manage access to subscriptions using role-based access control.
- Review the built-in Azure role-based access control roles.

Prerequisites

None

Implement Role-Based Access Control

Access management for cloud resources is a critical function for any organization that is using the cloud. Role-based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of resources in Azure.

²⁰ <https://docs.microsoft.com/learn/certifications/exams/az-104>

What can I do with Azure RBAC?

Here are some examples of what you can do with Azure RBAC:

- Allow an application to access all resources in a resource group
- Allow one user to manage virtual machines in a subscription and another user to manage virtual networks
- Allow a DBA group to manage SQL databases in a subscription
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets

Concepts

- **Security principal.** Object that represents something that is requesting access to resources. Examples: user, group, service principal, managed identity
- **Role definition.** Collection of permissions that lists the operations that can be performed. Examples: Reader, Contributor, Owner, User Access Administrator
- **Scope.** Boundary for the level of access that is requested. Examples: management group, subscription, resource group, resource
- **Assignment.** Attaching a role definition to a security principal at a particular scope. Users can grant access described in a role definition by creating an assignment. Deny assignments are currently read-only and can only be set by Azure.

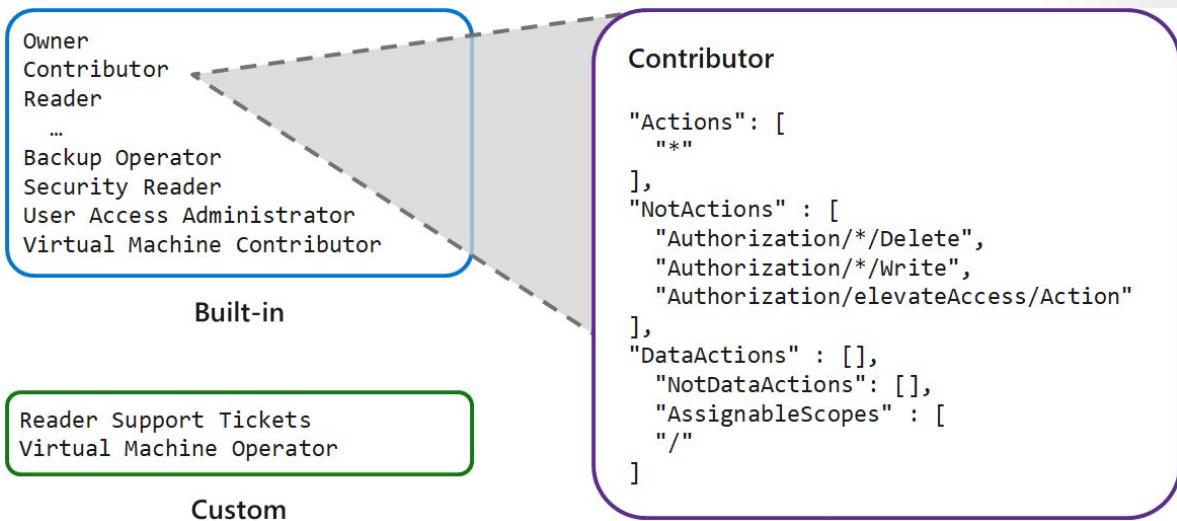
Considerations

Using Azure RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope.

When planning your access control strategy, it's a best practice to grant users the least privilege to get their work done. The following diagram shows a suggested pattern for using Azure RBAC.

Create a Role Definition

Each role is a set of properties defined in a JSON file. This role definition includes Name, Id, and Description. The definition also includes the allowable permissions (Actions), denied permissions (NotActions), and scope (read access, etc.) for the role.



In this example, the Owner role means all (asterisk) actions, no denied actions, and all (/) scopes.

```

Name: Owner
ID: 8e3af657-a8ff-443c-a75c-2fe8c4bcb65
IsCustom: False
Description: Manage everything, including access to resources
Actions: {*}
NotActions: {}
AssignableScopes: {/}

```

Actions and NotActions

The Actions and NotActions properties can be tailored to grant and deny the exact permissions you need. This table defines how the Owner, Contributor, and Reader roles.

Built-in Role	Action	NotActions
Owner (allow all actions)	*	
Contributor (allow all actions except writing or deleting role assignment)	*	Microsoft.Authorization/*/Delete, Microsoft.Authorization/*/Write, Microsoft.Authorization/elevateAccess/Action
Reader (allow all read actions)	*/read	

Scope your role

After defining the Actions and NotActions properties, you must scope the role.

The AssignableScopes property of the role specifies the role scope. The scope can be subscriptions, resource groups, or resources.

- * /subscriptions/[subscription id]
- * /subscriptions/[subscription id]/resourceGroups/[resource group name]
- * /subscriptions/[subscription id]/resourceGroups/[resource group name] /

```
[resource]
```

Example 1

Make a role available for assignment in two subscriptions.

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e", "/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624"
```

Example 2

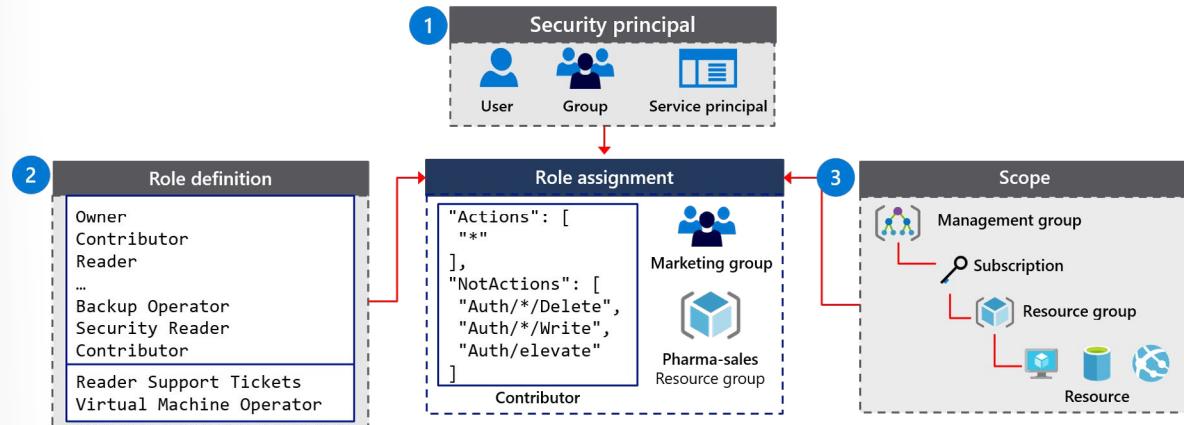
Makes a role available for assignment only in the Network resource group.

```
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups/Network"
```

Create a Role Assignment

A role assignment is the process of scoping a role definition to a user, group, service principal, or managed identity. The purpose of the role assignment is to grant access. Access is revoked by removing a role assignment.

For example, in the diagram, the Marketing group has been assigned the Contributor role for the pharma-sales resource group. Users in the Marketing group can create or manage any Azure resource in the pharma-sales resource group. Marketing users don't have access to resources outside the pharma-sales resource group, unless they are part of another role assignment.



Note: A resource inherits role assignments from its parent resource.

Compare Azure RBAC Roles to Azure AD Roles

When you are new to Azure, you may find it a little challenging to understand all the different roles in Azure. This article helps explain the following roles and when you would use each:

- Classic subscription administrator roles
- Azure role-based access control (RBAC) roles

- Azure Active Directory (Azure AD) administrator roles

To better understand roles in Azure, it helps to know some of the history. When Azure was initially released, access to resources was managed with just three administrator roles: Account Administrator, Service Administrator, and Co-Administrator. Later, role-based access control (RBAC) for Azure resources was added. Azure RBAC is a newer authorization system that provides fine-grained access management to Azure resources. RBAC includes many built-in roles, can be assigned at different scopes, and allows you to create your own custom roles. To manage resources in Azure AD, such as users, groups, and domains, there are several Azure AD administrator roles.

Differences between Azure RBAC roles and Azure AD roles

At a high level, Azure RBAC roles control permissions to manage Azure resources, while Azure AD administrator roles control permissions to manage Azure Active Directory resources. The following table compares some of the differences.

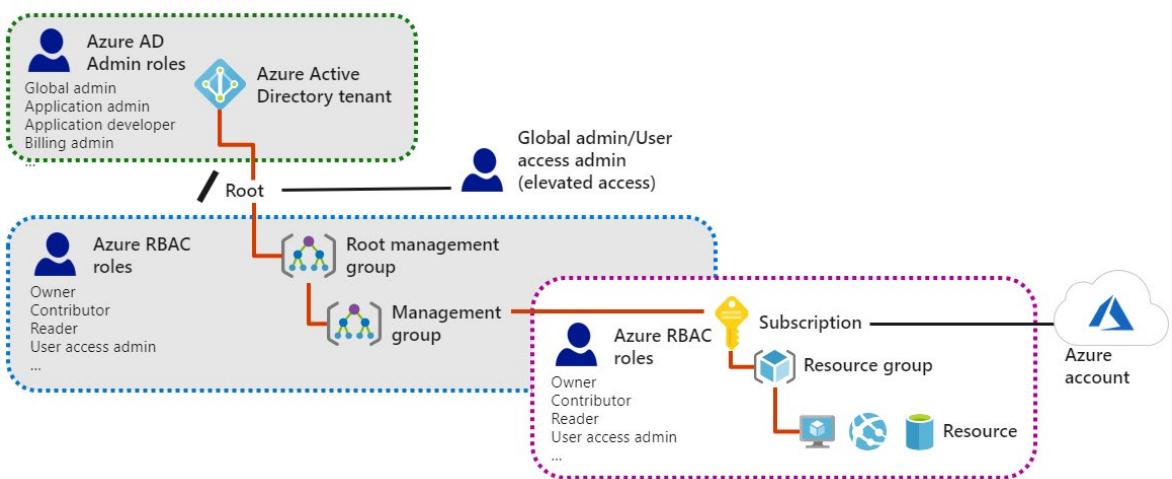
Azure RBAC roles	Azure AD roles
Manage access to Azure resources.	Manage access to Azure Active Directory resources.
Scope can be specified at multiple levels (management group, subscription, resource group, resource).	Scope is at the tenant level.
Role information can be accessed in Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API.	Role information can be accessed in Azure admin portal, Microsoft 365 admin portal, Microsoft Graph AzureAD PowerShell.

Note: Azure Resource Manager roles should be used instead of Classic administrator roles.

Apply RBAC Authentication

RBAC includes many built-in roles, can be assigned at different scopes, and allows you to create your own custom roles. To manage resources in Azure AD, such as users, groups, and domains, there are several Azure AD administrator roles.

This diagram is a high-level view of how the Azure RBAC roles and Azure AD administrator roles are related.



Note: Do you understand how Azure AD Admin roles and Azure RBAC roles work together to authenticate users?

Determine Azure RBAC Roles

Azure includes several built-in roles that you can use. There are four fundamental built-in roles. The first three apply to all resource types.

- **Owner.** Has full access to all resources including the right to delegate access to others. The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scope.
- **Contributor.** Can create and manage all types of Azure resources but can't grant access to others.
- **Reader.** Can view existing Azure resources.
- **User Access Administrator.** Lets you manage user access to Azure resources, rather than to managing resources.

Other things to know

- There are other built-in roles. For example, the **Virtual Machine Contributor** role allows a user to create and manage virtual machines.
- When the built-in roles don't meet the specific needs of your organization, you can create your own custom roles.
- Roles can grant access to data within an object. For example, if a user has read data access to a storage account, then they can read the blobs or messages in the storage account.

Demonstration - Azure RBAC

In this demonstration, we will learn about role assignments.

Locate Access Control blade

1. Access the Azure portal and select a resource group. Make a note of what resource group you use.
2. Select the **Access Control (IAM)** blade.
3. This blade will be available for many different resources so you can control access.

Review role permissions

1. Select the **Roles** tab (top).
2. Review the large number of built-in roles that are available.
3. Double-click a role, and then select **Permissions** (top).
4. Continue drilling into the role until you can view the **Read, Write, and Delete** actions for that role.
5. Return to the **Access Control (IAM)** blade.

Add a role assignment

1. Create a user.
2. Select **Add role assignment.**
 - **Role:** Owner
 - **Select:** Managers

- **Save** your changes.
3. Select **Check access**.
 4. Select the user.
 5. Notice the user is part of the Managers group and is an Owner.
 6. Notice that you can **Deny assignments**.

Optional - Explore PowerShell commands

1. Open the Azure Cloud Shell.
2. Select the PowerShell drop-down.
3. List role definitions.

```
Get-AzRoleDefinition | FT Name, Description
```

4. List the actions of a role.

```
Get-AzRoleDefinition owner | FL Actions, NotActions
```

5. List role assignments.

```
Get-AzRoleAssignment -ResourceGroupName <resource group name>
```

Knowledge check

Choose the best response for each question.

Multiple choice

Your company hires a new IT administrator. She needs to manage a resource group with first-tier web servers including assigning permissions. However, she should not have access to other resource groups inside the subscription. You need to configure role-based access. What should you do? Select one.

- Assign her as a Subscription Contributor.
- Assign her as a Resource Group Owner.
- Assign her as a Resource Group Contributor.

Multiple choice

You have three virtual machines (VM1, VM2, and VM3) in a resource group. The Helpdesk hires a new employee. The new employee must be able to modify the settings on VM3, but not on VM1 and VM2. Your solution must minimize administrative overhead. What should you do? Select one.

- Assign the user to the Contributor role on the resource group.
- Assign the user to the Contributor role on VM3.
- Move VM3 to a new resource group and assign the user to the Contributor role on VM3.

Multiple choice

Your company wants to allow some users to control the virtual machines in each environment. These users should be prevented from modifying networking and other resources in the same resource group or Azure subscription. What should you do? Select one.

- Create a policy in Azure Policy that audits resource usage
- Split the environment into separate resource groups
- Create a role assignment through Azure RBAC

Multiple choice

Suppose a team member can't view resources in a resource group. Where would the administrator go to check the team member's access? Select one.

- Check the team member's permissions by going to their Azure profile > My permissions.
- Go to the resource group and select Access control (IAM) > Role assignments.
- Go to one of the resources in the resource group and select Role assignments.

Multiple choice

A user who had Owner access to a subscription is leaving the company. No one else has access to this subscription. How can you grant another employee access to this subscription? Select one.

- Use the Azure portal to elevate your own access.
- Ask the former employee for their password.
- Ask the former employee to sign in and select a different employee to grant their permissions to.

Multiple choice

What's included in a custom Azure role definition? Select one.

- The assignment of the custom role
- Operations allowed for Azure resources and the scope of permissions
- Actions and DataActions operations that you can scope to the tenant level

Multiple choice

What information does an Action provide in a role definition? Select one.

- An Action provides the allowed management capabilities for the role.
- An Action determines what data the role can manipulate.
- An Action decides what resource the role is applied to.

Multiple choice

How are NotActions used in a role definition? Select one.

- NotActions are subtracted from the Actions to define the list of permissible operations.
- NotActions are consulted after Actions to deny access to a specific operation.
- NotActions allow you to specify a single operation that is not allowed.

Summary and Resources

Summary

Azure role-based access control (Azure RBAC) is a system that provides fine-grained access management of Azure resources. Using Azure RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

You should now be able to:

- Identify the features and usage cases for role-based access control.
- List and create role definitions.
- Create role assignments.
- Identify the differences between Azure role-based access control and Azure Active Directory roles.
- Manage access to subscriptions using role-based access control.
- Review the built-in Azure role-based access control roles. .

Learn more

You can learn more by reviewing the following.

- [Azure RBAC documentation²¹](https://docs.microsoft.com/azure/role-based-access-control/)
- [Learn - Create custom roles for Azure resources with role-based access control²²](https://docs.microsoft.com/learn/modules/create-custom-azure-roles-with-rbac/)
- [Learn - Manage access to an Azure subscription by using Azure role-based access control²³](https://docs.microsoft.com/learn/modules/manage-subscription-access-azure-rbac/)
- [Learn - Secure your Azure resources with role-based access control²⁴](https://docs.microsoft.com/learn/modules/secure-azure-resources-with-rbac/)

²¹ <https://docs.microsoft.com/azure/role-based-access-control/>

²² <https://docs.microsoft.com/learn/modules/create-custom-azure-roles-with-rbac/>

²³ <https://docs.microsoft.com/learn/modules/manage-subscription-access-azure-rbac/>

²⁴ <https://docs.microsoft.com/learn/modules/secure-azure-resources-with-rbac/>

Module 02 Lab

Lab 02a - Manage Subscriptions and Azure RBAC

Lab scenario

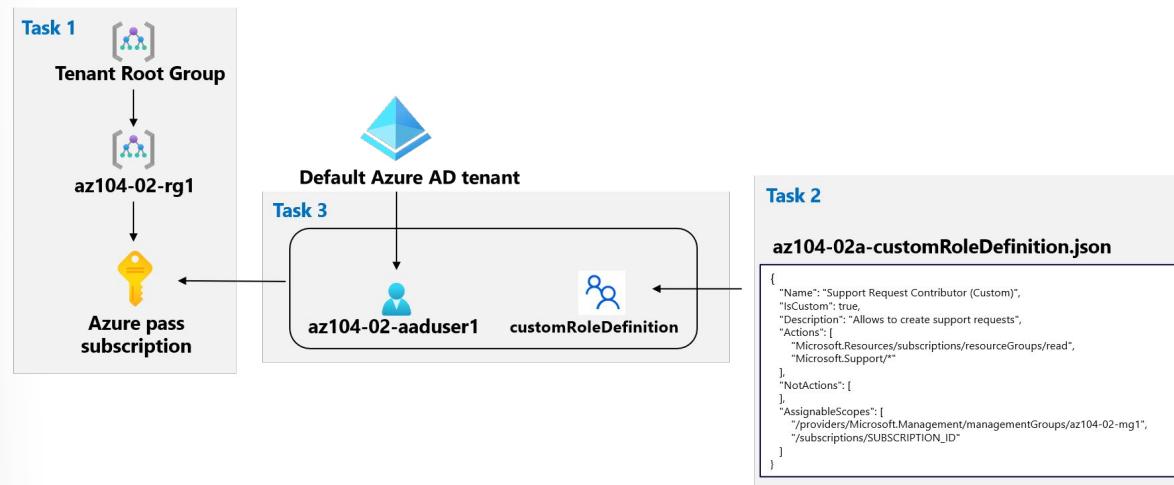
To improve the management of Azure resources in Contoso, you have been tasked with implementing the following functionality:

- using management groups for the Contoso's Azure subscriptions.
- granting user permissions for submitting support requests. This user would only be able to create support request tickets and view resource groups.

Objectives

In this lab, you will:

- Task 1: Implement Management Groups.
- Task 2: Create custom RBAC roles.
- Task 3: Assign RBAC roles.



Note: Consult with your instructor for how to access the lab instructions and lab environment (if provided)

Lab 02b - Manage Governance via Azure Policy

Lab scenario

To improve management of Azure resources in Contoso, you have been tasked with implementing the following functionality:

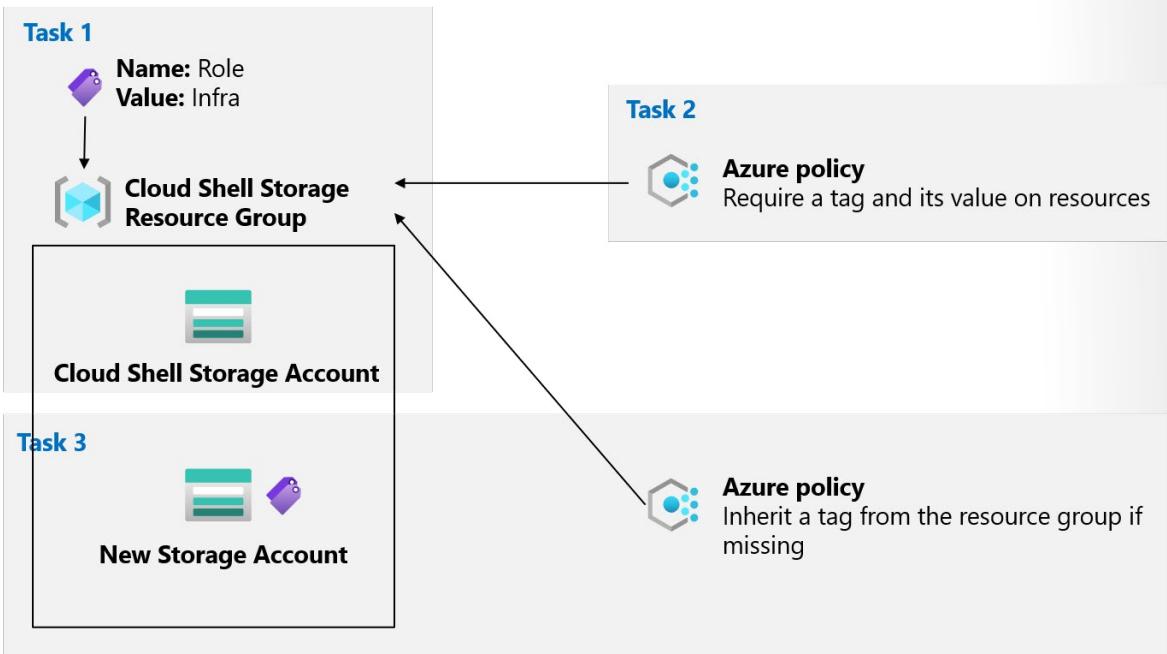
- tagging resource groups that include only infrastructure resources (such as Cloud Shell storage accounts)

- ensuring that only properly tagged infrastructure resources can be added to infrastructure resource groups
- remediating any non-compliant resources

Objectives

In this lab, we will:

- Task 1: Create and assign tags via the Azure portal.
- Task 2: Enforce tagging via an Azure policy.
- Task 3: Apply tagging via an Azure policy.



Note: Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Answers

Multiple choice

Your company financial comptroller wants to be notified whenever the company is half-way to spending the money allocated for cloud services. What should you do? Select one.

- Create an Azure reservation.
- Create a budget and a spending threshold.
- Create a management group.
- Enter workloads in the Total Cost of Ownership calculator.

Explanation

Create a budget and a spending threshold. Billing Alerts help you monitor and manage billing activity for your Azure accounts. You can set up a total of five billing alerts per subscription, with a different threshold and up to two email recipients for each alert. Monthly budgets are evaluated against spending every four hours. Budgets reset automatically at the end of a period.

Multiple choice

What tool can you use to gain greater visibility into your spending patterns? Select one.

- Cost Insights
- Cost Analysis
- Your invoice

Explanation

Cost analysis. Cost analysis is one of Azure Cost Management's primary tools to help you better understand costs.

Multiple choice

Your company is concerned about cost and provisioning too many virtual machines at once. What's the best way to control resource provisioning? Select one.

- Change your subscription to pay as you go.
- Apply spending limits to the development team's Azure subscription.
- Verbally give the managers a budget and hold them accountable for overages.

Explanation

Apply spending limits to the development team's Azure subscription. If you exceed your spending limit, active resources are deallocated. You can then decide whether to increase your limit or provision fewer resources.

Multiple choice

The leadership team wants information on resource costs by departments. What's the best way to categorize costs by department? Select one.

- Apply a tag to each resource that identifies the appropriate billing department.
- Split the cost evenly between departments.
- Keep a spreadsheet that lists each team's resources.

Explanation

Apply a tag to each resource that identifies the appropriate billing department. You can apply tags to groups of Azure resources to organize billing data.

Multiple choice

An Azure subscription ... Select one.

- is a logical container used to provision resources in Azure
- is associated with a single department or organization
- represents a single domain

Explanation

An Azure subscription is a logical container used to provision resources in Azure. A subscription might have one or more tenants, directories, and domains associated with it.

Multiple choice

Your organization has several Azure policies that they would like to create and enforce for a new branch office. What should you do? Select one.

- Create a policy initiative
- Create a management group
- Create a new subscriptions

Explanation

Create a policy initiative. A policy initiative would include all the policies of interest. Once your initiative is created, you can assign the definition to establish its scope. A scope determines what resources or grouping of resources the policy assignment gets enforced on.

Multiple choice

You would like to categorize resources and billing for different departments like IT and HR. The billing needs to be consolidated across multiple resource groups and you need to ensure everyone complies with the solution. You have created tags for each department, like department:HR. What should you do next?

- Create a billing group for each department
- Create an Azure policy
- Create a subscription account rule

Explanation

Create tags for each department and create an Azure policy. You should create a tag with a key:value pair like department:HR. You can then create an Azure policy which requires the tag be applied before a resource is created.

Multiple choice

Your company wants to ensure that only cost-effective virtual machine SKU sizes are deployed. What should you do? Select one.

- Periodically inspect the deployment to see which SKU sizes are used
- Create an Azure RBAC role that defines the allowed virtual machine SKU sizes
- Create a policy in Azure Policy that specifies the allowed SKU sizes

Explanation

Create a policy in Azure Policy that specifies the allowed SKU sizes. After you enable this policy, that policy is applied when you create new virtual machines or resize existing ones.

Multiple choice

Which of the following can be used to manage governance across multiple Azure subscriptions?

- Azure initiatives
- Resource groups
- Management groups

Explanation

Management groups. Management groups facilitate the hierarchical ordering of Azure resources into collections, at a level of scope above subscriptions. Distinct governance conditions can be applied to each management group, with Azure Policy and Azure role-based access controls, to manage Azure subscriptions effectively. The resources and subscriptions assigned to a management group automatically inherit the conditions applied to the management group.

Multiple choice

Your company hires a new IT administrator. She needs to manage a resource group with first-tier web servers including assigning permissions. However, she should not have access to other resource groups inside the subscription. You need to configure role-based access. What should you do? Select one.

- Assign her as a Subscription Contributor.
- Assign her as a Resource Group Owner.
- Assign her as a Resource Group Contributor.

Explanation

Assign her as a Resource Group owner. The new IT administrator needs to be able to assign permissions.

Multiple choice

You have three virtual machines (VM1, VM2, and VM3) in a resource group. The Helpdesk hires a new employee. The new employee must be able to modify the settings on VM3, but not on VM1 and VM2. Your solution must minimize administrative overhead. What should you do? Select one.

- Assign the user to the Contributor role on the resource group.
- Assign the user to the Contributor role on VM3.
- Move VM3 to a new resource group and assign the user to the Contributor role on VM3.

Explanation

Assign the user to the Contributor role on VM3. This means the user will not have access to VM1 or VM2. The Contributor role will allow the user to change the settings on VM1.

Multiple choice

Your company wants to allow some users to control the virtual machines in each environment. These users should be prevented from modifying networking and other resources in the same resource group or Azure subscription. What should you do? Select one.

- Create a policy in Azure Policy that audits resource usage
- Split the environment into separate resource groups
- Create a role assignment through Azure RBAC

Explanation

Create a role assignment through Azure RBAC. Azure RBAC enables you to create roles that define access permissions. You might create one role that limits access only to virtual machines and a second role that provides administrators with access to everything.

Multiple choice

Suppose a team member can't view resources in a resource group. Where would the administrator go to check the team member's access? Select one.

- Check the team member's permissions by going to their Azure profile > My permissions.
- Go to the resource group and select Access control (IAM) > Role assignments.
- Go to one of the resources in the resource group and select Role assignments.

Explanation

Go to the resource group and select Access control (IAM) > Role assignments. Find the list of role assignments on the resource group.

Multiple choice

A user who had Owner access to a subscription is leaving the company. No one else has access to this subscription. How can you grant another employee access to this subscription? Select one.

- Use the Azure portal to elevate your own access.
- Ask the former employee for their password.
- Ask the former employee to sign in and select a different employee to grant their permissions to.

Explanation

Use the Azure portal to elevate your own access. Temporarily elevate your own access to assign the Owner role to another user.

Multiple choice

What's included in a custom Azure role definition? Select one.

- The assignment of the custom role
- Operations allowed for Azure resources and the scope of permissions
- Actions and DataActions operations that you can scope to the tenant level

Explanation

Operations allowed for Azure resources and the scope of permissions. A custom role definition includes the operations allowed such as read, write, and delete for Azure resources and the scope of those permissions.

Multiple choice

What information does an Action provide in a role definition? Select one.

- An Action provides the allowed management capabilities for the role.
- An Action determines what data the role can manipulate.
- An Action decides what resource the role is applied to.

Explanation

An Action provides the allowed management capabilities for the role. The Action provides what the role can do.

Multiple choice

How are NotActions used in a role definition? Select one.

- NotActions are subtracted from the Actions to define the list of permissible operations.
- NotActions are consulted after Actions to deny access to a specific operation.
- NotActions allow you to specify a single operation that is not allowed.

Explanation

NotActions are subtracted from the Actions to define the list of permissible operations.

Module 3 Administer Azure Resources

Configure Azure Resources with Tools

Introduction

Scenario

Azure Administrators use tools to interact with the cloud environment and perform such tasks as:

- Deploying dozens or hundreds of resources at a time.
- Configuring individual services programmatically.
- Viewing rich reports across usage, health, costs, and more.

You must select and use a tooling options. Your choices can include the Azure portal, Azure PowerShell, Azure CLI, or Azure Cloud Shell.

Skills measured

These administrative tools are not directly tested on **Exam AZ-104: Microsoft Azure Administrator¹**. However, may be used during performance-based testing.

Learning objectives

In this module, you will learn how to:

- Manage resources with the Azure portal.
- Manage resources with Azure Cloud Shell.
- Manage resources with Azure PowerShell.
- Manage resources with Azure CLI.

¹ <https://docs.microsoft.com/learn/certifications/exams/az-104>

Prerequisites

None

Use the Azure Portal

The **Azure portal** lets you build, manage, and monitor everything from simple web apps to complex cloud applications in a single, unified console.

The screenshot shows the Azure portal's main dashboard. At the top is a search bar with the placeholder "Search resources, services, and docs (G+/-)". Below it is a dark navigation bar with the Microsoft logo and a "Log out" button. The main area has a light gray background. On the left, there's a sidebar titled "Azure services" with icons for "Create a resource" (plus sign), "Storage accounts", "Subscriptions", "Activity log", and "Network Watcher". To the right of the sidebar is a section titled "Recent resources" with a table:

Name	Type	Last Viewed
vault135	Recovery Services vault	22 hours ago
RSV-Backup	Recovery Services vault	22 hours ago

- Search resources, services, and docs.
- Manage resources.
- Create customized dashboards and favorites.
- Access the Cloud Shell.
- Receive notifications.
- Links to the Azure documentation.

Note: You can access the portal at <https://portal.azure.com>.

Demonstration - Azure Portal

In this demonstration, you will explore the Azure portal.

Help and Keyboard Shortcuts

1. Access the Azure Portal.
2. Click the ? Help and Support icon on the top banner.
3. Select **Launch Guided Tour** and click **Start Tour**. Review the help information.
4. Select **Keyboard Shortcuts** and read through the available shortcuts. Do any seem of interest?
5. Close the Help page, hold **G** and press **D** to go your Dashboard.

Customizing your experience

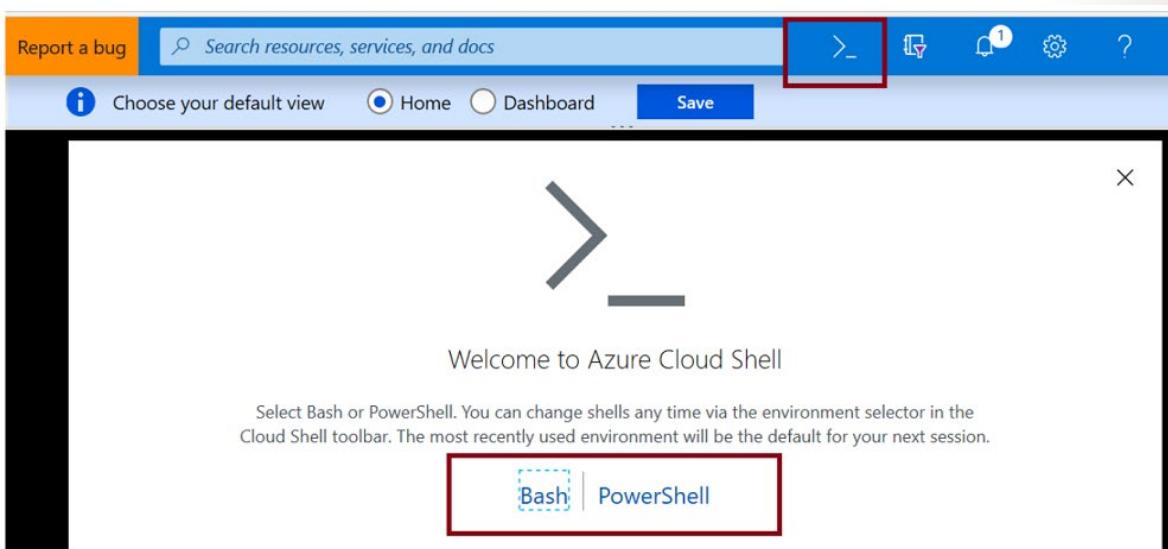
1. Examine the icons next to the Dashboard drop-down. For example, New Dashboard, Upload, Download, Edit, and Clone.

2. Click **New Dashboard**.
3. Practice adding, pinning, moving, resizing, and deleting tiles.
4. Click **Done customizing** to save your edits.
5. Select the **Settings** icon on the top banner. Experiment with different color themes. **Apply** your changes.
6. Practice reordering your **Favorites** list. Do this by holding and dragging list items up or down.
7. Notice how clicking a Favorite takes you to that page.
8. Click the **Cost Management and Billing** blade. **Pin** your Subscription information to your Dashboard.
9. Visit the Dashboard and make any arrangement changes you like.
10. Use the *search* textbox at the top of the page.
11. Type *resource* and notice context matches are provided.
12. Select **Resource groups** and then click **+ Add**.
13. **Review and create** your first resource group.

Use Azure Cloud Shell

Azure Cloud Shell is an interactive, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work. Linux users can opt for a Bash experience, while Windows users can opt for PowerShell.

Cloud Shell enables access to a browser-based command-line experience built with Azure management tasks in mind. You can use Cloud Shell to work untethered from a local machine in a way only the cloud can provide.



Azure Cloud Shell features

- Is temporary and requires a new or existing Azure Files share to be mounted.
- Offers an integrated graphical text editor based on the open-source Monaco Editor.

- Authenticates automatically for instant access to your resources.
- Runs on a temporary host provided on a per-session, per-user basis.
- Times out after 20 minutes without interactive activity.
- Requires a resource group, storage account, and Azure File share.
- Uses the same Azure file share for both Bash and PowerShell.
- Is assigned to one machine per user account.
- Persists \$HOME using a 5-GB image held in your file share.
- Permissions are set as a regular Linux user in Bash.

Demonstration - Cloud Shell

In this demonstration, we will experiment with the Cloud Shell.

Configure the Cloud Shell

1. Access the **Azure Portal**.
2. Click the **Cloud Shell** icon on the top banner.
3. On the Welcome to the Shell page, notice your selections for Bash or PowerShell. Select **PowerShell**.
4. The Azure Cloud Shell requires an Azure file share to persist files. As you have time, click Learn more to obtain information about the Cloud Shell storage and the associated pricing.
5. Select your **Subscription** and click **Create Storage**.

Experiment with Azure PowerShell

1. Wait for your storage to be created and your account to be initialized.
2. At the PowerShell prompt, type **Get-AzSubscription** to view your subscriptions.
3. Type **Get-AzResourceGroup** to view resource group information.

Experiment with the Bash shell

1. Use the drop-down to switch to the **Bash** shell and confirm your choice.
2. At the Bash shell prompt, type **az account list** to view your subscriptions. Also, try tab completion.
3. Type **az resource list** to view resource information.

Experiment with the Cloud Editor

1. To use the Cloud Editor, type **code ..** You can also select the curly braces icon.
2. Select a file from the left navigation pane. For example, **.profile**.
3. Notice on the editor top banner, selections for Settings (Text Size and Font) and Upload/Download files.
4. Notice on the ellipses (...) on the far right for Save, Close Editor, and Open File.
5. Experiment as you have time, then **close** the Cloud Editor.
6. Close the Cloud Shell.

Use Azure PowerShell

Azure PowerShell is a module that you add to Windows PowerShell or PowerShell Core to enable you to connect to your Azure subscription and manage resources. Azure PowerShell requires PowerShell to function. PowerShell provides services such as the shell window and command parsing. Azure PowerShell adds the Azure-specific commands.

For example, Azure PowerShell provides the **New-AzVm** command that creates a virtual machine inside your Azure subscription. To use it, you would launch the PowerShell application and then issue a command such as the following command:

```
New-AzVm  
  -ResourceGroupName "CrmTestingResourceGroup"  
  -Name "CrmUnitTests"  
  -Image "UbuntuLTS"  
  ...
```

Azure PowerShell is also available two ways: inside a browser via the Azure Cloud Shell, or with a local installation on Linux, macOS, or the Windows operating system. In both cases, you have two modes from which to choose: you can use it in interactive mode in which you manually issue one command at a time, or in scripting mode where you execute a script that consists of multiple commands.

What is the Az module?

Az is the formal name for the Azure PowerShell module containing cmdlets to work with Azure features. It contains hundreds of cmdlets that let you control nearly every aspect of every Azure resource. You can work with the following features, and more:

- Resource groups
- Storage
- VMs
- Azure AD
- Containers
- Machine learning

This module is an open-source component [available on GitHub](#)².

Note: You might have seen or used Azure PowerShell commands that used an **-AzureRM** format. In December 2018 Microsoft released for general availability the AzureRM module replacement with the Az module. This new module has several features, notably a shortened cmdlet noun prefix of **-Az**, which replaces **AzureRM**. The **Az** module ships with backwards compatibility for the AzureRM module, so the **-AzureRM** cmdlet format will work.

Note: Bookmark the [Azure PowerShell Reference](#)³

Demonstration - Working with PowerShell

In this demonstration, we will install Azure Az PowerShell module. The Az module is available from a global repository called the *PowerShell Gallery*. You can install the module onto your local machine

² <https://github.com/Azure/azure-powershell>

³ <https://docs.microsoft.com/powershell/module/az.compute/get-azvm?view=azps-3.3.0>

through the **Install-Module** command. You need an elevated PowerShell shell prompt to install modules from the PowerShell Gallery.

Note: If at any time you receive errors about *running scripts is disabled* be sure to set the execution policy:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine
```

Note: You may need to run this code in PowerShell to enable TLSv2:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Install the Az module

1. Open the **Start** menu, and type **Windows PowerShell**.
2. Right-click the **Windows PowerShell** icon, and select **Run as administrator**.
3. In the **User Account Control** dialog, select **Yes**.
4. Type the following command, and then press Enter. This command installs the module for all users by default. (It's controlled by the scope parameter.) AllowClobber overwrites the previous PowerShell module.

```
Install-Module -Name Az -AllowClobber
```

Install NuGet (if needed)

1. Depending on the NuGet version you have installed you might get a prompt to download and install the latest version.
2. If prompted, install and import the NuGet provider.

Trust the repository

1. By default, the PowerShell Gallery isn't configured as a trusted repository for PowerShellGet. The first time you use the PowerShell Gallery, you will be prompted.

You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from PSGallery'?

2. As prompted, install the modules.

Connect to Azure and view your subscription information

1. Connect to Azure.

```
Connect-AzAccount
```

2. When prompted provide your credentials.
3. Verify your subscription information.

```
Get-AzSubscription
```

Create resources

1. Create a new resource group. Provide a different location if you like. The *name* must be unique within your subscription. The *location* determines where the metadata for your resource group will be stored. You use strings like "West US", "North Europe", or "West India" to specify the location; alternatively, you can use single word equivalents, such as westus, northeurope, or westindia. The core syntax is:

```
New-AzResourceGroup -name <name> -location <location>
```

2. Verify your resource group.

```
Get-AzResourceGroup
```

3. Remove your resource group. When prompted, confirm.

```
Remove-AzResourceGroup -Name Test
```

Use Azure CLI

Azure CLI is a command-line program to connect to Azure and execute administrative commands on Azure resources. It runs on Linux, macOS, and Windows, and allows administrators and developers to execute their commands through a terminal, command-line prompt, or script instead of a web browser. For example, to restart a VM, you would use a command such as the following:

```
az vm restart -g MyResourceGroup -n MyVm
```

Azure CLI provides cross-platform command-line tools for managing Azure resources. You can install this locally on computers running the Linux, macOS, or Windows operating systems. You can also use Azure CLI from a browser through Azure Cloud Shell.

In both cases, Azure CLI can be used interactively or through scripts:

- **Interactive.** First, for Windows operating systems, launch a shell such as cmd.exe, or for Linux or macOS, use Bash. Then issue the command at the shell prompt.
- **Scripted.** Assemble the Azure CLI commands into a shell script using the script syntax of your chosen shell. Then execute the script.

Azure CLI lets you control nearly every aspect of every Azure resource. You can work with resource groups, storage, VMs, Azure Active Directory (Azure AD), containers, machine learning, and so on.

Commands in the CLI are structured in *groups* and *subgroups*. Each group represents a service provided by Azure, and the subgroups divide commands for these services into logical groupings. For example, the *storage* group contains subgroups including **account**, **blob**, **storage**, and **queue**.

So, how do you find the particular commands you need? One way is to use `az find`. For example, if you want to find commands that might help you manage a storage blob, you can use the following find command:

```
az find blob
```

If you already know the name of the command you want, the `--help` argument for that command will get you more detailed information on the command, and for a command group, a list of the available subcommands. For example, here's how you can get a list of the subgroups and commands for managing blob storage:

```
az storage blob --help
```

Note: Bookmark the [Azure CLI Reference⁴](#).

Demonstration-Working with Azure CLI

In this demonstration, we will install and use the CLI to create resources.

Install the CLI on Windows

You install Azure CLI on the Windows operating system using the MSI installer:

1. Go to <https://aka.ms/installazurecliwindows>, and in the browser security dialog box, click **Run**.
2. In the installer, accept the license terms, and then click **Install**.
3. In the **User Account Control** dialog, select **Yes**.

Verify Azure CLI installation

1. You run Azure CLI by opening a Bash shell for Linux or macOS, or from the command prompt or PowerShell for Windows.
2. Start Azure CLI and verify your installation by running the version check:

```
az --version
```

Note: Running Azure CLI from PowerShell has some advantages over running Azure CLI from the Windows command prompt. PowerShell provides more tab completion features than the command prompt.

Login to Azure

1. Because you're working with a local Azure CLI installation, you'll need to authenticate before you can execute Azure commands. You do this by using the Azure CLI **login** command:

```
az login
```

2. Azure CLI will typically launch your default browser to open the Azure sign-in page. If this doesn't work, follow the command-line instructions and enter an authorization code at <https://aka.ms/devicelogin>.
3. After a successful sign in, you'll be connected to your Azure subscription.

Create a resource group

1. You'll often need to create a new resource group before you create a new Azure service, so we'll use resource groups as an example to show how to create Azure resources from the CLI.
2. Azure CLI **group create** command creates a resource group. You must specify a name and location. The *name* must be unique within your subscription. The *location* determines where the metadata for your resource group will be stored. You use strings like "West US", "North Europe", or "West India" to specify the location; alternatively, you can use single word equivalents, such as westus, northeurope, or westindia. The core syntax is:

```
az group create --name <name> --location <location>
```

⁴ <https://docs.microsoft.com/cli/azure/?view=azure-cli-latest>

Verify the resource group

- For many Azure resources, Azure CLI provides a **list** subcommand to view resource details. For example, the Azure CLI **group list** command lists your Azure resource groups. This is useful to verify whether resource group creation was successful:

```
az group list
```

- To get a more concise view, you can format the output as a simple table:

```
az group list --output table
```

- If you have several items in the group list, you can filter the return values by adding a **query** option. Try this command:

```
az group list --query "[?name == '<rg name>']"
```

Knowledge check

Choose the best response for each question.

Multiple choice

Which of the following is not true about the Cloud Shell?

- Authenticates automatically for instant access to your resources.
- Cloud Shell is assigned multiple machines per user account.
- Provides both Bash and PowerShell sessions.

Multiple choice

You are managing Azure locally using PowerShell. You have launched the app as an Administrator. Which of the following commands would you do first?

- Connect-AzAccount
- Get-AzResourceGroup
- Get-AzSubscription

Multiple choice

What do you need to install on your machine so you can execute Azure CLI commands locally? Select one.

- The Azure cloud shell
- The Azure CLI and Azure PowerShell
- Only the Azure CLI

Multiple choice

Which parameter can you add to most CLI commands to get concise, formatted output? Select one.

- list
- table
- group

Multiple choice

What needs to be installed on your machine to let you execute Azure PowerShell cmdlets locally? Select one.

- The Azure cloud shell
- The Azure CLI and Azure PowerShell
- The base PowerShell product and the AZ module

Multiple choice

Suppose you are building a video-editing application that will offer online storage for user-generated video content. You will store the videos in Azure Blobs, so you need to create an Azure storage account to contain the blobs. Once the storage account is in place, it is unlikely you would remove and recreate it because this would delete all the user videos. Which tool is likely to offer the quickest and easiest way to create the storage account? Select one.

- Azure portal
- Azure CLI
- Azure PowerShell

Summary and Resources

Summary

Azure Administrators have many tools when it comes to managing resources. These tools include the Azure portal, Azure Cloud Shell, Azure PowerShell, and Azure CLI.

You should now be able to:

- Manage resources with the Azure portal.
- Manage resources with Azure Cloud Shell.
- Manage resources with Azure PowerShell.
- Manage resources with Azure CLI.

Learn more

You can learn more by reviewing the following.

- **Azure portal documentation⁵**

⁵ <https://docs.microsoft.com/azure/azure-portal/>

- **Azure Cloud Shell overview⁶**
- **Azure PowerShell Reference⁷**
- **Azure CLI Reference⁸.**
- **Learn - Manage services with the Azure portal⁹**
- **Learn - Introduction to PowerShell¹⁰**
- **Learn - Automate Azure tasks using scripts with PowerShell¹¹**
- **Learn - Control Azure services with the CLI¹²**

⁶ <https://docs.microsoft.com/azure/cloud-shell/overview>

⁷ <https://docs.microsoft.com/powershell/module/az.compute/get-azvm?view=azps-3.3.0>

⁸ <https://docs.microsoft.com/cli/azure/?view=azure-cli-latest>

⁹ <https://docs.microsoft.com/learn/modules/tour-azure-portal/>

¹⁰ <https://docs.microsoft.com/learn/modules/introduction-to-powershell/>

¹¹ <https://docs.microsoft.com/learn/modules/automate-azure-tasks-with-powershell/>

¹² <https://docs.microsoft.com/learn/modules/control-azure-services-with-cli/>

Use Azure Resource Manager

Introduction

Scenario

Your company is beginning to create resources in Azure. There is no organizational plan for standardizing the effort. There have been several instances where critical resources were inadvertently deleted. It is difficult to determine who owns which resource.

You need to use resource groups to organization the company's resources.

Skills measured

Managing resources is part of **Exam AZ-104: Microsoft Azure Administrator¹³**.

Manage Azure identities and governance (15–20%)

Manage subscriptions and governance

- Configure resource locks.
- Manage resource groups.

Deploy and manage Azure compute resources (20–25%)

Configure VMs

- Move VMs from one resource group to another.

Learning objectives

In this module, you will learn how to:

- Identify the features and usage cases for Azure Resource Manager.
- Describe each Azure Resource Manager component and its usage.
- Organize your Azure resources with resource groups.
- Apply Azure Resource Manager locks.
- Move Azure resources between groups, subscriptions, and regions.
- Remove resources and resource groups.
- Apply and track resource limits.

Prerequisites

None

Review Resource Manager Benefits

The infrastructure for your application is typically made up of many components – maybe a virtual machine, storage account, and virtual network, or a web app, database, database server, and third-party

¹³ <https://docs.microsoft.com/learn/certifications/exams/az-104>

services. These components are not separate entities, instead they are related and interdependent parts of a single entity. You want to deploy, manage, and monitor them as a group.

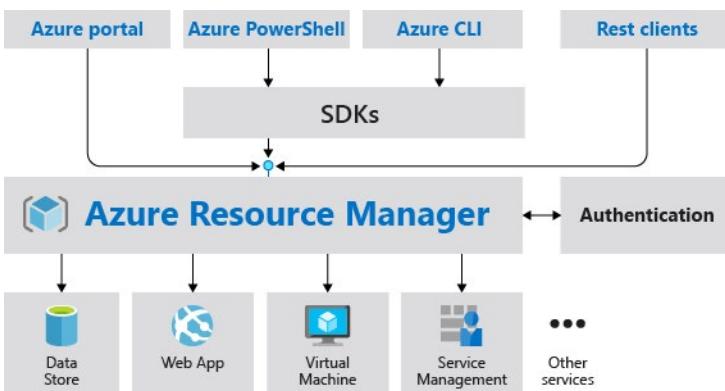
Azure Resource Manager enables you to work with the resources in your solution as a group. You can deploy, update, or delete all the resources for your solution in a single, coordinated operation. You use a template for deployment and that template can work for different environments such as testing, staging, and production. Resource Manager provides security, auditing, and tagging features to help you manage your resources after deployment.

Consistent management layer

Resource Manager provides a consistent management layer to perform tasks through Azure PowerShell, Azure CLI, Azure portal, REST API, and client SDKs. All capabilities that are available in the Azure portal are also available through Azure PowerShell, Azure CLI, the Azure REST APIs, and client SDKs. Functionality initially released through APIs will be represented in the portal within 180 days of initial release.

Choose the tools and APIs that work best for you - they have the same capability and provide consistent results.

The following image shows how all the tools interact with the same Azure Resource Manager API. The API passes requests to the Resource Manager service, which authenticates and authorizes the requests. Resource Manager then routes the requests to the appropriate resource providers.



Benefits

Resource Manager provides several benefits:

- You can deploy, manage, and monitor all the resources for your solution as a group, rather than handling these resources individually.
- You can repeatedly deploy your solution throughout the development lifecycle and have confidence your resources are deployed in a consistent state.
- You can manage your infrastructure through declarative templates rather than scripts.
- You can define the dependencies between resources so they're deployed in the correct order.
- You can apply access control to all services in your resource group because Role-Based Access Control (RBAC) is natively integrated into the management platform.
- You can apply tags to resources to logically organize all the resources in your subscription.
- You can clarify your organization's billing by viewing costs for a group of resources sharing the same tag.

Guidance

The following suggestions help you take full advantage of Resource Manager when working with your solutions.

- Define and deploy your infrastructure through the declarative syntax in Resource Manager templates, rather than through imperative commands.
- Define all deployment and configuration steps in the template. You should have no manual steps for setting up your solution.
- Run imperative commands to manage your resources, such as to start or stop an app or machine.
- Arrange resources with the same lifecycle in a resource group. Use tags for all other organizing of resources.

Review Azure Resource Terminology

If you're new to Azure Resource Manager (ARM), there are some terms you might not be familiar with.

- **resource** - A manageable item that is available through Azure. Some common resources are a virtual machine, storage account, web app, database, and virtual network, but there are many more.
- **resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.
- **resource provider** - A service that supplies the resources you can deploy and manage through Resource Manager. Each resource provider offers operations for working with the resources that are deployed. Some common resource providers are Microsoft.Compute, which supplies the virtual machine resource, Microsoft.Storage, which supplies the storage account resource, and Microsoft.Web, which supplies resources related to web apps.
- **ARM template** - A JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group. It also defines the dependencies between the deployed resources. The template can be used to deploy the resources consistently and repeatedly.
- **declarative syntax** - Syntax that lets you state "Here is what I intend to create" without having to write the sequence of programming commands to create it. The Resource Manager template is an example of declarative syntax. In the file, you define the properties for the infrastructure to deploy to Azure.

Resource providers

Each resource provider offers a set of resources and operations for working with an Azure service. For example, if you want to store keys and secrets, you work with the **Microsoft.KeyVault** resource provider. This resource provider offers a resource type called vaults for creating the key vault.

The name of a resource type is in the format: **{resource-provider}/{resource-type}**. For example, the key vault type is **Microsoft.KeyVault/vaults**.

Note: Before deploying your resources, you should gain an understanding of the available resource providers. Knowing the names of resource providers and resources helps you define resources you want to deploy to Azure. Also, you need to know the valid locations and API versions for each resource type.

Create Resource Groups

Resources can be deployed to any new or existing resource group. Deployment of resources to a resource group becomes a job where you can track the template execution. If deployment fails, the output of the job can describe why the deployment failed. Whether the deployment is a single resource to a group or a template to a group, you can use the information to fix any errors and redeploy. Deployments are incremental; if a resource group contains two web apps and you decide to deploy a third, the existing web apps will not be removed. Currently, immutable deployments are not supported in a resource group. To implement an immutable deployment, you must create a new resource group.

Considerations

Resource Groups are at their simplest a logical collection of resources. There are a couple of small rules for resource groups.

- Resources can only exist in one resource group.
- Resource Groups cannot be renamed.
- Resource Groups can have resources of many different types (services).
- Resource Groups can have resources from many different regions.

Creating resource groups

There are some important factors to consider when defining your resource group:

- All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.
- Each resource can only exist in one resource group.
- You can add or remove a resource to a resource group at any time.
- You can move a resource from one resource group to another group.
- A resource group can contain resources that reside in different regions.
- A resource group can be used to scope access control for administrative actions.
- A resource can interact with resources in other resource groups. This interaction is common when the two resources are related but don't share the same lifecycle (for example, web apps connecting to a database).

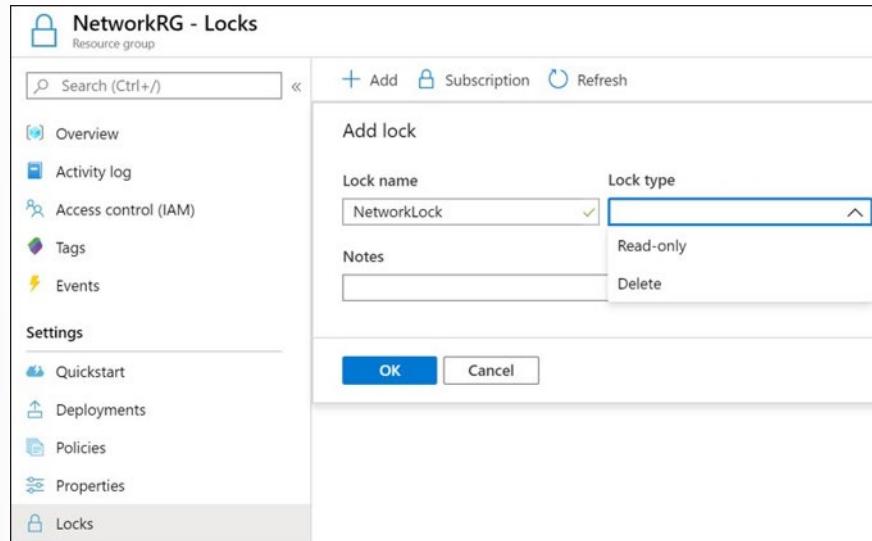
When creating a resource group, you need to provide a location for that resource group. You may be wondering, "Why does a resource group need a location? And, if the resources can have different locations than the resource group, why does the resource group location matter at all?" The resource group stores metadata about the resources. Therefore, when you specify a location for the resource group, you're specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region.

Note: By scoping permissions to a resource group, you can add/remove and modify resources easily without having to recreate assignments and scopes.

Create Resource Manager Locks

A common concern with resources provisioned in Azure is the ease with which they can be deleted. An over-zealous or careless administrator can accidentally erase months of work with a few steps. Resource Manager locks allow organizations to put a structure in place that prevents the accidental deletion of resources in Azure.

- You can associate the lock with a subscription, resource group, or resource.
- Locks are inherited by child resources.



Lock types

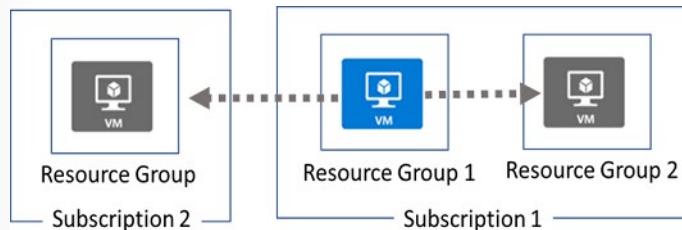
There are two types of resource locks.

- **Read-Only locks**, which prevent any changes to the resource.
- **Delete locks**, which prevent deletion.

Note: Only the Owner and User Access Administrator roles can create or delete management locks.

Reorganize Azure Resources

Sometimes you may need to move resources to either a new subscription or a new resource group in the same subscription.



When moving resources, both the source group and the target group are locked during the operation. Write and delete operations are blocked on the resource groups until the move completes. This lock means you can't add, update, or delete resources in the resource groups. Locks don't mean the resources

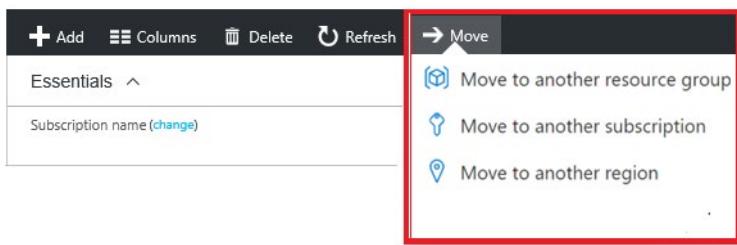
aren't available. For example, if you move a virtual machine to a new resource group, an application can still access the virtual machine.

Limitations

Before beginning this process be sure to read the **Move operation support for resources¹⁴** page. This page details what resources can be moved between resources group, subscriptions, and regions.

Implementation

To move resources, select the resource group containing those resources, and then select the **Move** button. Select the resources to move and the destination resource group. Acknowledge that you need to update scripts.



Note: Just because a service can be moved doesn't mean there aren't restrictions. For example, you can move a virtual network, but you must also move its dependent resources, like gateways.

Remove Resources and Resource Groups

Use caution when deleting a resource group. Deleting a resource group deletes all the resources contained within it. That resource group might contain resources that resources in other resource groups depend on.



Using PowerShell to delete resource groups

To remove a resource group use, **Remove-AzResourceGroup**. In this example, we are removing the ContosoRG01 resource group from the subscription. The cmdlet prompts you for confirmation and returns no output.

```
Remove-AzResourceGroup -Name "ContosoRG01"
```

Removing Resources

You can also delete individual resources within a resource group. For example, here we are deleting a virtual network. Notice you can change the resource group on this page.

¹⁴ <https://docs.microsoft.com/azure/azure-resource-manager/management/move-support-resources>

ASH-vnet
Virtual network

Refresh Move Delete

Resource group (change) : ASH

Location : West Central US

Subscription (change) : Visual Studio Enterprise

Subscription ID : aa509d92-2

Tags (change) : Click here to add tags

Determine Resource Limits

Azure lets you view resource usage against limits this is helpful to track current usage, and plan for future use.

ASC DEMO | Usage + quotas

Subscription

Settings

- Programmatic deployment
- Resource groups
- Resources
- Usage + quotas
- Policies
- Security
- Events

You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. [Learn more](#)

[Request Increase](#)

Quota	Provider	Location	Usage	Limit
Total Regional vCPUs	Microsoft.Compute	East US	<div style="width: 25%;">25 %</div>	25 of 100
Total Regional vCPUs	Microsoft.Compute	West Europe	<div style="width: 21%;">21 %</div>	21 of 100
Total Regional vCPUs	Microsoft.Compute	Central US	<div style="width: 17%;">17 %</div>	17 of 100
Standard Dv2 Family vCPUs	Microsoft.Compute	West Europe	<div style="width: 16%;">16 %</div>	16 of 100
Standard DSv2 Family vCPUs	Microsoft.Compute	Central US	<div style="width: 14%;">14 %</div>	14 of 100

- The limits shown are the limits for your subscription.
- When you need to increase a default limit, there is a Request Increase link.
- All resources have a maximum limit listed in Azure [limits¹⁵](#).
- If you are at the maximum limit, the limit can't be increased.

Demonstration - Resource Manager

In this demonstration, we will work with the Azure Resource Manager.

Note: Only the Owner and User Access Administrator roles can manage the locks on the resources.

Manage resource groups in the portal

- Access the Azure portal.
- Create a resource group. Remember the name of this resource group.
- In the **Settings** blade for the resource group, select **Locks**.

¹⁵ <https://docs.microsoft.com/azure/azure-subscription-service-limits?toc=%2fazure%2fnetworking%2ftoc.json>

4. To add a lock, select **Add**. If you want to create a lock at a parent level, select the parent. The currently selected resource inherits the lock from the parent. For example, you could lock the resource group to apply a lock to all its resources.
5. Give the lock a **name** and **lock type**. Optionally, you can add notes that describe the lock.
6. To delete the lock, select the ellipsis and **Delete** from the available options.

Optional - Manage resource groups with PowerShell

1. Access the Cloud Shell.
2. Create the resource lock and confirm your action.

```
New-AzResourceLock -LockName <lockName> -LockLevel CanNotDelete -Resource-  
GroupName <resourceGroupName>
```

3. View resource lock information. Notice the LockId that will be used in the next step to delete the lock.

```
Get-AzResourceLock
```

4. Delete the resource lock and confirm your action.

```
Remove-AzResourceLock -LockName <Name> -ResourceGroupName <Resource Group>
```

5. Verify the resource lock has been removed.

```
Get-AzResourceLock
```

Knowledge check

Choose the best response for each question.

Multiple choice

You have a new Azure subscription and need to move resources to that subscription. Which of the following resources cannot be moved? Select one.

- Key vault
- Storage account
- Tenant

Multiple choice

You are reviewing your virtual machine usage. You notice that you have reached the limit for virtual machines in the US East region. Which of the following provides the easiest solution? Select one.

- Add another resource group
- Change your subscription plan
- Request support increase your limit

Multiple choice

Which of the following would be good example of when to use a resource lock? Select one.

- A ExpressRoute circuit with connectivity back to your on-premises network.
- A non-production virtual machine used to test occasional application builds.
- A storage account used to temporarily store images processed in a development environment.

Multiple choice

Your manager asks you to explain how Azure uses resource groups. You provide all of the following information, except? Select one.

- Resources can be in only one resource group.
- Resources can be moved from one resource group to another resource group.
- Resource groups can be nested.

Summary and Resources

Summary

Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment.

You should now be able to:

- Identify the features and usage cases for Azure Resource Manager.
- Describe each Azure Resource Manager component and its usage.
- Organize your Azure resources with resource groups.
- Apply Azure Resource Manager locks.
- Move Azure resources between groups, subscriptions, and regions.
- Remove resources and resource groups.
- Apply and track resource limits.

Learn more

You can learn more by reviewing the following.

- **Azure Resource Manager documentation¹⁶**
- **Learn - Control and organize Azure resources with Azure Resource Manager¹⁷**

¹⁶ <https://docs.microsoft.com/azure/azure-resource-manager/management/overview>

¹⁷ <https://docs.microsoft.com/learn/modules/control-and-organize-with-azure-resource-manager/>

Configure Resources ARM Templates

Introduction

Scenario

Your company needs to ensure virtual machine deployments are consistent across the organization.

You use Azure Resource Manager templates to deploy resources including virtual machines.

Skills measured

Deploying resources using Azure Resource Manager templates is part of **Exam AZ-104: Microsoft Azure Administrator¹⁸**.

Deploy and manage Azure compute resources (20–25%)

Automate deployment of virtual machines (VMs) by using Azure Resource Manager templates

- Modify an Azure Resource Manager template.
- Deploy from a template.
- Save a deployment as an Azure Resource Manager template.

Learning objectives

In this module, you will learn how to:

- List the advantages of Azure templates.
- Identify the Azure template schema components.
- Specify Azure template parameters.
- Locate and use Azure QuickStart templates.

Prerequisites

None

Review ARM Template Advantages

An **Azure Resource Manager template** precisely defines all the Resource Manager resources in a deployment. You can deploy a Resource Manager template into a resource group as a single operation.

Using Resource Manager templates will make your deployments faster and more repeatable. For example, you no longer have to create a VM in the portal, wait for it to finish, and then create the next VM. Resource Manager takes care of the entire deployment for you.

¹⁸ <https://docs.microsoft.com/learn/certifications/exams/az-104>

Template Benefits

- **Templates improve consistency.** Resource Manager templates provide a common language for you and others to describe your deployments. Regardless of the tool or SDK that you use to deploy the template, the structure, format, and expressions inside the template remain the same.
- **Templates help express complex deployments.** Templates enable you to deploy multiple resources in the correct order. For example, you wouldn't want to deploy a virtual machine prior to creating an operating system (OS) disk or network interface. Resource Manager maps out each resource and its dependent resources, and creates dependent resources first. Dependency mapping helps ensure that the deployment is carried out in the correct order.
- **Templates reduce manual, error-prone tasks.** Manually creating and connecting resources can be time consuming, and it's easy to make mistakes. Resource Manager ensures that the deployment happens the same way every time.
- **Templates are code.** Templates express your requirements through code. Think of a template as a type of Infrastructure as Code that can be shared, tested, and versioned similar to any other piece of software. Also, because templates are code, you can create a "paper trail" that you can follow. The template code documents the deployment. Most users maintain their templates under some kind of revision control, such as GIT. When you change the template, its revision history also documents how the template (and your deployment) has evolved over time.
- **Templates promote reuse.** Your template can contain parameters that are filled in when the template runs. A parameter can define a username or password, a domain name, and so on. Template parameters enable you to create multiple versions of your infrastructure, such as staging and production, while still using the exact same template.
- **Templates are linkable.** You can link Resource Manager templates together to make the templates themselves modular. You can write small templates that each define a piece of a solution, and then combine them to create a complete system.
- **Templates simplify orchestration.** You only need to deploy the template to deploy all of your resources. Normally this would take multiple operations.

Explore the ARM Template Schema

ARM templates are written in JSON, which allows you to express data stored as an object (such as a virtual machine) in text. A JSON document is essentially a collection of key-value pairs. Each key is a string, whose value can be:

- A string
- A number
- A Boolean expression
- A list of values
- An object (which is a collection of other key-value pairs)

A Resource Manager template can contain sections that are expressed using JSON notation, but are not related to the JSON language itself:

```
{  
    "$schema": "http://schema.management.azure.com/schemas/2019-04- 01/  
deploymentTemplate.json#",  
    "contentVersion": "",  
    "parameters": {} ,
```

```

    "variables": {},
    "functions": [],
    "resources": [],
    "outputs": {}
}

```

Element name	Required	Description
\$schema	Yes	Location of the JSON schema file that describes the version of the template language. Use the URL shown in the preceding example.
contentVersion	Yes	Version of the template (such as 1.0.0.0). You can provide any value for this element. Use this value to document significant changes in your template. When deploying resources using the template, this value can be used to make sure that the right template is being used.
parameters	No	Values that are provided when deployment is executed to customize resource deployment.
variables	No	Values that are used as JSON fragments in the template to simplify template language expressions.
functions	No	User-defined functions that are available within the template.
resources	Yes	Resource types that are deployed or updated in a resource group.
outputs	No	Values that are returned after deployment.

Explore the ARM Template Parameters

In the parameters section of the template, you specify which values you can input when deploying the resources. The available properties for a parameter are:

```

"parameters": {
    "<parameter-name>" : {
        "type" : "<type-of-parameter-value>",
        "defaultValue": "<default-value-of-parameter>",
        "allowedValues": [ "<array-of-allowed-values>" ],
        "minValue": <minimum-value-for-int>,
        "maxValue": <maximum-value-for-int>,
        "minLength": <minimum-length-for-string-or-array>,
        "maxLength": <maximum-length-for-string-or-array-parameters>,
        "metadata": {
            ...
        }
    }
}

```

```
        "description": "<description-of-the parameter>"  
    }  
}  
}
```

Here's an example that illustrates two parameters: one for a virtual machine's username, and one for its password:

```
"parameters": {  
    "adminUsername": {  
        "type": "string",  
        "metadata": {  
            "description": "Username for the Virtual Machine."  
        }  
    },  
    "adminPassword": {  
        "type": "securestring",  
        "metadata": {  
            "description": "Password for the Virtual Machine."  
        }  
    }  
}
```

Note: You're limited to 256 parameters in a template. You can reduce the number of parameters by using objects that contain multiple properties.

Review QuickStart Templates

Azure Quickstart templates¹⁹ are Resource Manager templates provided by the Azure community.

The screenshot shows a grid of four preview cards for Azure Quickstart templates:

- Create Configuration Manager Tech Preview Lab in Azure**: This template creates a new System Center Configuration Manager Technical Preview Lab environment. It creates 4 new Azure VMs, configuring a new AD Domain Contr...
- Create a Standard Storage Account**: This template creates a Standard Storage Account.
- Deploy a Django app**: This template uses the Azure Linux CustomScript extension to deploy an application. This example creates an Ubuntu VM, does a silent install of Python, Django...
- Create an new AD Domain with 2 Domain Controllers**: This template creates 2 new VMs to be AD DCs (primary and backup) for a new Forest and Domain.

Templates provide everything you need to deploy your solution, while others might serve as a starting point for your template. Either way, you can study these templates to learn how to best author and structure your own templates.

- The README.md file provides an overview of what the template does.

¹⁹ <https://azure.microsoft.com/resources/templates/>

- The azuredeploy.json file defines the resources that will be deployed.
- The azuredeploy.parameters.json file provides the values the template needs.

Note: Take a few minutes to browse the available templates. Anything of interest?

Demonstration - QuickStart Templates

In this demonstration, we will explore QuickStart templates.

Explore the gallery

1. Start by browsing to the [Azure Quickstart Templates gallery²⁰](#). In the gallery you will find several popular and recently updated templates. These templates work with both Azure resources and popular software packages.
2. Browse through the many different types of templates that are available.
3. Are there any templates that are of interest to you?

Explore a template

1. Let's say you come across the Deploy a simple Windows VM template.

Note: The **Deploy to Azure** button enables you to deploy the template directly through the Azure portal if you wish.

Note: Scroll-down to the Use the template **PowerShell** code. You will need the **TemplateURI** in the next demo. **Copy the value**. For example,

```
https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredeploy.json
```

2. Click **Browse on GitHub** to navigate to the template's source code on GitHub.
3. Notice from this page you can also **Deploy to Azure**. Take a minute to view the Readme file. This helps to determine if the template is for you.
4. Click **Visualize** to navigate to the **Azure Resource Manager Visualizer**.
5. Notice the resources that make up the deployment, including a VM, a storage account, and network resources.
6. Use your mouse to arrange the resources. You can also use your mouse's scroll wheel to zoom in or out.
7. Click on the VM resource labeled **SimpleWinVM**.
8. Review the source code that defines the VM resource.
 - The resource's type is **Microsoft.Compute/virtualMachines**.
 - Its location, or Azure region, comes from the template parameter named **location**.
 - The VM's size is **Standard_A2**.
 - The computer name is read from a template variable, and the username and password for the VM are read from template parameters.
9. Return to the QuickStart page that shows the files in the template. Copy the link to the azuredeploy.json file.

²⁰ <https://azure.microsoft.com/resources/templates?azure-portal=true>

Note: You will need the template link in the next demonstration.

Demonstration - Run Templates with PowerShell

In this demonstration, we will create new Azure resources using PowerShell and Resource Manager templates.

Connect to your subscription

1. If you are working with a local install of the PowerShell, you'll need to authenticate before you can execute Azure commands. To do this, open the PowerShell ISE, or a PowerShell console as administrator, and run the following command:

```
Connect-AzAccount
```

2. After successfully signing in, your account and subscription details should display in the PowerShell console window. You must now select either a subscription or context, in which you will deploy your resources. If only one subscription is present it will set the context to that subscription by default. Otherwise you can specify the subscription to deploy resources into by running the following commands in sequence:

```
Get-AzContext
```

```
Set-AzContext -subscription < your subscription ID >
```

Create the resource group

1. You'll often need to create a new resource group before you create a new Azure service or resource. We'll use resource groups as an example to show how to create Azure resources from Azure PowerShell.
2. The Azure PowerShell **New-AzResourceGroup** command creates a resource group. You must specify a name and location. The name must be unique within your subscription, and the location determines where the metadata for your resource group will be stored. You use strings such as West US, North Europe, or West India to specify the location. Alternatively, you can use single word equivalents, such as westus, northeurope, or westindia.
3. Create the resource group into which we will deploy our resources using the following commands.

```
New-AzResourceGroup -Name < resource group name > -Location < your nearest datacenter >
```

Deploy the template into the resource group

1. Deploy the template with this command.

```
$templateUri = <location of the template from the previous demonstration>
New-AzResourceGroupDeployment -Name rg9deployment1 -ResourceGroupName rg9
-TemplateUri $templateUri
```

2. You will be prompted to enter values for:

- Adminusername. For example, azureuser.
- Password. Any compliant password will work, for example Passw0rd0134.
- DnsLabelprefix. This is any unique DNS name, such as your initials and random numbers.

3. To make scripts free of manual input, you can create a .ps1 file, and then enter all the commands and inputs. You could use parameter values in the script to define the *username*, *password* and *dnslabel-prefix* values, and then run the PowerShell file without input. Use the file **build.ps1²¹** as an example of how you can do this.

Note: In the previous example, we called a publicly available template on GitHub. You could also call a local template or a secure storage location, and you could define the template filename and location as a variable for use in the script. You can also specify the mode of deployment, including incremental or complete.

Verify the template deployed

1. Once you have successfully deployed the template, you need to verify the deployment. To do this, run the following commands:

```
Get-AzVM
```

2. Notice the VM name, then run the following command to obtain additional VM details:

```
Get-AzVM -Name < your VM name i.e. SimpleWinVM > -resourcegroupname < your resource group name >
```

3. You can also list the VMs in your subscription with the **Get-AzVM -Status** command. This can also specify a VM with the **-Name** property. In the following example, we assign it to a PowerShell variable:

```
$vm = Get-AzVM -Name < your VM name i.e. SimpleWinVM > -ResourceGroupName < your resource group name >
```

4. The interesting thing is that this is an object you can interact with. For example, you can take that object, make changes, and then push changes back to Azure with the **Update-AzVM** command:

```
$ResourceGroupName = "ExerciseResources"  
$vm = Get-AzVM -Name MyVM -ResourceGroupName $ResourceGroupName  
$vm.HardwareProfile.vmSize = "Standard_A3"
```

```
Update-AzVM -ResourceGroupName $ResourceGroupName -VM $vm
```

Note: Depending on your datacenter location, you could receive an error related to the VM size not being available in your region. You can modify the vmSize value to one that is available in your region.

Note: PowerShell's interactive mode is appropriate for one-off tasks. In our example, we'll likely use the same resource group for the lifetime of the project, which means that creating it interactively is reasonable. Interactive mode is often quicker and easier for this task than writing a script and then executing it only once.

Knowledge check

Choose the best response for each question.

²¹ <https://github.com/Microsoft/PartsUnlimited/blob/master/build.ps1?azure-portal=true>

Multiple choice

Which of the following is not an element in the template schema? Select one.

- Functions
- Inputs
- Outputs

Multiple choice

Which of the following best describes the format of an Azure Resource Manager template? Select one.

- A JSON document with key-value pairs
- A TXT document with key-value pairs
- An XML document with element-value pairs

Multiple choice

Azure Resource Manager templates are idempotent. This means that if you run a template with no changes a second time ... Select one.

- Azure Resource Manager will deploy new resources as copies of the previously deployed resources.
- Azure Resource Manager won't make any changes to the deployed resources.
- Azure Resource Manager will delete the previously deployed resources and redeploy them.

Summary and Resources

Summary

To implement infrastructure as code for your Azure solutions, use Azure Resource Manager templates (ARM templates). The template is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration for your project. The template uses declarative syntax, which lets you state what you intend to deploy without having to write the sequence of programming commands to create it. In the template, you specify the resources to deploy and the properties for those resources.

You should now be able to:

- List the advantages of Azure templates.
- Identify the Azure template schema components.
- Specify Azure template parameters.
- Locate and use Azure QuickStart templates.

Learn more

You can learn more by reviewing the following.

- **ARM template documentation²²**

²² <https://docs.microsoft.com/azure/azure-resource-manager/templates/>

- **Azure Quickstart Templates²³**
- **Learn - Build Azure Resource Manager templates²⁴**
- **Learn - Deploy Azure infrastructure by using ARM templates²⁵**
- **Learn - Deploy to multiple Azure environments by using ARM template features²⁶**
- **Learn - Extend ARM templates by using deployment scripts²⁷**

²³ <https://azure.microsoft.com/resources/templates/>

²⁴ <https://docs.microsoft.com/learn/modules/build-azure-vm-templates/>

²⁵ <https://docs.microsoft.com/learn/modules/create-azure-resource-manager-template-vs-code/>

²⁶ <https://docs.microsoft.com/learn/modules/extend-resource-manager-template-deployment-scripts/>

²⁷ <https://docs.microsoft.com/learn/modules/extend-resource-manager-template-deployment-scripts/>

Module 03 Lab

Lab 03a - Manage Azure Resources using the Portal

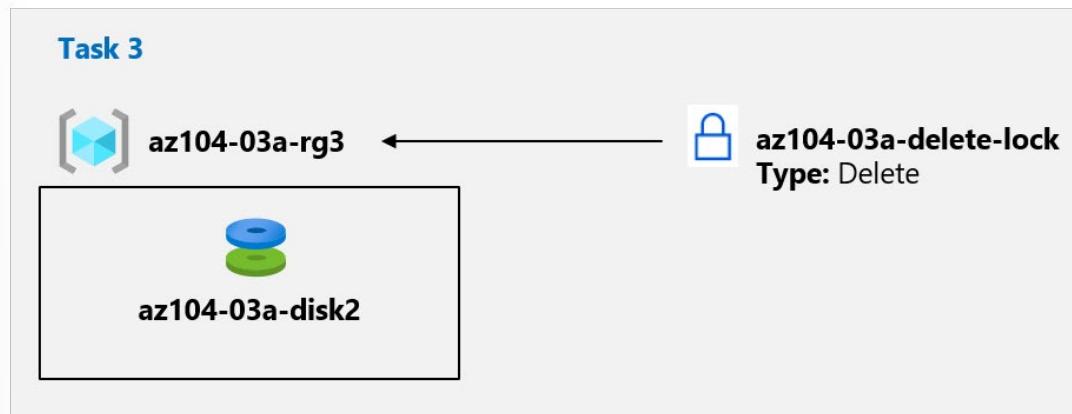
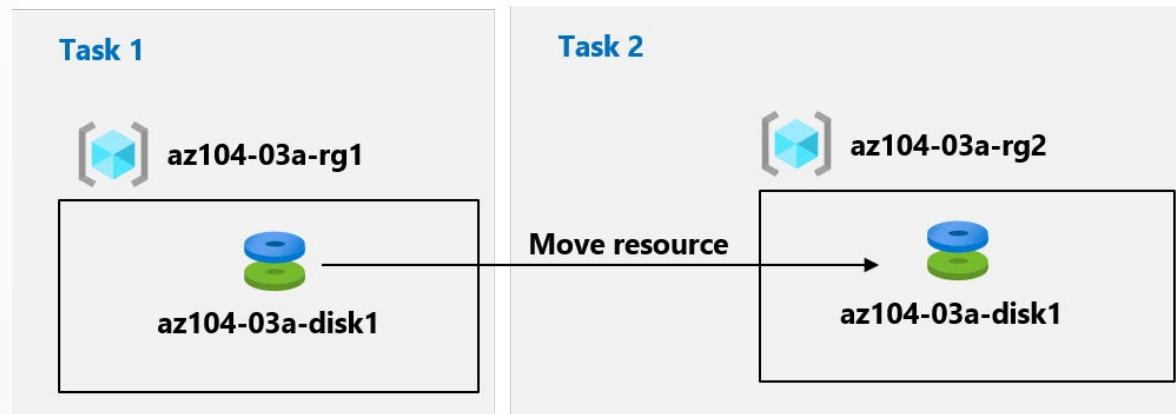
Lab scenario

You need to explore the basic Azure administration capabilities associated with provisioning resources and organizing them based on resource groups, including moving resources between resource groups. You also want to explore options for protecting disk resources from being accidentally deleted, while still allowing for modifying their performance characteristics and size.

Objectives

In this lab, we will:

- Task 1: Create resource groups and deploy resources to resource groups.
- Task 2: Move resources between resource groups.
- Task 3: Implement and test resource locks.



Note: Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Lab 03b - Manage Azure Resources using ARM templates

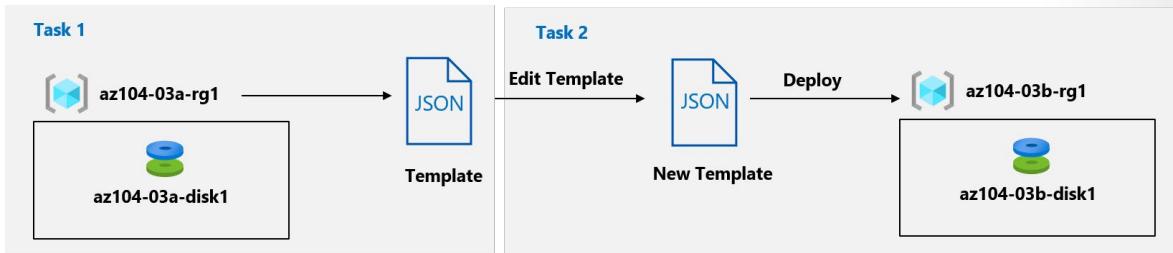
Lab scenario

Now that you explored the basic Azure administration capabilities associated with provisioning resources and organizing them based on resource groups by using the Azure portal, you need to carry out the equivalent task by using Azure Resource Manager templates.

Objectives

In this lab, you will:

- Task 1: Review an ARM template for deployment of an Azure managed disk.
- Task 2: Create an Azure managed disk by using an ARM template.
- Task 3: Review the ARM template-based deployment of the managed disk.



Note: Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Lab 03c - Manage Azure Resources using PowerShell

Lab scenario

Now that you explored the basic Azure administration capabilities associated with provisioning resources and organizing them based on resource groups by using the Azure portal and Azure Resource Manager templates, you need to carry out the equivalent task by using Azure PowerShell. To avoid installing Azure PowerShell modules, you will leverage PowerShell environment available in Azure Cloud Shell.

Objectives

In this lab, you will:

- Task 1: Start a PowerShell session in Azure Cloud Shell.

- Task 2: Create a resource group and an Azure managed disk by using Azure PowerShell.
- Task 3: Configure the managed disk by using Azure PowerShell.

Task 1, Task 2, Task 3



az104-03c-disk1

Note: Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Lab 03d - Manage Azure Resources using the CLI

Lab scenario

Now that you explored the basic Azure administration capabilities associated with provisioning resources and organizing them based on resource groups by using the Azure portal, Azure Resource Manager templates, and Azure PowerShell, you need to carry out the equivalent task by using Azure CLI. To avoid installing Azure CLI, you will leverage Bash environment available in Azure Cloud Shell.

Objectives

In this lab, you will:

- Task 1: Start a Bash session in Azure Cloud Shell.
- Task 2: Create a resource group and an Azure managed disk by using Azure CLI.
- Task 3: Configure the managed disk by using Azure CLI.

Task 1, Task 2, Task 3**az104-03d-rg1****az104-03d-disk1**

Note: Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Answers

Multiple choice

Which of the following is not true about the Cloud Shell?

- Authenticates automatically for instant access to your resources.
- Cloud Shell is assigned multiple machines per user account.
- Provides both Bash and PowerShell sessions.

Explanation

Cloud Shell is assigned multiple machines per user account, is not true. The cloud shell is assigned one machine per user account.

Multiple choice

You are managing Azure locally using PowerShell. You have launched the app as an Administrator. Which of the following commands would you do first?

- Connect-AzAccount
- Get-AzResourceGroup
- Get-AzSubscription

Explanation

Connect-AzAccount. When you are working locally you are not automatically logged in to Azure. So, the first thing you should do is to connect to Azure and provide your credentials.

Multiple choice

What do you need to install on your machine so you can execute Azure CLI commands locally? Select one.

- The Azure cloud shell
- The Azure CLI and Azure PowerShell
- Only the Azure CLI

Explanation

Only the Azure CLI. You only need to install the Azure CLI. You will use a shell to issue the CLI commands, but every platform has at least one built-in shell.

Multiple choice

Which parameter can you add to most CLI commands to get concise, formatted output? Select one.

- list
- table
- group

Explanation

Table. The table parameter formats the output as a table. This can make things much more readable for commands that produce a large amount of output.

Multiple choice

What needs to be installed on your machine to let you execute Azure PowerShell cmdlets locally? Select one.

- The Azure cloud shell
- The Azure CLI and Azure PowerShell
- The base PowerShell product and the AZ module

Explanation

The base PowerShell product and the Az module. You need both the base PowerShell product and the Az module. The base product gives you the shell itself, a few core commands, and programming constructs like loops, variables, etc. The Az modules adds the cmdlets you need to work with Azure resources.

Multiple choice

Suppose you are building a video-editing application that will offer online storage for user-generated video content. You will store the videos in Azure Blobs, so you need to create an Azure storage account to contain the blobs. Once the storage account is in place, it is unlikely you would remove and recreate it because this would delete all the user videos. Which tool is likely to offer the quickest and easiest way to create the storage account? Select one.

- Azure portal
- Azure CLI
- Azure PowerShell

Explanation

Azure portal. The portal is a good choice for one-off operations like creating a long-lived storage account. The portal gives you a GUI containing all the storage-account properties and provides tool tips to help you select the right options for your needs.

Multiple choice

You have a new Azure subscription and need to move resources to that subscription. Which of the following resources cannot be moved? Select one.

- Key vault
- Storage account
- Tenant

Explanation

Tenant. A tenant cannot be moved between subscriptions.

Multiple choice

You are reviewing your virtual machine usage. You notice that you have reached the limit for virtual machines in the US East region. Which of the following provides the easiest solution? Select one.

- Add another resource group
- Change your subscription plan
- Request support increase your limit

Explanation

Request support increase your limit. If you need to increase a default limit, there is a Request Increase link. You will complete and submit the support request.

Multiple choice

Which of the following would be good example of when to use a resource lock? Select one.

- A ExpressRoute circuit with connectivity back to your on-premises network.
- A non-production virtual machine used to test occasional application builds.
- A storage account used to temporarily store images processed in a development environment.

Explanation

An ExpressRoute circuit with connectivity back to your on-premises network. Resource locks prevent other users in your organization from accidentally deleting or modifying critical resources.

Multiple choice

Your manager asks you to explain how Azure uses resource groups. You provide all of the following information, except? Select one.

- Resources can be in only one resource group.
- Resources can be moved from one resource group to another resource group.
- Resource groups can be nested.

Explanation

Resource groups cannot be nested. You should carefully plan your resource group deployments.

Multiple choice

Which of the following is not an element in the template schema? Select one.

- Functions
- Inputs
- Outputs

Explanation

Inputs. Inputs is not a part of the template schema. The elements of an Azure Resource Manager template are schema, contentVersion, apiProfile, parameters, variables, functions, resources, and output.

Multiple choice

Which of the following best describes the format of an Azure Resource Manager template? Select one.

- A JSON document with key-value pairs
- A TXT document with key-value pairs
- An XML document with element-value pairs

Explanation

A JSON document with key-value pairs. An Azure Resource Template is a JSON document with key-value pairs.

Multiple choice

Azure Resource Manager templates are idempotent. This means that if you run a template with no changes a second time ... Select one.

- Azure Resource Manager will deploy new resources as copies of the previously deployed resources.
- Azure Resource Manager won't make any changes to the deployed resources.
- Azure Resource Manager will delete the previously deployed resources and redeploy them.

Explanation

Azure Resource Manager won't make any changes to the deployed resources. If the resource already exists and no change is detected in the properties, no action is taken. If the resource already exists and a property has changed, the resource is updated. If the resource doesn't exist, it's created.

Module 4 Administer Virtual Networking

Configure Virtual Networks

Introduction

Scenario

Your company is migrating to Azure. They want to replicate their on-premises network in the cloud. Azure resources must be organized into virtual networks and subnets. Your company requires an Azure IP addressing schema. The schema should provide flexibility, room for growth, and integration with on-premises networks. The schema should also minimize public exposure of systems, and give the organization flexibility in its network design. If not properly designed, systems might not be able to communicate, and additional work will be required to remediate.

You need to configure the necessary virtual networks and subnets, including IP addressing.

Skills measured

Virtual network and subnets are part of **Exam AZ-104: Microsoft Azure Administrator¹**.

Configure and manage virtual networking (25–30%)

Implement and manage virtual networking

- Create and configure virtual networks.
- Implement subnets.
- Configure private and public IP addresses.

¹ <https://docs.microsoft.com/learn/certifications/exams/az-104>

Learning objectives

In this module, you will learn how to:

- Describe virtual network features and components.
- Identify features and usage cases for subnets and subnetting.
- Identify usage cases for private and public IP addresses.
- Create and determine which resources require public IP addresses.
- Create and determine which resources require private IP addresses.
- Create virtual networks.

Prerequisites

- Familiarity with IP address formats and subnetting.

Plan Virtual Networks

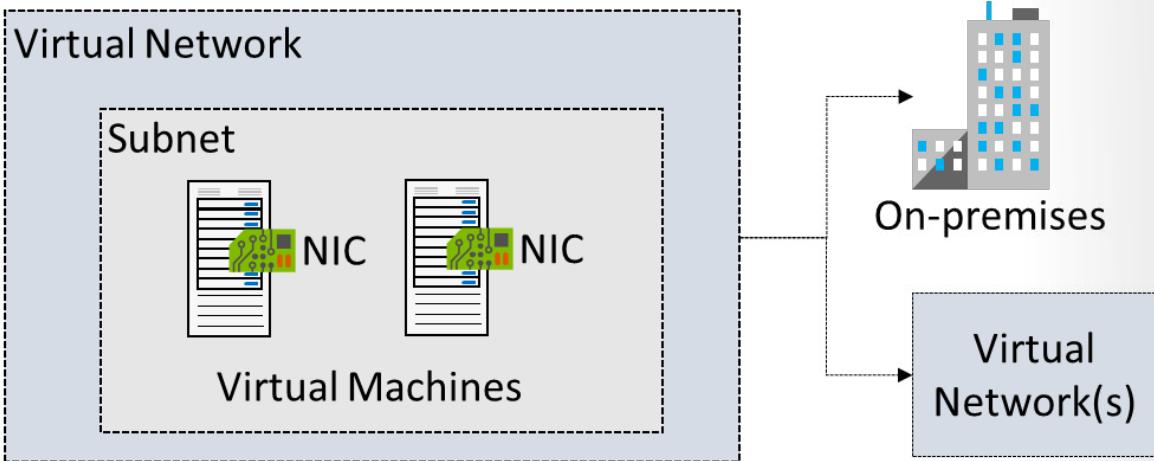
A major incentive for adopting cloud solutions such as Azure is to enable information technology departments to move server resources to the cloud. Moving resources can save money and simplify administrative operations. Moving resources removes the need to maintain expensive datacenters with uninterruptible power supplies, generators, multiple fail-safes, or clustered database servers. For small and medium-sized companies, which might not have the expertise to maintain their own robust infrastructure, moving to the cloud is particularly appealing.

Once the resources are moved to Azure, they require the same networking functionality as an on-premises deployment, and in specific scenarios require some level of network isolation. Azure networking components offer a range of functionalities and services.

 Virtual Network Microsoft Create a logically isolated section in Microsoft Azure and securely connect it outward. 	 Load Balancer Microsoft A load balancer that distributes incoming traffic among backend virtual machine instances. 	 Application Gateway Microsoft Scalable layer-7 load balancer offering various traffic routing rules and SSL termination for backend 
 Traffic Manager profile Microsoft Create a Microsoft Azure Traffic Manager Profile that allows you to control the distribution of user 	 Virtual network gateway Microsoft The VPN device in your Azure virtual network and used with site-to-site and VNet-to-VNet VPN 	 Virtual WAN Microsoft Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch 

Implementation

An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. You can use VNets to provision and manage virtual private networks (VPNs) in Azure and, optionally, link the VNets with other VNets in Azure, or with your on-premises IT infrastructure to create hybrid or cross-premises solutions. Each VNet you create has its own CIDR block and can be linked to other VNets and on-premises networks if the CIDR blocks do not overlap. You also have control of DNS server settings for VNets, and segmentation of the VNet into subnets.



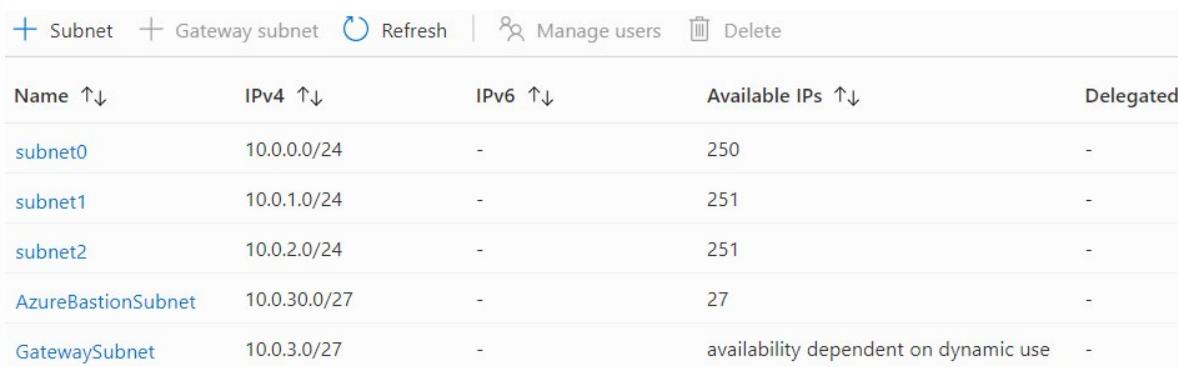
Virtual networks can be used in many ways.

- **Create a dedicated private cloud-only VNet.** Sometimes you don't require a cross-premises configuration for your solution. When you create a VNet, your services and VMs within your VNet can communicate directly and securely with each other in the cloud. You can still configure endpoint connections for the VMs and services that require internet communication, as part of your solution.
- **Securely extend your data center With VNets.** You can build traditional site-to-site (S2S) VPNs to securely scale your datacenter capacity. S2S VPNs use IPSEC to provide a secure connection between your corporate VPN gateway and Azure.
- **Enable hybrid cloud scenarios.** VNets give you the flexibility to support a range of hybrid cloud scenarios. You can securely connect cloud-based applications to any type of on-premises system such as mainframes and Unix systems.

Create Subnets

A virtual network can be segmented into one or more subnets. Subnets provide logical divisions within your network. Subnets can help improve security, increase performance, and make it easier to manage the network.

Each subnet contains a range of IP addresses that fall within the virtual network address space. The range must be unique within the address space for the virtual network. The range can't overlap with other subnet address ranges within the virtual network. The address space must be specified by using Classless Inter-Domain Routing (CIDR) notation.



The screenshot shows a table of subnets within a virtual network. The columns are: Name, IPv4, IPv6, Available IPs, and Delegated. The subnets listed are: subnet0 (10.0.0.0/24), subnet1 (10.0.1.0/24), subnet2 (10.0.2.0/24), AzureBastionSubnet (10.0.30.0/27), and GatewaySubnet (10.0.3.0/27). The Available IPs column shows values 250, 251, 251, 27, and availability dependent on dynamic use respectively.

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/27	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

Considerations

- **Service requirements.** Each service directly deployed into virtual network has specific requirements for routing and the types of traffic that must be allowed into and out of subnets. A service may require, or create, their own subnet, so there must be enough unallocated space for them to do so. For example, if you connect a virtual network to an on-premises network using an Azure VPN Gateway, the virtual network must have a dedicated subnet for the gateway.
- **Virtual appliances.** Azure routes network traffic between all subnets in a virtual network, by default. You can override Azure's default routing to prevent Azure routing between subnets, or to route traffic between subnets through a network virtual appliance. So, if you require that traffic between resources in the same virtual network flow through a network virtual appliance (NVA), deploy the resources to different subnets.
- **Service endpoints.** You can limit access to Azure resources such as an Azure storage account or Azure SQL database, to specific subnets with a virtual network service endpoint. Further, you can deny access to the resources from the internet. You may create multiple subnets, and enable a service endpoint for some subnets, but not others.
- **Network security groups.** You can associate zero or one network security group to each subnet in a virtual network. You can associate the same, or a different, network security group to each subnet. Each network security group contains rules, which allow or deny traffic to and from sources and destinations.

Note: There are no restrictions on using IP addresses. Azure reserves five IP addresses within each subnet.

- x.x.x.0: Network address
- x.x.x.1: Reserved by Azure for the default gateway
- x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space
- x.x.x.255: Network broadcast address

Create Virtual Networks

You can create new virtual networks at any time. You can also add virtual networks when you create a virtual machine. Either way you will need to define the address space, and at least one subnet. By default, you can create up to 50 virtual networks per subscription per region. You can increase this limit to 500 by contacting Azure support.

Note: Default limits on Azure networking resources can change periodically so it's a good idea to consult the documentation for the latest information.

Create virtual network

[Basics](#) IP Addresses Security Tags Review + create

Project details

Subscription * [Visual Studio Enterprise](#) ▾
Resource group * [Lab04](#) ▾ [Create new](#)

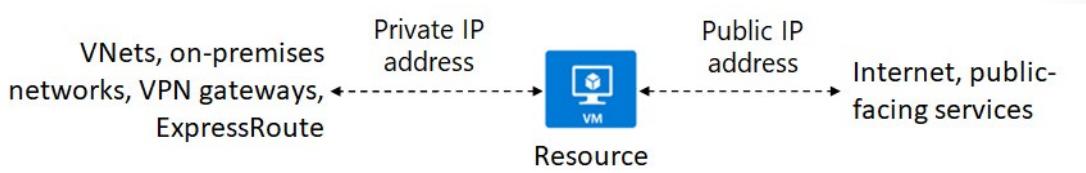
Instance details

Name * [VNet2](#) ✓
Region * [\(US\) East US 2](#) ▾

Note: Plan to use an address space that is not already in use in your organization, either on-premises or in the cloud. Even if you plan for cloud-only virtual networks, you may later decide to connect an on-premises site.

Plan IP Addressing

You can assign IP addresses to Azure resources to communicate with other Azure resources, your on-premises network, and the Internet. There are two types of Azure IP addresses: public and private IP addresses.



- Private IP addresses:** Used for communication within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure.
- Public IP addresses:** Used for communication with the Internet, including Azure public-facing services.

Note: IP Addresses are never managed from within a virtual machine.

Static vs Dynamic addressing

IP addresses can also be statically assigned or dynamically assigned. Static IP addresses do not change and are best for certain situations such as:

- DNS name resolution, where a change in the IP address would require updating host records.
- IP address-based security models that require apps or services to have a static IP address.
- TSL/SSL certificates linked to an IP address.
- Firewall rules that allow or deny traffic using IP address ranges.
- Role-based VMs such as Domain Controllers and DNS servers.

Note: You may decide to separate dynamically and statically assigned IP resources into different subnets.

Create Public IP Addresses

Create public IP address

IP Version * ⓘ
 IPv4 IPv6 Both

SKU * ⓘ
 Basic Standard

IPv4 IP Address Configuration

Name *

IP address assignment *
 Dynamic Static

IP Version. Select IPv4 or IPv6 or Both. Selecting Both will result in two Public IP addresses being created—one IPv4 address and one IPv6 address.

SKU. You cannot change the SKU after the public IP address is created. A standalone virtual machine, virtual machines within an availability set, or virtual machine scale sets can use Basic or Standard SKUs. Mixing SKUs between virtual machines within availability sets or scale sets or standalone VMs is not allowed.

Name. The name must be unique within the resource group you select.

IP address assignment

- **Dynamic.** Dynamic addresses are assigned only after a public IP address is associated to an Azure resource, and the resource is started for the first time. Dynamic addresses can change if they're assigned to a resource, such as a virtual machine, and the virtual machine is stopped (deallocated), and then restarted. The address remains the same if a virtual machine is rebooted or stopped (but not deallocated). Dynamic addresses are released when a public IP address resource is dissociated from a resource.
- **Static.** Static addresses are assigned when a public IP address is created. Static addresses aren't released until a public IP address resource is deleted. If the address isn't associated to a resource, you can change the assignment method after the address is created. If the address is associated to a resource, you may not be able to change the assignment method. If you select IPv6 for the IP version, the assignment method must be Dynamic for Basic SKU. Standard SKU addresses are Static for both IPv4 and IPv6.

Associate Public IP Addresses

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways.

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	Yes*
Application Gateway	Front-end configuration	Yes	Yes*

- Static IP addresses only available on certain SKUs.

Address SKUs

When you create a public IP address, you are given a SKU choice of either **Basic** or **Standard**. Your SKU choice affects the IP assignment method, security, available resources, and redundancy. This table summarizes the differences.

Feature	Basic SKU	Standard SKU
IP assignment	Static or dynamic	Static
Security	Open by default	Are secure by default and closed to inbound traffic
Resources	Network interfaces, VPN Gateways, Application Gateways, and Internet-facing load balancers	Network interfaces or public standard load balancers
Redundancy	Not zone redundant	Zone redundant by default

Associate Private IP Addresses

A private IP address resource can be associated with virtual machine network interfaces, internal load balancers, and application gateways. Azure can provide an IP address (dynamic assignment) or you can assign the IP address (static assignment).

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

A private IP address is allocated from the address range of the virtual network subnet a resource is deployed in.

- **Dynamic.** Azure assigns the next available unassigned or unreserved IP address in the subnet's address range. For example, Azure assigns 10.0.0.10 to a new resource, if addresses 10.0.0.4-10.0.0.9 are already assigned to other resources. Dynamic is the default allocation method.
- **Static.** You select and assign any unassigned or unreserved IP address in the subnet's address range. For example, if a subnet's address range is 10.0.0.0/16 and addresses 10.0.0.4-10.0.0.9 are already assigned to other resources, you can assign any address between 10.0.0.10 - 10.0.255.254.

Demonstration - Create Virtual Networks

In this demonstration, you will create virtual networks.

Note: You can use the suggested values for the settings, or your own custom values if you prefer.

Create a virtual network in the portal

1. Sign in to the Azure portal and search for **Virtual Networks**.
2. On the Virtual Networks page, click **Add**.
 - **Name:** myVNet1.
 - **Address:** 10.1.0.0/16.
 - **Subscription:** Select your subscription.

- **Resource group:** Select new or choose an existing resource group
 - **Location** - Select your location
 - **Subnet** - Enter *mySubnet1*.
 - **Subnet - Address range:** *10.1.0.0/24*
3. Leave the rest of the default settings and select **Create**.
 4. Verify your virtual network was created.
- Optional - Create a virtual network using PowerShell**
1. Create a virtual network. Use values as appropriate.
- ```
$myVNet2 = New-AzVirtualNetwork -ResourceGroupName myResourceGroup -Location EastUS -Name myVNet2 -AddressPrefix 10.0.0.0/16
```
2. Verify your new virtual network information.
- ```
Get-AzVirtualNetwork -Name myVNet2
```
3. Create a subnet. Use values as appropriate.
- ```
$mySubnet2 = Add-AzVirtualNetworkSubnetConfig -Name mySubnet2 -AddressPrefix 10.0.0.0/24 -VirtualNetwork $myVNet2
```
4. Verify your new subnet information.
- ```
Get-AzVirtualNetworkSubnetConfig -Name mySubnet2 -VirtualNetwork $myVNet2
```
5. Associate the subnet to the virtual network.
- ```
$mySubnet2 | Set-AzVirtualNetwork
```
6. Return to the portal and verify your new virtual network with subnet was created.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Your company has implemented Firewall rules to deny traffic based on IP address ranges. In this situation, what should you do?*

- Use dynamically assigned IP addresses.
- Use statically assigned IP addresses.
- Use IP addresses in the reserved range.

## Multiple choice

You are planning your Azure network implementation to support your company's migration to Azure. Your first task is to prepare for the deployment of the first set of VMs. For these machines, consumers on the internet must be able to communicate directly with the web application on the VMs. Also, the IP configuration must be zone redundant. You should minimize costs, whenever possible, while still meeting the requirements. What should you do? Select one.

- Create a standard public IP address. During the creation of the first VM, associate the public IP address with the VM's NIC.
- Create a standard public IP address. After the first VM is created, remove the private IP address and assign the public IP address to the NIC.
- Create a basic public IP address. During the creation of the first VM, associate the public IP address with the VM.

## Multiple choice

You have a VM with two NICs named NIC1 and NIC2. NIC1 is connected to the 10.10.8.0/24 subnet. NIC2 is connected to the 10.20.8.0/24 subnet. You plan enable direct communication from the internet to TCP port 443. You would like to maintain existing communication across the 10.10.8.0/24 and 10.20.8.0/24 subnets. To support the new functionality and keep things simple. What should you do? Select one.

- Remove the private IP address from NIC2 and then assign a public IP address to it. Then, create an inbound security rule.
- Associate a public IP address to NIC2 and create an inbound security rule.
- Create an inbound security rule for TCP port 443.

## Summary and Resources

### Summary

Azure Virtual Network is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines, to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

Azure IP addressing is critical to ensuring resources are accessible. Private IP addresses to communicate between resources in Azure. Public IP addresses enable Azure resources to be accessible directly from the internet..

You should now be able to:

- Identify features and usage cases for subnets and subnetting.
- Create a virtual network with subnetting.
- Identify usage cases for private and public IP addresses.
- Create and determine which resources require public and private IP addresses.

## Learn more

You can learn more by reviewing the following.

- **Virtual Network Documentation<sup>2</sup>.**
- **Public IP Addresses<sup>3</sup>**
- **Private IP Addresses<sup>4</sup>**
- **Learn - Networking Fundamentals Principals<sup>5</sup>**
- **Learn - Design an IP addressing schema for your Azure deployment<sup>6</sup>**
- **Learn - Implement Windows Server IaaS VM IP addressing and routing<sup>7</sup>**

---

<sup>2</sup> <https://docs.microsoft.com/azure/virtual-network/>

<sup>3</sup> <https://docs.microsoft.com/azure/virtual-network/public-ip-addresses>

<sup>4</sup> <https://docs.microsoft.com/azure/virtual-network/private-ip-addresses>

<sup>5</sup> <https://docs.microsoft.com/learn/modules/network-fundamentals/>

<sup>6</sup> <https://docs.microsoft.com/learn/modules/design-ip-addressing-for-azure/>

<sup>7</sup> <https://docs.microsoft.com/learn/modules/implement-windows-server-iaas-virtual-machine-ip-addressing-routing/>

# Configure Network Security Groups

## Introduction

### Scenario

Your company has several sites, and users throughout the company will need to use an enterprise resource planning (ERP) app to migrate to Azure. The company will only consider moving key systems onto the platform if stringent security requirements can be met, including tight control over which computers have network access to the servers running the app. You want to secure both virtual machine (VM) networking and Azure services networking as part of your company's network security strategy. Your goal is to prevent unwanted or unsecured network traffic from being able to reach key systems.

You need to implement network security groups. You need to implement network security group rules and ensure the rules are correctly applied.

### Skills measured

Network security groups are part of **Exam AZ-104: Microsoft Azure Administrator<sup>8</sup>**.

Configure and manage virtual networking (25–30%)

Secure access to virtual networks

- Create security rules.
- Associate a network security group (NSG) to a subnet or network interface.
- Evaluate effective security rules.

### Learning objectives

In this module, you will learn how to:

- Determine when to use network security groups.
- Implement network security group rules.
- Evaluate network security group effective rules.

### Prerequisites

None

## Implement Network Security Groups

You can limit network traffic to resources in a virtual network using a network security group (NSG). A network security group contains a list of security rules that allow or deny inbound or outbound network traffic. An NSG can be associated to a subnet or a network interface. A network security group can be associated multiple times.

<sup>8</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

## Subnets

You can assign NSGs to subnets and create protected screened subnets (also called a DMZ). These NSGs can restrict traffic flow to all the machines that reside within that subnet. Each subnet can have zero, or one, associated network security groups.

## Network Interfaces

You can assign NSGs to a NIC so that all the traffic that flows through that NIC is controlled by NSG rules. Each network interface that exists in a subnet can have zero, or one, associated network security groups.

## Associations

When you create an NSG the Overview blade provides information about the NSG such as, associated subnets, associated network interfaces, and security rules.

nsg0  
Network security group | Directory: Microsoft

Search (Ctrl+ /) | Move | Delete | Refresh

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

Resource group (change) : rg01 | Custom security rules : 1 inbound, 0 outbound  
Location : East US | Associated with : 1 subnets, 0 network interfaces  
Subscription (change) :  
Subscription ID :  
Tags (change) : Click here to add tags

## Determine NSG Rules

Security rules in network security groups enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces. Azure creates several default security rules within each network security group.

You can add more rules by specifying:

- Name
- Priority
- Port
- Protocol (Any, TCP, UDP)
- Source (Any, IP Addresses, Service tag)
- Destination (Any, IP Addresses, Virtual Network)
- Action (Allow or Deny).

Azure creates the default rules in each network security group that you create. You cannot remove the default rules, but you can override them by creating rules with higher priorities.

## Inbound rules

There are three default inbound security rules. The rules deny all inbound traffic except from the virtual network and Azure load balancers.

| VM1-nsg - Inbound security rules |                               |      |          |                   |                |                                          |
|----------------------------------|-------------------------------|------|----------|-------------------|----------------|------------------------------------------|
| PRIORITY                         | NAME                          | PORT | PROTOCOL | SOURCE            | DESTINATION    | ACTION                                   |
| 65000                            | AllowVnetInBound              | Any  | Any      | VirtualNetwork    | VirtualNetwork | <span style="color: green;">Allow</span> |
| 65001                            | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer | Any            | <span style="color: green;">Allow</span> |
| 65500                            | DenyAllInBound                | Any  | Any      | Any               | Any            | <span style="color: red;">Deny</span>    |

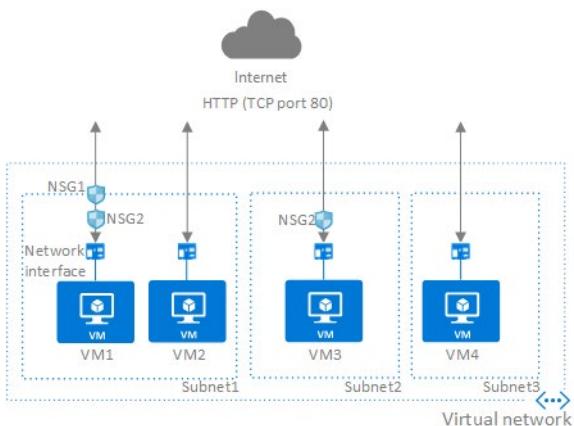
## Outbound rules

There are three default outbound security rules. The rules only allow outbound traffic to the Internet and the virtual network.

| VM1-nsg - Outbound security rules |                       |      |          |                |                |                                          |
|-----------------------------------|-----------------------|------|----------|----------------|----------------|------------------------------------------|
| PRIORITY                          | NAME                  | PORT | PROTOCOL | SOURCE         | DESTINATION    | ACTION                                   |
| 65000                             | AllowVnetOutBound     | Any  | Any      | VirtualNetwork | VirtualNetwork | <span style="color: green;">Allow</span> |
| 65001                             | AllowInternetOutBound | Any  | Any      | Any            | Internet       | <span style="color: green;">Allow</span> |
| 65500                             | DenyAllOutBound       | Any  | Any      | Any            | Any            | <span style="color: red;">Deny</span>    |

## Determine NSG Effective Rules

NSGs are evaluated independently, and an “allow” rule must exist at both levels otherwise traffic will not be allowed.



In the above example, if there was incoming traffic on port 80, you would need to have the NSG at the subnet level ALLOW port 80. You would also need another NSG with an ALLOW rule on port 80 at the NIC level.

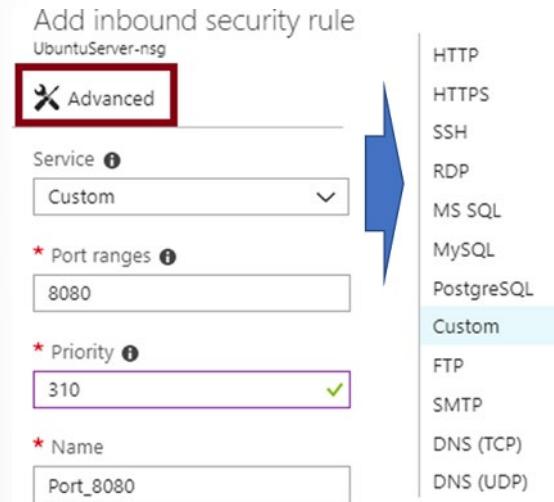
For incoming traffic, the NSG set at the subnet level is evaluated first, then the NSG set at the NIC level is evaluated. For outgoing traffic, it is the reverse.

If you have several NSGs and are not sure which security rules are being applied, you can use the **Effective security rules** link. For example, you could verify the security rules being applied to a network interface.



## Create NSG Rules

It is easy to add inbound and outbound rules. There is a Basic and Advanced page. The Advanced page lets you select from a large variety of services. These services include HTTPS, RDP, FTP, and DNS.



**Service.** Service specifies the destination protocol and port range for this rule. You can choose a pre-defined service, like HTTPS and SSH. When you select a service, the Port range is automatically completed. Choose custom to provide your own port range.

**Port ranges.** Port ranges can include a single port, a port range, or a comma-separated list of ports. The ports designate the traffic will be allowed or denied by this rule. Provide an asterisk (\*) to allow traffic on any port.

**Priority.** Rules are processed in priority order. The lower the number, the higher the priority. We recommend leaving gaps between rules to make it easier to add new rules. The value is between 100-4096 and unique for all security rules within the network security group.

**Note:** Will you need to create rules? Which services will you need to control the network traffic?

## Demonstration - NSGs

In this demonstration, you will explore NSGs and service endpoints.

### Access the NSGs blade

1. Access the Azure Portal.
2. Search for and access the **Network Security Groups** blade.
3. If you have virtual machines, you may already have NSGs. Notice the ability to filter the list.

### Add a new NSG

1. + **Add** a network security group.
  - **Name:** *select a unique name*
  - **Subscription:** *select your subscription*
  - **Resource Group:** *create new or select an existing resource group*
  - **Location:** *your choice*
  - Click **Create**

2. Wait for the new NSG to deploy.

### Explore inbound and outbound rules

1. Select your new NSG.
2. Notice the NSG can be associated with subnets and network interfaces (summary information above the rules).
3. Notice the three inbound and three outbound NSG rules.
4. Under **Settings** select **Inbound security rules**.
5. Notice you can use **Default rules** to hide the default rules.
6. + **Add** a new inbound security rule.
7. Click **Basic** to change to the Advanced mode.
8. Use the **Service** drop-down to review the predefined services that are available.
9. When you make a service selection (like HTTPS) the port range (like 443) is automatically populated. This makes it easy to configure the rule.
10. Use the Information icon next to the Priority label to learn how to configure the priority.
11. Exit the rule without making any changes.
12. As you have time, review adding an outbound security rule.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Your company has two NSG security rules for inbound traffic to your web servers. There is an allow rule with a priority of 200. And, there is a deny rule with a priority of 150. Which rule takes precedence? Select one.*

- The allow rule takes precedence
- The deny rule takes precedence
- The rule that was created first takes precedence.

## Multiple choice

*Which of the following is a default inbound security rule? Select one.*

- Allow inbound coming from any VM to any other VM within the subnet.
- Allow inbound coming from any VM to any other VM within the virtual network.
- Allow traffic from any external source to any of the VMs.

## Multiple choice

*Your company wants to simplify network security group rules by using service tags. Which of the following is a valid service tag? Select one.*

- VirtualNetwork
- VPNGateway
- Database

## Summary and Resources

### Summary

Isolating and securing network resources in Azure is an important job skill. Network security groups secure virtual networks by creating rules to control network traffic.

You should now be able to:

- Determine when to use network security groups.
- Implement network security group rules.
- Evaluate network security group effective rules.

### Learn more

You can learn more by reviewing the following.

- **Network Security Groups documentation<sup>9</sup>.**
- **Learn - Secure and isolate access to Azure resources by using network security groups and service endpoints<sup>10</sup>**

---

<sup>9</sup> <https://docs.microsoft.com/azure/virtual-network/security-overview>

<sup>10</sup> <https://docs.microsoft.com/learn/modules/secure-and-isolate-with-nsg-and-service-endpoints/>

# Configure Azure Firewall

## Introduction

### Scenario

Your company is spread across multiple Azure regions. The networking infrastructure includes multiple virtual networks and connections to an on-premises network. The IT staff is concerned about malicious actors trying to infiltrate the network.

You need to implement Azure Firewall. You need to configure Azure Firewall to deny incoming and outgoing threats while also allowing legitimate traffic.

### Skills measured

Implementing Azure Firewall is part of **Exam AZ-104: Microsoft Azure Administrator<sup>11</sup>**.

Configure and manage virtual networking (25–30%)

Secure access to virtual networks

- Implement Azure Firewall.

### Learning objectives

In this module, you will learn how to:

- Determine when to use Azure Firewall.
- Implement Azure Firewall including firewall rules.

### Prerequisites

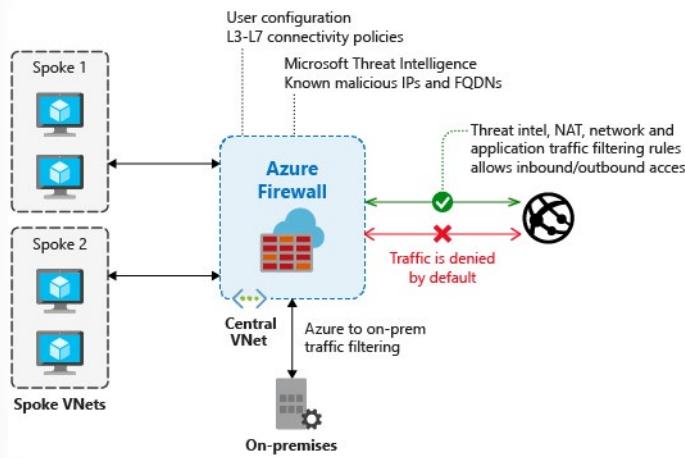
None

## Determine Azure Firewall Uses

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

<sup>11</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>



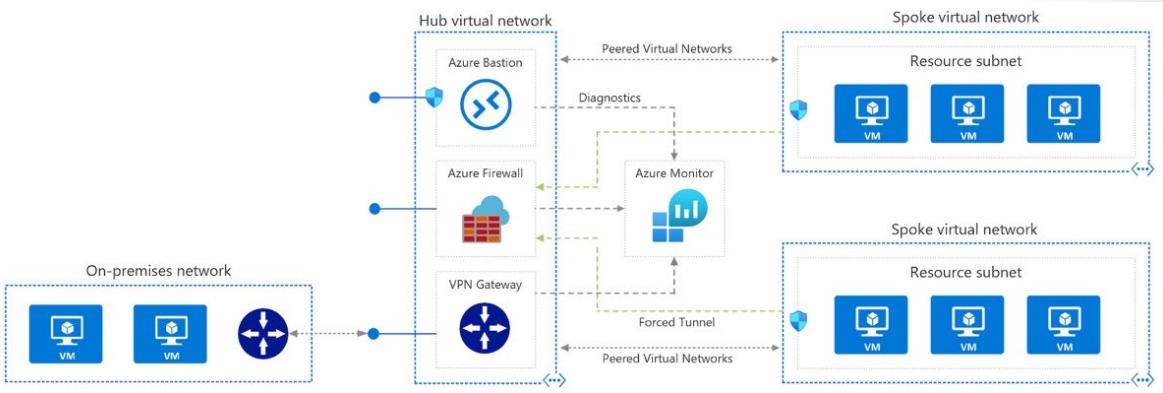
## Azure Firewall features

- **Built-in high availability.** High availability is built in, so additional load balancers aren't required. There's nothing you need to configure.
- **Availability Zones.** Azure Firewall can be configured during deployment to span multiple Availability Zones for increased availability.
- **Unrestricted cloud scalability.** Azure Firewall can scale up as much as you need to accommodate changing network traffic flows, so you don't need to budget for your peak traffic.
- **Application FQDN filtering rules.** You can limit outbound HTTP/S traffic or Azure SQL traffic to a specified list of fully qualified domain names (FQDN) including wild cards.
- **Network traffic filtering rules.** You can centrally create allow or deny network filtering rules by source and destination IP address, port, and protocol. Azure Firewall is fully stateful, so it can distinguish legitimate packets for different types of connections. Rules are enforced and logged across multiple subscriptions and virtual networks.
- **Threat intelligence.** Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains. The IP addresses and domains are sourced from the Microsoft Threat Intelligence feed.
- **Multiple public IP addresses.** You can associate multiple public IP addresses (up to 100) with your firewall.

## Create Azure Firewalls

It's recommended to use a hub-spoke network topology when deploying a firewall.

- The *hub* is a virtual network in Azure that acts as a central point of connectivity to your on-premises network.
- The *spokes* are virtual networks that peer with the hub, and can be used to isolate workloads.
- Traffic flows between the on-premises datacenter and the hub through an ExpressRoute or VPN gateway connection.



The benefits of this topology include:

- Cost savings by centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs) and DNS servers, in a single location.
- Overcome subscriptions limits by peering virtual networks from different subscriptions to the central hub.
- Separation of concerns between central IT (SecOps, InfraOps) and workloads (DevOps).

Typical uses for a hub-spoke network architecture include:

- Workloads in different environments that require shared services. For example, development and testing environments that require DNS. Shared services are placed in the hub virtual network. Each environment is deployed to a spoke to maintain isolation.
- Workloads that don't require connectivity to each other, but require access to shared services.
- Enterprises that require central control over security aspects. For example, a firewall in the hub and workloads in each spoke.

## Create Azure Firewall Rules

There are three kinds of rules that you can configure in the Azure Firewall. Remember, by default, Azure Firewall blocks all traffic, unless you enable it.

| Settings                                                                           | NAT rule collection               | Network rule collection | Application rule collection |
|------------------------------------------------------------------------------------|-----------------------------------|-------------------------|-----------------------------|
| <input type="checkbox"/> Rules<br><input type="checkbox"/> Public IP configuration |                                   |                         |                             |
|                                                                                    | + Add application rule collection |                         |                             |

## NAT Rules

You can configure Azure Firewall Destination Network Address Translation (DNAT) to translate and filter inbound traffic to your subnets. Each rule in the NAT rule collection is used to translate your firewall public IP and port to a private IP and port. Scenarios where NAT rules might be helpful are publishing SSH, RDP, or non-HTTP/S applications to the Internet. A NAT rule that routes traffic must be accompanied by a matching network rule to allow the traffic. Configuration settings include:

- **Name:** A label for the rule.
- **Protocol:** TCP or UDP.

- **Source Address:** \* (Internet), a specific Internet address, or a CIDR block.
- **Destination Address:** The external address of the firewall that the rule will inspect.
- **Destination Ports:** The TCP or UDP ports that the rule will listen to on the external IP address of the firewall.
- **Translated Address:** The IP address of the service (virtual machine, internal load balancer, and so on) that privately hosts or presents the service.
- **Translated Port:** The port that the inbound traffic will be routed to by the Azure Firewall.

## Network Rules

Any non-HTTP/S traffic that will be allowed to flow through the firewall must have a network rule. For example, if resources in one subnet must communicate with resources in another subnet, then you would configure a network rule from the source to the destination. Configuration settings include:

- **Name:** A friendly label for the rule.
- **Protocol:** TCP, UDP, ICMP (ping and traceroute) or Any.
- **Source Address:** The address or CIDR block of the source.
- **Destination Addresses:** The addresses or CIDR blocks of the destination(s).
- **Destination Ports:** The destination port of the traffic.

## Application Rules

Application rules define fully qualified domain names (FQDNs) that can be accessed from a subnet. For example, specify the Windows Update network traffic through the firewall. Configuration settings include:

- **Name:** A friendly label for the rule.
- **Source Addresses:** The IP address of the source.
- **Protocol:Port:** HTTP/HTTPS and the port that the web server is listening on.
- **Target FQDNs:** The domain name of the service, such as www.contoso.com. Wildcards can be used. An FQDN tag represents a group of FQDNs associated with well known Microsoft services. Example FQDN tags include Windows Update, App Service Environment, and Azure Backup.

## Rule Processing

When a packet is being inspected to determine if it is allowed or not, the rules are processed in this order:

1. Network Rules
2. Application Rules (network and application)

Once a rule is found that allows the traffic through, no more rules are checked.

## Knowledge check

Choose the best response for each question.

## Multiple choice

You are configuring the Azure Firewall. You need to allow Windows Update network traffic through the firewall. Which of the following should you use? Select one.

- Application rules
- Destination inbound rules
- Network rules

## Multiple choice

Your company wants to allow external users to access an Azure virtual server with a remote desktop connection. Which one of the following items would you implement on Azure Firewall to allow these connections? Select one.

- Service tag
- Source network address translation
- Destination network address translation

## Multiple choice

Your company wants to allow access to an Azure SQL Database instance. Which of the following network rules types should they use to configure Azure Firewall? Select one.

- Application
- Network
- NAT

# Summary and Resources

## Summary

Azure Firewall acts as a barrier between your Azure virtual network and the internet. Azure Firewall examines all inbound and outbound traffic. Azure Firewall uses threat intelligence, rules, and other policy settings to allow legitimate traffic and deny threatening or unknown traffic.

You should now be able to:

- Determine when to use Azure Firewall.
- Implement Azure Firewall including firewall rules.

## Learn more

You can learn more by reviewing the following.

- **Azure Firewall documentation<sup>12</sup>**
- **Learn - Introduction to Azure Firewall<sup>13</sup>**

---

<sup>12</sup> <https://docs.microsoft.com/azure/firewall/>

<sup>13</sup> <https://docs.microsoft.com/learn/modules/introduction-azure-firewall/>

- Learn - Introduction to Azure Firewall Manager<sup>14</sup>

---

<sup>14</sup> <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-firewall-manager/>

# Configure Azure DNS

## Introduction

### Scenario

Azure DNS enables you to host your DNS records for your domains on Azure infrastructure. With Azure DNS, you can use the same credentials, APIs, tools, and billing as your other Azure services.

Your company obtains a custom domain name for a new website. You need to use Azure DNS to manage this domain.

### Skills measured

Configuring Azure DNS is part of **Exam AZ-104: Microsoft Azure Administrator<sup>15</sup>**.

Configure and manage virtual networking (25–30%)

Implement and manage virtual networking

- Configure Azure DNS, including custom DNS settings and private or public DNS zones.

### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for domains, custom domains, and private zones.
- Verify custom domain names using DNS records.
- Implement DNS zones, DNS delegation, and DNS record sets.

### Prerequisites

- Familiarity with DNS including record sets, delegation, and zones.

## Identify Domains and Custom Domains

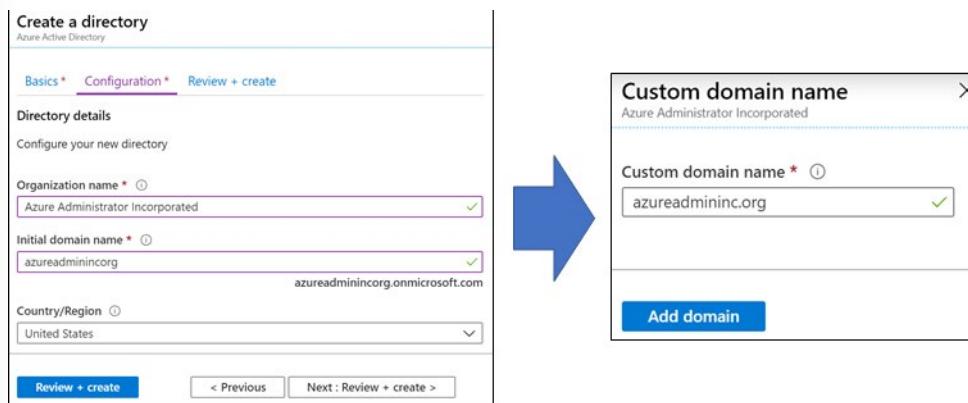
### Initial domain name

When you create an Azure subscription, an Azure AD domain is automatically created. This instance of the domain has an *initial domain name* in the form *domainname.onmicrosoft.com*. The initial domain name is intended to be used until a custom domain name is verified.

### Custom domain name

The initial domain name can't be changed or deleted. You can however add a routable custom domain name you control. A custom domain name simplifies the user sign-on experience. Users can use credentials they are familiar with. For example, a contosogold.onmicrosoft.com, could be assigned to contoso-gold.com.

<sup>15</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>



## Practical information about domain names

- You must be a global administrator to perform domain management tasks. The global administrator is the user who created the subscription.
- Domain names in Azure AD are globally unique. When one Azure AD directory has verified a domain name, other directories can't use that name.
- Before a custom domain name can be used by Azure AD, the custom domain name must be added to your directory and verified.

## Verify Custom Domain Names

When an administrator adds a custom domain name to an Azure AD, it is initially in an unverified state. Azure AD won't allow any directory resources to use an unverified domain name. Only one directory can use a domain name, the organization that owns the domain name.

After adding the custom domain name, you must verify ownership of the domain name. Verification is performed by adding a DNS record. The DNS record can be MX or TXT. Once the DNS record is added, Azure will query the DNS domain for the presence of the record. This could take several minutes or several hours. When Azure verifies the presence of the DNS record, it will then add the domain name to the subscription.

The screenshot shows the Azure portal interface for managing a custom domain. At the top, the domain name "azureadmininc.org" is displayed, along with a "Delete" button and a "Got feedback?" link. A note below the domain name instructs users to create a new TXT record at their domain registrar. The "Record type" is set to "TXT". The "Alias or host name" field contains "@". The "Destination or points to address" field contains "MS=ms79094380". The "TTL" field is set to 3600. A "Share these settings via email" link is present, along with a note that verification will not succeed until the domain is configured at the registrar.

## Create Azure DNS Zones

Azure DNS provides a reliable, secure DNS service to manage and resolve domain names in a virtual network without needing to add a custom DNS solution.

A DNS zone hosts the DNS records for a domain. So, to start hosting your domain in Azure DNS, you need to create a DNS zone for that domain name. Each DNS record for your domain is then created inside this DNS zone.

From the Azure portal, you can easily add a DNS zone. Information for the DNS zone includes name, number of records, resource group, location, subscription, and name servers.

**Create DNS zone**

**Basics** Tags Review + create

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

**Project details**

Subscription \*

Resource group \*    
[Create new](#)

**Instance details**

Name \*

Resource group location

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

## Considerations

- The name of the zone must be unique within the resource group, and the zone must not exist already.
- The same zone name can be reused in a different resource group or a different Azure subscription.
- Where multiple zones share the same name, each instance is assigned different name server addresses.
- Root/Parent domain is registered at the registrar and pointed to Azure NS.
- Child domains are registered in AzureDNS directly.

**Note:** You do not have to own a domain name to create a DNS zone with that domain name in Azure DNS. However, you do need to own the domain to configure the domain.

## Delegate DNS Domains

To delegate your domain to Azure DNS, you first need to know the name server names for your zone. Each time a DNS zone is created Azure DNS allocates name servers from a pool. Once the Name Servers are assigned, Azure DNS automatically creates authoritative NS records in your zone.

**Note:** When you copy each name server address, make sure you copy the trailing period at the end of the address. The trailing period indicates the end of a fully qualified domain name. Some registrars append the period if the NS name doesn't have it at the end. To be compliant with the DNS RFC, include the trailing period.

The easiest way to locate the name servers assigned to your zone is through the Azure portal. In this example, the zone 'contoso.net' has been assigned four name servers: 'ns1-01.azure-dns.com', 'ns2-01.azure-dns.net', 'ns3-01.azure-dns.org', and 'ns4-01.azure-dns.info':

A screenshot of the Azure portal showing the 'azureadmininc.org' DNS zone. The interface includes a 'DNS' icon, the zone name 'azureadmininc.org', and a 'DNS zone' label. Below these are buttons for 'Record set', 'Move', 'Delete zone', and 'Refresh'. The main content area displays resource details and assigned name servers:

|                                           |                                             |                                         |
|-------------------------------------------|---------------------------------------------|-----------------------------------------|
| Resource group ( <a href="#">change</a> ) | rg-dns                                      | Name server 1<br>ns1-01.azure-dns.com.  |
| Subscription ( <a href="#">change</a> )   | <a href="#">MSDN Platforms Subscription</a> | Name server 2<br>ns2-01.azure-dns.net.  |
| Subscription ID                           |                                             | Name server 3<br>ns3-01.azure-dns.org.  |
| Tags ( <a href="#">change</a> )           |                                             | Name server 4<br>ns4-01.azure-dns.info. |
| <a href="#">Click here to add tags</a>    |                                             |                                         |

Once the DNS zone is created, and you have the name servers, you need to update the parent domain. Each registrar has their own DNS management tools to change the name server records for a domain. In the registrar's DNS management page, edit the NS records and replace the NS records with the ones Azure DNS created.

**Note:** When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS. You should always use all four name server names, regardless of the name of your domain.

## Child Domains

If you want to set up a separate child zone, you can delegate a subdomain in Azure DNS. For example, after configuring contoso.com in Azure DNS, you could configure a separate child zone for partners. contoso.com.

Setting up a subdomain follows the same process as typical delegation. The only difference is that NS records must be created in the parent zone contoso.com in Azure DNS, rather than in the domain registrar.

**Note:** The parent and child zones can be in the same or different resource group. Notice that the record set name in the parent zone matches the child zone name, in this case *partners*.

## Add DNS Record Sets

It's important to understand the difference between DNS record sets and individual DNS records. A record set is a collection of records in a zone that have the same name and are the same type.



Resource group (change) : rgtest  
Subscription (change) : Azure Pass - Sponsorship  
Subscription ID :  
Tags (change) : Click here to add tags

A record set cannot contain two identical records. Empty record sets (with zero records) can be created, but do not appear on the Azure DNS name servers. Record sets of type CNAME can contain one record at most.

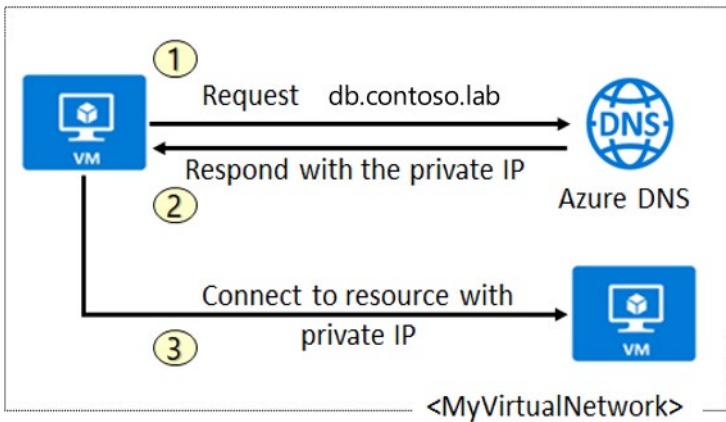
The **Add record set** page will change depending on the type of record you select. For an A record, you will need the TTL (Time to Live) and IP address. The time to live, or TTL, specifies how long each record is cached by clients before being requeried.

The screenshot shows the 'Add record set' dialog box. At the top, it says 'Add record set' and 'azureadmininc.org'. There is a close button 'X' in the top right corner. The form fields are as follows:

- Name:** A text input field containing 'helloworld' with a green checkmark icon to its right.
- Type:** A dropdown menu currently set to 'A'.
- Alias record set:** A section with a help icon (i) and two radio buttons: 'Yes' (unselected) and 'No' (selected).
- TTL \***: An input field containing '1'.
- TTL unit:** A dropdown menu currently set to 'Hours'.
- IP address:** An input field containing '0.0.0.0' with a three-dot ellipsis button to its right.

## Plan for Private DNS Zones

When using private DNS zones, you can use your own custom domain names rather than the Azure-provided names. Using custom domain names helps you to tailor your virtual network architecture to best suit your organization's needs. It provides name resolution for virtual machines (VMs) within a virtual network and between virtual networks. Additionally, you can configure zones names with a split-horizon view, which allows a private and a public DNS zone to share the name.



The DNS records for the private zone are not viewable or retrievable. But, the DNS records are registered and will resolve successfully.

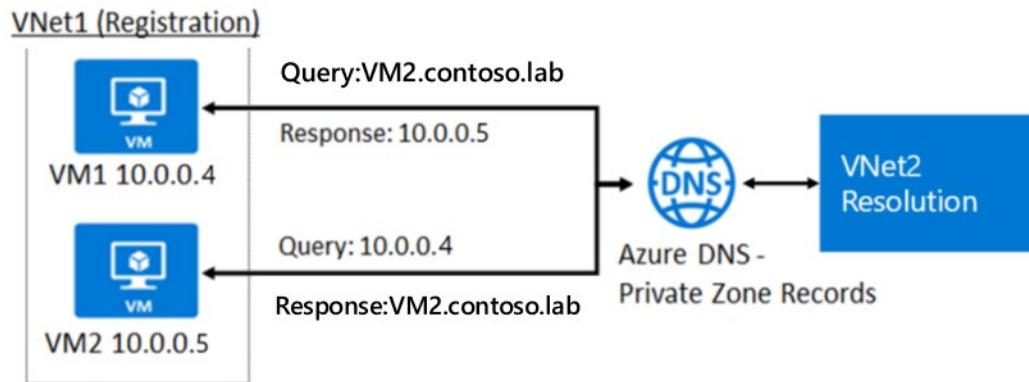
## Azure Private DNS benefits

- **Removes the need for custom DNS solutions.** Previously, many customers created custom DNS solutions to manage DNS zones in their virtual network. You can now perform DNS zone management by using the native Azure infrastructure. This removes the burden of creating and managing custom DNS solutions.
- **Use all common DNS records types.** Azure DNS supports A, AAAA, CNAME, MX, PTR, SOA, SRV, and TXT records.
- **Automatic hostname record management.** Along with hosting your custom DNS records, Azure automatically maintains hostname records for the VMs in the specified virtual networks. In this scenario, you can optimize the domain names you use without needing to create custom DNS solutions or modify applications.
- **Hostname resolution between virtual networks.** Unlike Azure-provided host names, private DNS zones can be shared between virtual networks. This capability simplifies cross-network and service-discovery scenarios, such as virtual network peering.
- **Familiar tools and user experience.** To reduce the learning curve, this new offering uses well-established Azure DNS tools (PowerShell, Azure Resource Manager templates, and the REST API).
- **Split-horizon DNS support.** With Azure DNS, you can create zones with the same name that resolve to different answers from within a virtual network and from the public internet. A typical scenario for split-horizon DNS is to provide a dedicated version of a service for use inside your virtual network.
- **Available in all Azure regions.** The Azure DNS private zones feature is available in all Azure regions in the Azure public cloud.

## Determine Private Zone Scenarios

### Scenario 1: Name resolution scoped to a single virtual network

In this scenario, you have a virtual network and resources in Azure, including virtual machines (VMs). You want to resolve the resources from within the virtual network via a specific domain name (DNS zone). You also need the name resolution to be private and not accessible from the internet. Furthermore, for the VMs within the VNET, you need Azure to automatically register them into the DNS zone.

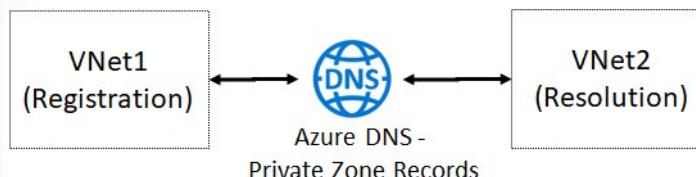


In the above diagram, VNET1 contains two VMs (VM1 and VM2). Each VM has a private IP address. When you create and a Private Zone (`contoso.lab`) to the Registration virtual network, Azure DNS will automatically create two A records in the zone. DNS queries from VM1 to resolve `VM2.contoso.lab` will receive a DNS response that contains the Private IP of VM2. And, a Reverse DNS query (PTR) for the Private IP of VM1 (10.0.0.4) issued from VM2 will receive a DNS response that contains the FQDN of VM1, as expected.

### Scenario 2: Name resolution for multiple networks

Name resolution across multiple virtual networks is probably the most common usage for DNS private zones. The following diagram shows a simple version of this scenario where there are only two virtual networks - VNet1 and VNet2.

- VNet1 is designated as a **Registration** virtual network and VNET2 is designated as a **Resolution** virtual network.
- The intent is for both virtual networks to share a common zone `contoso.lab`.
- The Resolution and Registration virtual networks are linked to the zone.
- DNS records for the Registration VNet VMs are automatically created. You can manually add DNS records for VMs in the Resolution virtual network.



In this configuration:

1. **DNS queries across the virtual networks are resolved.** A DNS query from a VM in the Resolution VNet, for a VM in the Registration VNet, will receive a DNS response containing the Private IP of VM.
2. **Reverse DNS queries are scoped to the same virtual network.** A Reverse DNS (PTR) query from a VM in the Resolution virtual network, for a VM in the Registration VNet, will receive a DNS response containing the FQDN of the VM. But, a reverse DNS query from a VM in the Resolution VNet, for a VM in the same VNet, will receive NXDOMAIN.

## Demonstration - DNS Name Resolution

In this demonstration, you will explore Azure DNS.

**Note:** There is a DNS lab.

### Create a DNS zone

1. Access the Azure Portal.
2. Search for the **DNS zones** service.
3. On the **Create DNS zone** blade enter the following values, and **Create** the new DNS zone.
  - **Name:** contoso.internal.com
  - **Subscription:** <your subscription>
  - **Resource group:** Select or create a resource group
  - **Location:** Select your Location
4. Wait for the DNS zone to be created.
5. You may need to **Refresh** the page.

### Add a DNS record set

1. Select **+Record Set**.
2. Use the **Type** drop-down to view the different types of records.
3. Notice how the required information changes as you change record types.
4. Change the **Type** to **A** and enter these values.
  - **Name:** ARecord
  - **IP Address:** 1.2.3.4
5. Notice you can add other records.
6. Click **OK** to save your record.
7. **Refresh** the page to observe the new record set.
8. You will need the resource group name.

### Optional - Use PowerShell to view DNS information

1. Open the Cloud Shell.
2. Get information about your DNS zones. Notice the name servers and number of record sets.

```
Get-AzDnsZone -Name "contoso.internal.com" -ResourceGroupName <resource-groupname>
```

3. Get information about your DNS record set.

```
Get-AzDnsRecordSet -ResourceGroupName <resourcegroupname> -ZoneName contoso.internal.com
```

### **View your name servers**

1. Access the Azure Portal and your DNS zone.
2. Review the Name Server information. There should be four name servers.
3. Open the Cloud Shell.
4. Use PowerShell to confirm your NS records.

```
Retrieve the zone information
$zone = Get-AzDnsZone -Name contoso.internal.com -ResourceGroupName <resourcegroupname>

Retrieve the name server records
Get-AzDnsRecordSet -Name "@" -RecordType NS -Zone $zone
```

### **Test the resolution**

1. Continue in the Cloud Shell.
2. Use a Name Server in your zone to review records.

```
nslookup arecord.contoso.internal.com <name server for the zone>
```

3. Nslookup should provide the IP address for the record.

### **Explore DNS metrics**

1. Return to the Azure portal.
2. Select a DNS zone, and then select **Metrics**.
3. Use the **Metrics** drop-down to view the different metrics that are available.
4. Select **Query Volume**. If you have been using nslookup, there should be queries.
5. Use the **Line Chart** drop-down to observe other chart types, like Area Chart, Bar Chart, and Scatter Chart.

For more information, [Nslookup<sup>16</sup>](#)

## **Knowledge Check**

Choose the best response for each question.

---

<sup>16</sup> <https://docs.microsoft.com/windows-server/administration/windows-commands/nslookup>

## Multiple choice

*What does Azure DNS allow you to do?*

- Manage the security and access to your website.
- Register new domain names, removing the need to use a domain registrar.
- Manage and host your registered domain and associated records.

## Multiple choice

*What type of DNS record should you create to map one or more IP addresses against a single domain?*

- CNAME
- A or AAAA
- SOA

## Multiple choice

*To perform Azure domain management tasks you must be a?*

- Global Administrator
- User Administrator
- Network Administrator

# Summary and Resources

## Summary

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.

You should now be able to:

- Identify features and usage cases for domains, custom domains, and private zones.
- Verify custom domain names using DNS records.
- Implement DNS zones, DNS delegation, and DNS record sets.

## Learn more

You can learn more by reviewing the following.

- **Azure DNS documentation<sup>17</sup>**
- **Learn - Host your domain on Azure DNS<sup>18</sup>**
- **Learn - Implement DNS for Windows Server IaaS VMs<sup>19</sup>**

<sup>17</sup> <https://docs.microsoft.com/azure/dns/>

<sup>18</sup> <https://docs.microsoft.com/learn/modules/host-domain-azure-dns/>

<sup>19</sup> <https://docs.microsoft.com/learn/modules/implement-dns-for-windows-server-iaas-virtual-machines/>

- Learn - Secure Windows Server DNS<sup>20</sup>

---

<sup>20</sup> <https://docs.microsoft.com/learn/modules/secure-windows-server-domain-name-system/>

# Module 04 Lab

## Lab 04 - Implement Virtual Networking

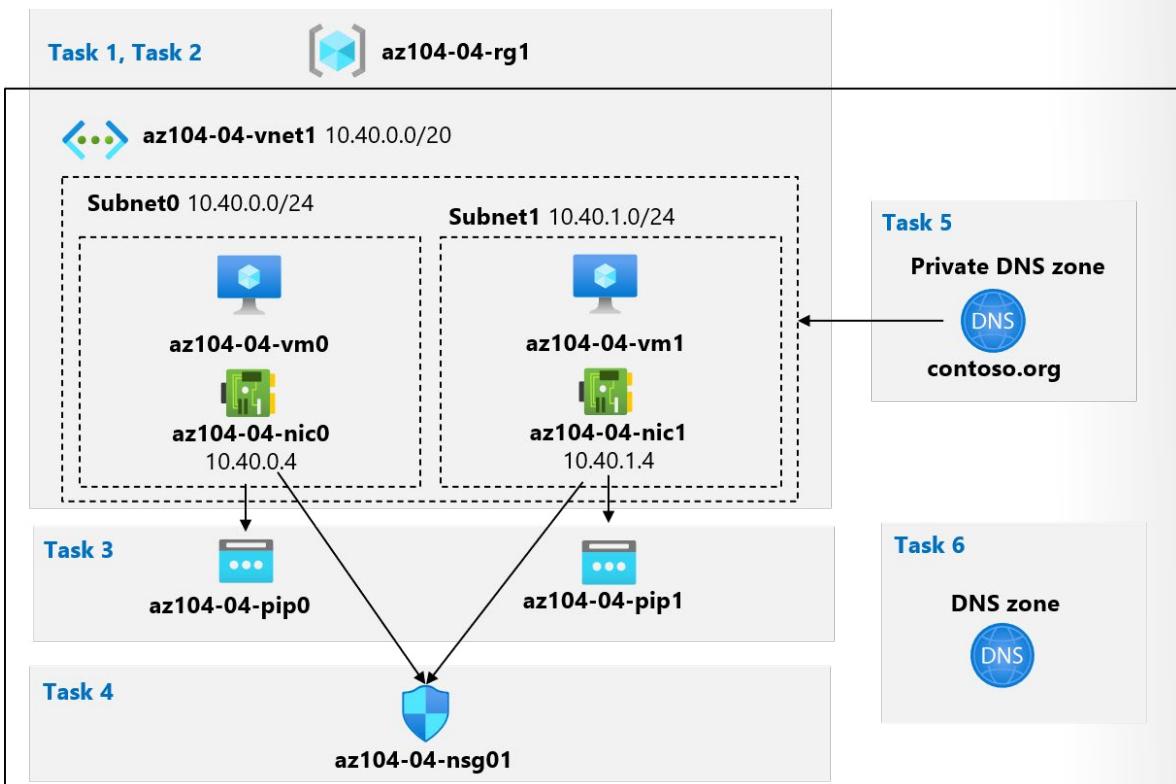
### Lab scenario

You need to explore Azure virtual networking capabilities. To start, you plan to create a virtual network in Azure that will host a couple of Azure virtual machines. Since you intend to implement network-based segmentation, you will deploy them into different subnets of the virtual network. You also want to make sure that their private and public IP addresses will not change over time. To comply with Contoso security requirements, you need to protect public endpoints of Azure virtual machines accessible from Internet. Finally, you need to implement DNS name resolution for Azure virtual machines both within the virtual network and from Internet.

### Objectives

In this lab, you will:

- Task 1: Create and configure a virtual network.
- Task 2: Deploy virtual machines into the virtual network.
- Task 3: Configure private and public IP addresses of Azure VMs.
- Task 4: Configure network security groups.
- Task 5: Configure Azure DNS for internal name resolution.
- Task 6: Configure Azure DNS for external name resolution.



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Answers

## Multiple choice

Your company has implemented Firewall rules to deny traffic based on IP address ranges. In this situation, what should you do?

- Use dynamically assigned IP addresses.
- Use statically assigned IP addresses.
- Use IP addresses in the reserved range.

### Explanation

*In this situation, use statically assigned IP addresses to avoid having to change the Firewall rules.*

## Multiple choice

You are planning your Azure network implementation to support your company's migration to Azure. Your first task is to prepare for the deployment of the first set of VMs. For these machines, consumers on the internet must be able to communicate directly with the web application on the VMs. Also, the IP configuration must be zone redundant. You should minimize costs, whenever possible, while still meeting the requirements. What should you do? Select one.

- Create a standard public IP address. During the creation of the first VM, associate the public IP address with the VM's NIC.
- Create a standard public IP address. After the first VM is created, remove the private IP address and assign the public IP address to the NIC.
- Create a basic public IP address. During the creation of the first VM, associate the public IP address with the VM.

### Explanation

*To meet the requirement of communicating directly with consumers on the internet, you must use a public IP address. To meet the requirement of having a zone redundant configuration, you must use a standard public IP address. Of the answer choices, only the answer that creates the standard public IP address first, then associates it during VM creation, functions and meets the requirements. You cannot configure a VM with only a public IP address. Instead, all VMs have a private IP address and can optionally have one or more public IP addresses.*

## Multiple choice

You have a VM with two NICs named NIC1 and NIC2. NIC1 is connected to the 10.10.8.0/24 subnet. NIC2 is connected to the 10.20.8.0/24 subnet. You plan enable direct communication from the internet to TCP port 443. You would like to maintain existing communication across the 10.10.8.0/24 and 10.20.8.0/24 subnets. To support the new functionality and keep things simple. What should you do? Select one.

- Remove the private IP address from NIC2 and then assign a public IP address to it. Then, create an inbound security rule.
- Associate a public IP address to NIC2 and create an inbound security rule.
- Create an inbound security rule for TCP port 443.

### Explanation

*To enable direct communication from the internet to the VM, you must have a public IP address. You also need an inbound security rule. You can associate the public IP address with NIC1 or NIC2, although this scenario only presents an option to associate it with NIC2 so that is the correct answer.*

**Multiple choice**

Your company has two NSG security rules for inbound traffic to your web servers. There is an allow rule with a priority of 200. And, there is a deny rule with a priority of 150. Which rule takes precedence? Select one.

- The allow rule takes precedence
- The deny rule takes precedence
- The rule that was created first takes precedence.

*Explanation*

*The deny rule takes precedence because it's processed first. The rule with priority 150 is processed before the rule with priority 200.*

**Multiple choice**

Which of the following is a default inbound security rule? Select one.

- Allow inbound coming from any VM to any other VM within the subnet.
- Allow inbound coming from any VM to any other VM within the virtual network.
- Allow traffic from any external source to any of the VMs.

*Explanation*

*By default, inbound security rules allow traffic from any VM to any other VM within the subnet.*

**Multiple choice**

Your company wants to simplify network security group rules by using service tags. Which of the following is a valid service tag? Select one.

- VirtualNetwork
- VPNGateway
- Database

*Explanation*

*VirtualNetwork. Service tags represent a group of IP addresses. For resources that you can specify by using a tag, you don't need to know the IP address or port details. Other valid service tags are Internet, SQL, Storage, AzureLoadBalancer, and AzureTrafficManager.*

**Multiple choice**

You are configuring the Azure Firewall. You need to allow Windows Update network traffic through the firewall. Which of the following should you use? Select one.

- Application rules
- Destination inbound rules
- Network rules

*Explanation*

*Application rules. Application rules define fully qualified domain names (FQDNs) that can be accessed from a subnet. That would be appropriate to allow Windows Update network traffic.*

**Multiple choice**

Your company wants to allow external users to access an Azure virtual server with a remote desktop connection. Which one of the following items would you implement on Azure Firewall to allow these connections? Select one.

- Service tag
- Source network address translation
- Destination network address translation

*Explanation*

*Destination network address translation (DNAT). You use DNAT to translate Azure Firewall's public IP address to the private IP address of the virtual server.*

**Multiple choice**

Your company wants to allow access to an Azure SQL Database instance. Which of the following network rules types should they use to configure Azure Firewall? Select one.

- Application
- Network
- NAT

*Explanation*

*Application. You use an application rule to filter traffic based on an FQDN such as server1.database.windows.net.*

**Multiple choice**

What does Azure DNS allow you to do?

- Manage the security and access to your website.
- Register new domain names, removing the need to use a domain registrar.
- Manage and host your registered domain and associated records.

*Explanation*

*Azure DNS allows you to host your registered domains. You can control and configure the domain records, like A, CNAME, MX, and setup alias records.*

**Multiple choice**

What type of DNS record should you create to map one or more IP addresses against a single domain?

- CNAME
- A or AAAA
- SOA

*Explanation*

*The A or AAAA record maps an IP address to a domain. Multiple IP addresses are known as a record set.*

**Multiple choice**

To perform Azure domain management tasks you must be a?

- Global Administrator
- User Administrator
- Network Administrator

*Explanation*

*To perform Azure domain management tasks you must be a Global Administrator.*

# Module 5 Administer Intersite Connectivity

## Configure VNet Peering

### Introduction

#### Scenario

Your engineering company has been migrating services into Azure. The company has deployed services into separate virtual networks. It hasn't configured private connectivity between the virtual networks.

Several business units have identified services in these virtual networks that need to communicate with each other. You need to enable this connectivity, but you don't want to expose these services to the internet. You also want to keep the integration as simple as possible.

You need to implement a virtual network peering solution. This solution should address transit and connectivity concerns.

#### Skills measured

Configuring virtual network peering is part of **Exam AZ-104: Microsoft Azure Administrator<sup>1</sup>**.

Configure and manage virtual networking (25–30%)

Implement and manage virtual networking

- Create and configure virtual networks, including peering.

#### Learning objectives

In this module, you will learn how to:

- Identify usage cases and product features of virtual network peering.
- Configure gateway transit, connectivity, and service chaining.

<sup>1</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

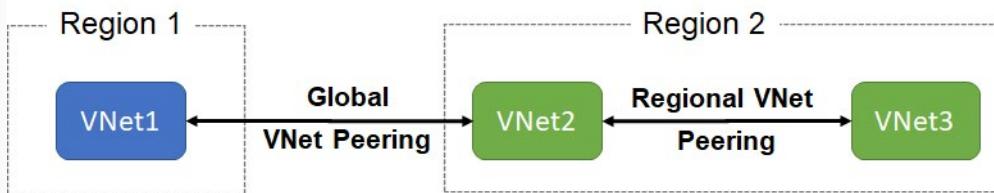
## Prerequisites

None.

## Determine VNet Peering Uses

Perhaps the simplest and quickest way to connect your VNets is to use VNet peering. Virtual network peering enables you to seamlessly connect two Azure virtual networks. Once peered, the virtual networks appear as one, for connectivity purposes. There are two types of VNet peering.

- **Regional VNet peering** connects Azure virtual networks in the same region.
- **Global VNet peering** connects Azure virtual networks in different regions. When creating a global peering, the peered virtual networks can exist in any Azure public cloud region or China cloud regions, but not in Government cloud regions. You can only peer virtual networks in the same region in Azure Government cloud regions.



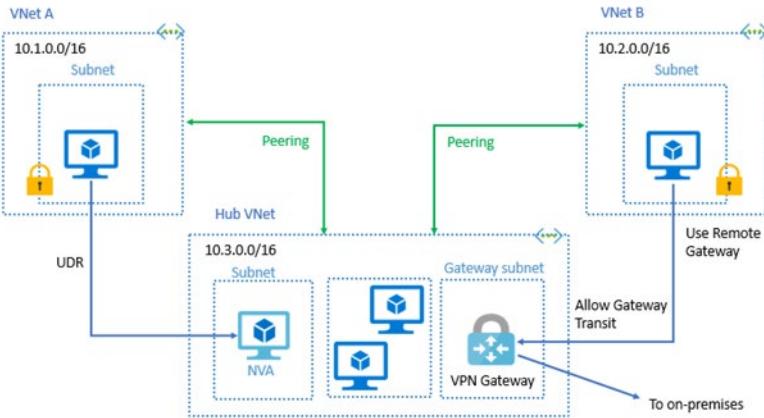
## Benefits of virtual network peering

The benefits of using local or global virtual network peering, include:

- **Private.** Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network. No public Internet, gateways, or encryption is required in the communication between the virtual networks.
- **Performance.** A low-latency, high-bandwidth connection between resources in different virtual networks.
- **Communication.** The ability for resources in one virtual network to communicate with resources in a different virtual network, once the virtual networks are peered.
- **Seamless.** The ability to transfer data across Azure subscriptions, deployment models, and across Azure regions.
- **No disruption.** No downtime to resources in either virtual network when creating the peering, or after the peering is created.

## Determine Gateway Transit and Connectivity Needs

When virtual networks are peered, you configure a VPN gateway in the peered virtual network as a transit point. In this case, a peered virtual network uses the remote gateway to gain access to other resources. A virtual network can have only one gateway. Gateway transit is supported for both VNet Peering and Global VNet Peering.



When you Allow Gateway Transit the virtual network can communicate to resources outside the peering. For example, the subnet gateway could:

- Use a site-to-site VPN to connect to an on-premises network.
- Use a VNet-to-VNet connection to another virtual network.
- Use a point-to-site VPN to connect to a client.

In these scenarios, gateway transit allows peered virtual networks to share the gateway and get access to resources. This means you do not need to deploy a VPN gateway in the peer virtual network.

**Note:** Network security groups can be applied in either virtual network to block access to other virtual networks or subnets. When configuring virtual network peering, you can either open or close the network security group rules between the virtual networks.

## Create VNet Peering

Here are the steps to configure VNet peering. Notice you will need two virtual networks. To test the peering, you will need a virtual machine in each network. Initially, the VMs will not be able to communicate, but after configuration the communication will work. The step that is new is configuring the peering of the virtual networks.

1. Create two virtual networks.
2. **Peer the virtual networks.**
3. Create virtual machines in each virtual network.
4. Test the communication between the virtual machines.

To configure the peering use the **Add peering** page. There are only a few optional configuration parameters to consider.

This virtual network

Peering link name \*

Traffic to remote virtual network ⓘ

Allow (default)

Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

Allow (default)

Block traffic that originates from outside this virtual network

Virtual network gateway ⓘ

Use this virtual network's gateway

Use the remote virtual network's gateway

None (default)

Remote virtual network

Peering link name \*

**Note:** When you add a peering on one virtual network, the second virtual network configuration is automatically added.

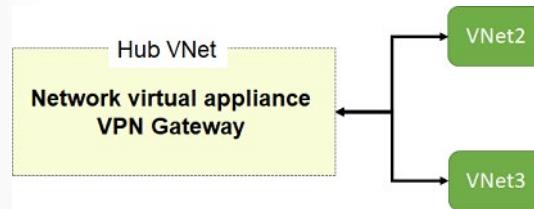
## Determine Service Chaining Uses

VNet Peering is nontransitive. When you establish VNet peering between VNet1 and VNet2 and between VNet2 and VNet3, VNet peering capabilities do not apply between VNet1 and VNet3. However, you can configure user-defined routes and service chaining to provide the transitivity. This allows you to:

- Implement a multi-level hub and spoke architecture.
- Overcome the limit on the number of VNet peerings per virtual network.

## Hub and spoke architecture

When you deploy hub-and-spoke networks, the hub virtual network can host infrastructure components like the network virtual appliance or VPN gateway. All the spoke virtual networks can then peer with the hub virtual network. Traffic can flow through network virtual appliances or VPN gateways in the hub virtual network.



## User-defined routes and service chaining

Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network, or a VPN gateway.

Service chaining lets you define user routes. These routes direct traffic from one virtual network to a virtual appliance, or virtual network gateway.

## Checking connectivity

You can check the status of the VNet peering.

- **Initiated:** When you create the peering to the second virtual network from the first virtual network, the peering status is Initiated.
- **Connected:** When you create the peering from the second virtual network to the first virtual network, its peering status is Connected. When you view the peering status for the first virtual network, you see its status changed from Initiated to Connected. The peering is not successfully established until the peering status for both virtual network peerings is Connected.

## Demonstration - VNet Peering

**Note:** For this demonstration you will need two virtual networks.

### Configure VNet peering on the first virtual network

1. In the **Azure portal**, select the first virtual network.
2. Under **Settings**, select **Peerings**.
3. Select **+ Add**.
  - Provide a **Peering link name** for **This** virtual network peering. For example, VNet1toVNet2.
  - Provide a **Peering link name** for the **Remote** virtual network peering. For example, VNet2toVNet1.
  - In the **Virtual network** drop-down, select the **Remote virtual network** you would like to peer with ensuring you also select the correct **Subscription**.
  - Use the informational icons to review the **Traffic to remote virtual network**, **Traffic forwarded from remote virtual network**, and **Virtual network gateway or Route Server** settings. If you do not have a VPN Gateway, those settings will be greyed out.
  - Click **Add** to save your settings.
4. On the **Peerings** page, discuss the **Peering Status**.

### Confirm VNet peering on the second virtual network

1. In the **Azure portal**, select the second virtual network
2. Under **Settings**, select **Peerings**.
3. Notice that a peering has automatically been created. The name is what you provided when the first virtual network peering was configured.
4. Notice that the **Peering Status** is **Connected**.
5. Discuss how the settings could be changed.
6. **Cancel** your changes.

## Knowledge check

Choose the best response for each question.

## Multiple choice

You want to connect different VNets in the same region as well as different regions and decide to use VNet peering to accomplish this. Which of the following statements is not true about VNet peering? Select one.

- The virtual networks can only exist in the same azure cloud region.
- Network traffic between peered virtual networks is private.
- Peering is easy to configure and manage, requiring little to no downtime.

## Multiple choice

You are configuring VNet Peering across two Azure two virtual networks, VNET1 and VNET2. You are configuring the VPN Gateways. You want VNET2 to be able to use to VNET1's gateway to get to resources outside the peering. What should you do? Select one.

- Select allow gateway transit on VNET1 and use remote gateways on VNET2.
- Select allow gateway transit on VNET2 and use remote gateways on VNET1.
- Select allow gateway transit and use remote gateways on both VNET1 and VNET2.

## Multiple choice

The traffic between virtual machines in peered virtual networks is routed ... Select one.

- directly through the Microsoft backbone infrastructure
- through a VPN gateway
- through the public Internet

## Summary and Resources

### Summary

Virtual network peering connects virtual networks in a hub and spoke topology. Virtual network peering is a cost-effective and easy to configure.

You should now be able to:

- Identify usage cases and product features of virtual network peering.
- Configure gateway transit, connectivity, and service chaining.

### Learn more

You can learn more by reviewing the following.

- **Virtual network peering documentation<sup>2</sup>**
- **Learn - Distribute your services across Azure virtual networks and integrate them by using virtual network peering<sup>3</sup>**

---

<sup>2</sup> <https://docs.microsoft.com/azure/virtual-network/virtual-network-peering-overview>

<sup>3</sup> <https://docs.microsoft.com/learn/modules/integrate-vnets-with-vnet-peering/>

# Configure VPN Gateway

## Introduction

### Scenario

Your company would like to connect your datacenter and other larger regional facilities to Azure. You need secure connectivity so that patient health information is protected while it's crossing the network. You don't currently have the bandwidth requirements for a dedicated circuit, and you're looking for a way to integrate these networks in a cost-effective way.

You need to create VPN gateways to securely connect your company sites to Azure.

### Skills measured

Configuring VPN Gateways is part of **Exam AZ-104: Microsoft Azure Administrator<sup>4</sup>**.

Configure and manage virtual networking (25–30%)

Integrate an on-premises network with an Azure virtual network

- Create and configure Azure VPN gateway.

### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for VPN gateways.
- Implement high availability scenarios.
- Configure site-to-site VPN connections using a VPN gateway.

### Prerequisites

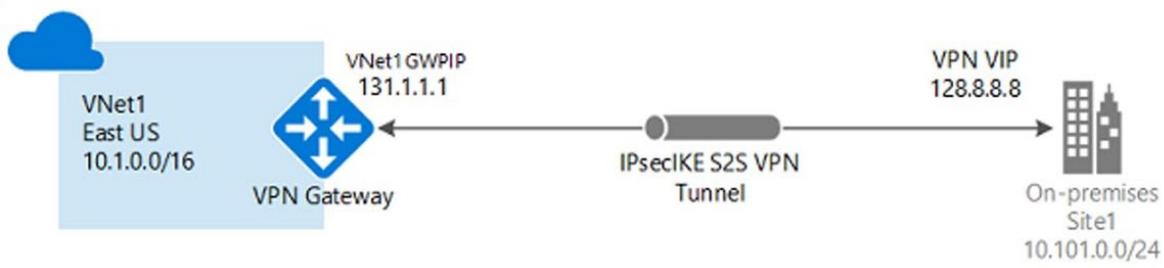
None.

## Determine VPN Gateway Uses

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.

Each virtual network can have only one VPN gateway. However, you can create multiple connections to the same VPN gateway. When you create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.

<sup>4</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>



- **Site-to-site** connections connect on-premises datacenters to Azure virtual networks
- **VNet-to-VNet** connections connect Azure virtual networks (custom)
- **Point-to-site (User VPN)** connections connect individual devices to Azure virtual networks

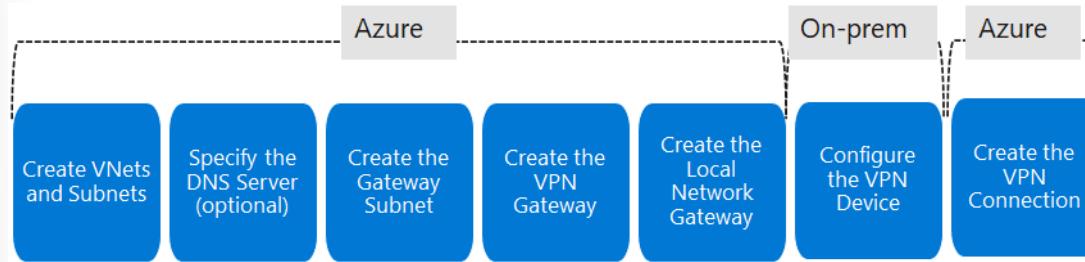
A virtual network gateway is composed of two or more VMs that are deployed to a specific subnet you create called the gateway subnet. Virtual network gateway VMs contain routing tables and run specific gateway services. These VMs are created when you create the virtual network gateway. You can't directly configure the VMs that are part of the virtual network gateway.

VPN gateways can be deployed in Azure Availability Zones. Availability zones bring resiliency, scalability, and higher availability to virtual network gateways. Availability Zones physically and logically separates gateways within a region, while protecting your on-premises network connectivity to Azure from zone-level failures.

**Note:** Creating a virtual network gateway can take up to 45 minutes to complete.

## Create Site to Site Connections

Here are the high-level steps to create a VNet-to-VNet connection. The on-premises part is only needed when you are configuring Site-to-Site. We will review in detail each step.



**Create VNets and subnets.** By now you should be familiar with creating virtual networks and subnets. Remember for this VNet to connect to an on-premises location. Contact your on-premises network administrator to reserve an IP address range for this virtual network.

**Specify the DNS server (optional).** DNS is not required to create a Site-to-Site connection. However, if you need name resolution for resources that are deployed to your virtual network, you should specify a DNS server in the virtual network configuration.

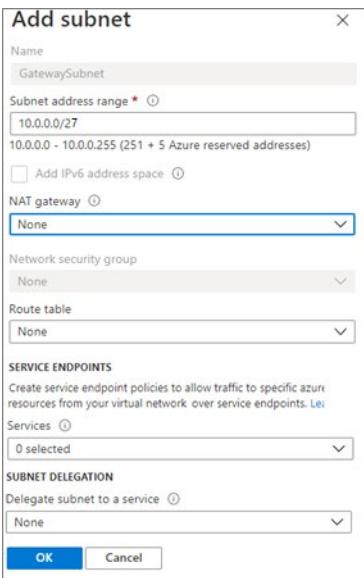
**Note:** Take time to carefully plan your network configuration. If a duplicate IP address exists on both sides of the VPN connection, traffic will not route the way you may expect it to.

## Create the Gateway Subnet

Before creating a virtual network gateway for your virtual network, you first need to create the gateway subnet. The gateway subnet contains the IP addresses that are used by the virtual network gateway. If possible, it's best to create a gateway subnet by using a CIDR block of /28 or /27 to provide enough IP addresses to accommodate future configuration requirements.

When you create your gateway subnet, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings. Never deploy other resources (for example, additional VMs) to the gateway subnet. The gateway subnet must be named *GatewaySubnet*.

Deploy a gateway in your virtual network by adding a gateway subnet.



## Create the VPN Gateway

The VPN gateway settings that you chose are critical to creating a successful connection.

Create virtual network gateway

**Instance details**

Name \*

Region \* (US) East US

Gateway type \*  VPN  ExpressRoute

VPN type \*  Route-based  Policy-based

SKU \*  VpnGw1

Generation  Generation1

**VIRTUAL NETWORK**

Virtual network \*

Only virtual networks in the currently selected subscription and region are listed.

Enable active-active mode \*  Enabled  Disabled

Configure BGP ASN \*  Enabled  Disabled

- **Gateway type.** VPN or ExpressRoute.
- **VPN Type.** Route based or Policy based. Most VPN types are Route-based. The type of VPN you choose depends on the make and model of your VPN device, and the kind of VPN connection you intend to create. Typical route-based gateway scenarios include point-to-site, inter-virtual network, or multiple site-to-site connections. Route-based is also selected when you coexist with an ExpressRoute gateway or if you need to use IKEv2. Policy-based gateways support only IKEv1.
- **SKU.** Use the drop-down to select a gateway SKU. Your choice will affect the number of tunnels you can have and the aggregate throughput benchmark. The benchmark is based on measurements of multiple tunnels aggregated through a single gateway. It is not a guaranteed throughput due to Internet traffic conditions and your application behaviors.
- **Generation.** Generation1 or Generation2. You cannot change generations or SKUs across generations. Basic and VpnGw1 SKUs are only supported in Generation1. VpnGw4 and VpnGw5 SKUs are only supported in Generation2.
- **Virtual Networks.** The virtual network that will be able to send and receive traffic through the virtual network gateway. A virtual network cannot be associated with more than one gateway.

**Note:** You can view the IP address assigned to the gateway. The gateway should appear as a connected device.

## Determine the VPN Gateway Type

When you create the virtual network gateway, you must specify a VPN type. The VPN type that you choose depends on the connection topology that you want to create. For example, a Point-to-Site (P2S) connection requires a Route-based VPN type.

A VPN type can also depend on the hardware that you are using. Site-to-Site (S2S) configurations require a VPN device. Some VPN devices only support a certain VPN type.

## Create virtual network gateway

VPN type   Route-based  Policy-based

- **Route-based VPNs.** Route-based VPNs use *routes* in the IP forwarding or routing table to direct packets into their corresponding tunnel interfaces. The tunnel interfaces then encrypt or decrypt the packets in and out of the tunnels. The policy (or traffic selector) for Route-based VPNs are configured as any-to-any (or wild cards).
- **Policy-based VPNs.** Policy-based VPNs encrypt and direct packets through IPsec tunnels based on the IPsec policies configured with the combinations of address prefixes between your on-premises network and the Azure VNet. The policy (or traffic selector) is defined as an access list in the VPN device configuration. When using a Policy-based VPN, keep in mind the following limitations:
  - Policy-Based VPNs can only be used on the Basic gateway SKU and is not compatible with other gateway SKUs.
  - You can have only one tunnel when using a Policy-based VPN.
  - You can only use Policy-based VPNs for S2S connections, and only for certain configurations. Most VPN Gateway configurations require a Route-based VPN.

**Note:** Once a virtual network gateway has been created, you can't change the VPN type.

## Determine Gateway SKU and Generation

When you create a virtual network gateway, you need to specify the gateway SKU that you want to use. Select the SKU that satisfies your requirements based on the types of workloads, throughputs, features, and SLAs.

| Gen | SKU       | S2S/VNet-to-VNet Tunnels | P2S IKEv2 Connections | Aggregate Throughput Benchmark |
|-----|-----------|--------------------------|-----------------------|--------------------------------|
| 1   | VpnGw1/Az | Max. 30                  | Max. 250              | 650 Mbps                       |
| 1   | VpnGw2/Az | Max. 30                  | Max. 500              | 1.0 Gbps                       |
| 2   | VpnGw2/Az | Max. 30                  | Max. 500              | 1.25 Gbps                      |
| 1   | VPNGw3/Az | Max. 30                  | Max. 1000             | 1.25 Gbps                      |
| 2   | VPNGw3/Az | Max. 30                  | Max. 1000             | 2.5 Gbps                       |
| 2   | VPNGw4/Az | Max. 30                  | Max. 5000             | 5.0 Gbps                       |

Aggregate Throughput Benchmark is based on measurements of multiple tunnels aggregated through a single gateway. The Aggregate Throughput Benchmark for a VPN Gateway is S2S + P2S combined. The Aggregate Throughput Benchmark is not a guaranteed throughput due to Internet traffic conditions and your application behaviors.

**Note:** The Basic SKU (not shown) is considered a legacy SKU.

## Create the Local Network Gateway

The local network gateway typically refers to the on-premises location. You give the site a name by which Azure can refer to it, then specify the IP address or FQDN of the on-premises VPN device for the connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located in the on-premises network.

## Create local network gateway

Name \*

 ✓

Endpoint ⓘ

IP address FQDN

IP address \* ⓘ

 ✓

Address space ⓘ

 ... ... Configure BGP settings

**IP Address.** The public IP address of the local gateway.

**Address Space.** One or more IP address ranges (in CIDR notation) that define your local network's address space. If you plan to use this local network gateway in a BGP-enabled connection, then the minimum prefix you need to declare is the host address of your BGP Peer IP address on your VPN device.

## Setup the On-Premises VPN Device

There is a validated list of standard VPN devices that work well with the VPN gateway. This list was created in partnership with device manufacturers like Cisco, Juniper, Ubiquiti, and Barracuda Networks.

When your device is not listed in the validated VPN devices table, the device may still work. Contact your device manufacturer for support and configuration instructions.

To configure your VPN device, you will need:

- **A shared key.** The same shared key that you specify when creating the VPN connection.
- **The public IP address of your VPN gateway.** The IP address can be new or existing.

**Note:** Depending on the VPN device that you have, you may be able to **download a VPN device configuration script<sup>5</sup>**.

## Create the VPN Connection

Once your VPN gateways are created, you can create the connection between them. If your VNets are in the same subscription, you can use the portal.

---

<sup>5</sup> <https://docs.microsoft.com/azure/vpn-gateway/vpn-gateway-download-vpndevicescript>

The screenshot shows two overlapping windows. The left window is titled 'Add connection' and has a sub-header 'vng01'. It contains fields for 'Name \*' (set to 'Azure-to-OnPrem'), 'Connection type' (set to 'Site-to-site (IPsec)'), 'Virtual network gateway' (set to 'vng01'), 'Local network gateway' (set to 'Azure-to-OnPrem'), and 'Shared key (PSK)' (set to 'abc123'). The right window is titled 'Choose local network gat...' and lists a single item: 'Create new' followed by 'Azure-to-OnPrem NetworkRG'.

- **Name.** Enter a name for your connection.
- **Connection type.** Select Site-to-Site (IPSec) from the drop-down.
- **Shared key (PSK).** In this field, enter a shared key for your connection. You can generate or create this key yourself. In a site-to-site connection, the key you use is the same for your on-premises device and your virtual network gateway connection.

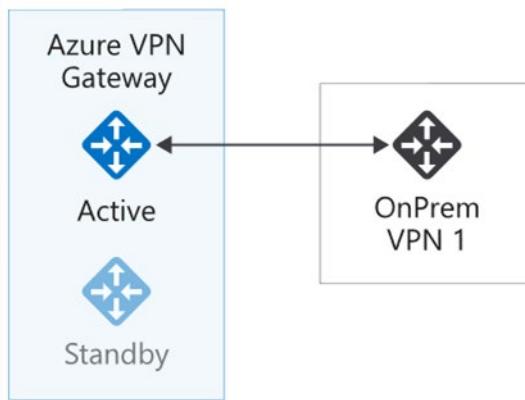
## Verify the VPN Connection

After you have configured all the Site-to-Site components, it is time to verify that everything is working. You can verify the connections either in the portal, or by using PowerShell.

## Determine High Availability Scenarios

### Active/standby

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically, and resume the S2S VPN or VNet-to-VNet connections. The switch over will cause a brief interruption. For planned maintenance, the connectivity should be restored within 10 to 15 seconds. For unplanned issues, the connection recovery will be longer, about 1 minute to 1 and a half minutes in the worst case. For P2S VPN client connections to the gateway, the P2S connections will be disconnected and the users will need to reconnect from the client machines.



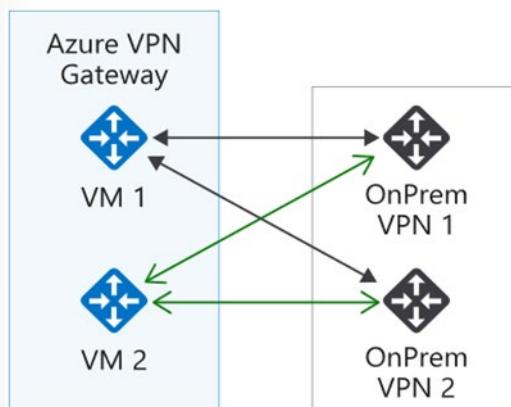
## Active/active

You can now create an Azure VPN gateway in an active-active configuration, where both instances of the gateway VMs will establish S2S VPN tunnels to your on-premises VPN device.

In this configuration, each Azure gateway instance will have a unique public IP address, and each will establish an IPsec/IKE S2S VPN tunnel to your on-premises VPN device specified in your local network gateway and connection. Both VPN tunnels are actually part of the same connection. You will still need to configure your on-premises VPN device to accept or establish two S2S VPN tunnels to those two Azure VPN gateway public IP addresses.

When in active-active configuration, the traffic from your Azure virtual network to your on-premises network will be routed through both tunnels simultaneously. The same TCP or UDP flow will always traverse the same tunnel or path, unless a maintenance event happens on one of the instances.

When a planned maintenance or unplanned event happens to one gateway instance, the IPsec tunnel from that instance to your on-premises VPN device will be disconnected. The corresponding routes on your VPN devices should be removed or withdrawn automatically so that the traffic will be switched over to the other active IPsec tunnel. On the Azure side, the switch over will happen automatically from the affected instance to the active instance.



## Demonstration - VPN Gateways

In this demonstration, we will explore virtual network gateways.

**Note:** This demonstration works best with two virtual networks with subnets.

### Explore the Gateway subnet blade

1. For one of your virtual networks, select the **Subnets** blade.
2. Select **+ Gateway subnet**. Notice the name of the subnet cannot be changed. Notice the **address range** of the gateway subnet. The address must be contained by the address space of the virtual network.
3. Remember each virtual network needs a gateway subnet.
4. Close the Add gateway subnet page. You do not need to save your changes.

### Explore the Connected Devices blade

1. For the virtual network, select the **Connected Devices** blade.
2. After a gateway subnet is deployed it will appear on the list of connected devices.

### Explore adding a virtual network gateway

1. Search for **Virtual network gateways**.
2. Click **+ Add**.
3. Review each setting for the virtual network gateway.
4. Use the Information icons to learn more about the settings.
5. Notice the **Gateway type**, **VPN type**, and **SKU**.
6. Notice the need for a **Public IP address**.
7. Remember each virtual network will need a virtual network gateway.
8. Close the Add virtual network gateway. You do not need to save your changes.

### Explore adding a connection between the virtual networks

1. Search for **Connections**.
2. Click **+ Add**.
3. Notice the **Connection type** can be VNet-to-VNet, Site-to-Site (IPsec), or ExpressRoute.
4. Provide enough information, so you can click the **Ok** button.
5. On the **Settings** page, notice that you will need select the two different virtual networks.
6. Read the Help information on the **Establish bidirectional connectivity** checkbox.
7. Notice the **Shared key (PSK)** information.
8. Close the Add connection page. You do not need to save your changes.

## Knowledge check

Choose the best response for each question.

## Multiple choice

*Your company is preparing to implement a Site-to-Site VPN to Microsoft Azure. You do all the following, except? Select one.*

- Obtain a VPN device for the on-premises environment.
- Obtain a VPN device for the Azure environment.
- Create a virtual network gateway (VPN) and the local network gateway in Azure.

## Multiple choice

*Your company is preparing to implement persistent connectivity to Microsoft Azure. The company has a single site, headquarters, which has an on-premises data center. The company requires the connectivity be persistent. Connectivity must provide for the entire on-premises site. You need to implement a connectivity solution to meet the requirements. What should you do? Select one.*

- Implement a Site-to-Site VPN.
- Implement a Virtual Private Cloud (VPC).
- Implement a VNet-to-VNet VPN.

## Multiple choice

*You are configuring a site-to-site VPN connection between your on-premises network and your Azure network. The on-premises network uses a Cisco ASA VPN device. Before starting the configuration, you ensure you have all the following, except? Select one.*

- The shared access signature key for the recovery services vault.
- The shared key you provided when you created your site-to-site VPN connection.
- The public IP address of your virtual network gateway.

## Multiple choice

*Your VPN gateway works with ExpressRoute. Which VPN type should you select? Select one.*

- Path-based
- Route-based
- SKU-based

## Multiple choice

*You are creating a connection between two virtual networks. Performance is a key concern. Which of the following will most influence performance? Select one.*

- Ensuring you select a route-based VPN.
- Ensuring you select a policy-based VPN.
- Ensuring you select an appropriate Gateway SKU.

# Summary and Resources

## Summary

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.

You should now be able to:

- Identify features and usage cases for VPN gateways.
- Implement high availability scenarios.
- Configure site-to-site VPN connections using a VPN gateway.

## Learn more

You can learn more by reviewing the following.

- **VPN Gateway documentation<sup>6</sup>**
- **Validated VPN devices list<sup>7</sup>**
- **Learn - Connect your on-premises network to Azure with VPN Gateway<sup>8</sup>**

<sup>6</sup> <https://docs.microsoft.com/azure/vpn-gateway/>

<sup>7</sup> <https://docs.microsoft.com/azure/vpn-gateway/vpn-gateway-about-vpn-devices>

<sup>8</sup> <https://docs.microsoft.com/learn/modules/connect-on-premises-network-with-vpn-gateway/>

# ExpressRoute and Virtual WAN

## Introduction

### Scenario

Your company has major offices located throughout the world. In some cases, on-premises must connect to Azure. These connections must be private and secure. In other cases, a global transit network architecture is needed.

You need to evaluate using ExpressRoute and Virtual WAN to provide these connection services.

### Skills measured

ExpressRoute and Virtual WAN are part of **Exam AZ-104: Microsoft Azure Administrator<sup>9</sup>**.

Configure and manage virtual networking (25–30%)

Integrate an on-premises network with an Azure virtual network

- Create and configure Azure ExpressRoute.
- Configure Azure Virtual WAN.

### Learning objectives

In this module, you will learn how to:

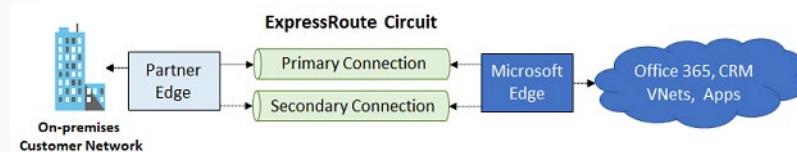
- Identify features and usage cases for ExpressRoute.
- Coexist site-to-site and ExpressRoute networks.
- Identify features and usage cases for virtual WAN.

### Prerequisites

None.

## Determine ExpressRoute Uses

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud. The connection is facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Microsoft 365, and CRM Online.



<sup>9</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

## Make your connections fast, reliable, and private

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet, and they offer more reliability, faster speeds, and lower latencies than typical Internet connections. In some cases, using ExpressRoute connections to transfer data between on-premises systems and Azure can give you significant cost benefits.

With ExpressRoute, establish connections to Azure at an ExpressRoute location, such as an Exchange provider facility, or directly connect to Azure from your existing WAN network, such as a multiprotocol label switching (MPLS) VPN, provided by a network service provider.

## Use a virtual private cloud for storage, backup, and recovery

ExpressRoute gives you a fast and reliable connection to Azure with bandwidths up to 100 Gbps. The high connection speeds make it excellent for scenarios like periodic data migration, replication for business continuity, and disaster recovery. ExpressRoute is a cost-effective option for transferring large amounts of data, such as datasets for high-performance computing applications, or moving large virtual machines between your dev-test environments.

## Extend and connect your datacenters

Use ExpressRoute to connect and add compute and storage capacity to your existing datacenters. With high throughput and fast latencies, Azure will feel like a natural extension to or between your datacenters, so you enjoy the scale and economics of the public cloud without having to compromise on network performance.

## Build hybrid applications

Build applications that span on-premises infrastructure and Azure without compromising privacy or performance. For example, run a corporate intranet application in Azure that authenticates your customers with an on-premises Active Directory service. You serve all of your corporate customers without traffic ever routing through the public Internet.

## Determine ExpressRoute Capabilities

ExpressRoute is supported across all Azure regions and locations. This map provides a list of Azure regions and ExpressRoute locations. ExpressRoute locations are where Microsoft peers with several service providers. When you connected to at least one ExpressRoute location within the geopolitical region, you will access Azure services across all regions within a geopolitical region.



## ExpressRoute benefits

### Layer 3 connectivity

Microsoft uses BGP to exchange routes between your on-premises network, your instances in Azure, and Microsoft public addresses. Multiple BGP sessions are created for different traffic profiles.

### Redundancy

Each ExpressRoute circuit consists of two connections to two Microsoft Enterprise edge routers (MSEEs) from the connectivity provider/your network edge. Microsoft requires dual BGP connection from the connectivity provider/your network edge – one to each MSEE.

### Connectivity to Microsoft cloud services

ExpressRoute connections enable access to Microsoft Azure services, Microsoft 365 services, and Microsoft Dynamics 365. Microsoft 365 was created to be accessed securely and reliably via the Internet, so ExpressRoute requires Microsoft authorization.

### Connectivity to all regions within a geopolitical region

You connect to Microsoft in one of our peering locations and access regions within the geopolitical region. For example, if you connect to Microsoft in Amsterdam through ExpressRoute, you'll have access to all Microsoft cloud services hosted in Northern and Western Europe.

### Global connectivity with ExpressRoute premium add-on

You enable the ExpressRoute premium add-on feature to extend connectivity across geopolitical boundaries. For example, if you connect to Microsoft in Amsterdam through ExpressRoute, you will have access to all Microsoft cloud services hosted in all regions across the world, except national clouds.

### Across on-premises connectivity with ExpressRoute Global Reach

You enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. For example, if you have a private data center in California connected to ExpressRoute in Silicon Valley, and another private data center in Texas connected to ExpressRoute in

Dallas, with ExpressRoute Global Reach, you can connect your private data centers together through two ExpressRoute circuits. Your cross-data-center traffic will traverse through Microsoft's network.

### Bandwidth options

You purchase ExpressRoute circuits for a wide range of bandwidths from 50 Mbps to 100 Gbit. Be sure to check with your connectivity provider to determine the bandwidths they support.

### Flexible billing models

You pick a billing model that works best for you. Choose between the billing models listed below.

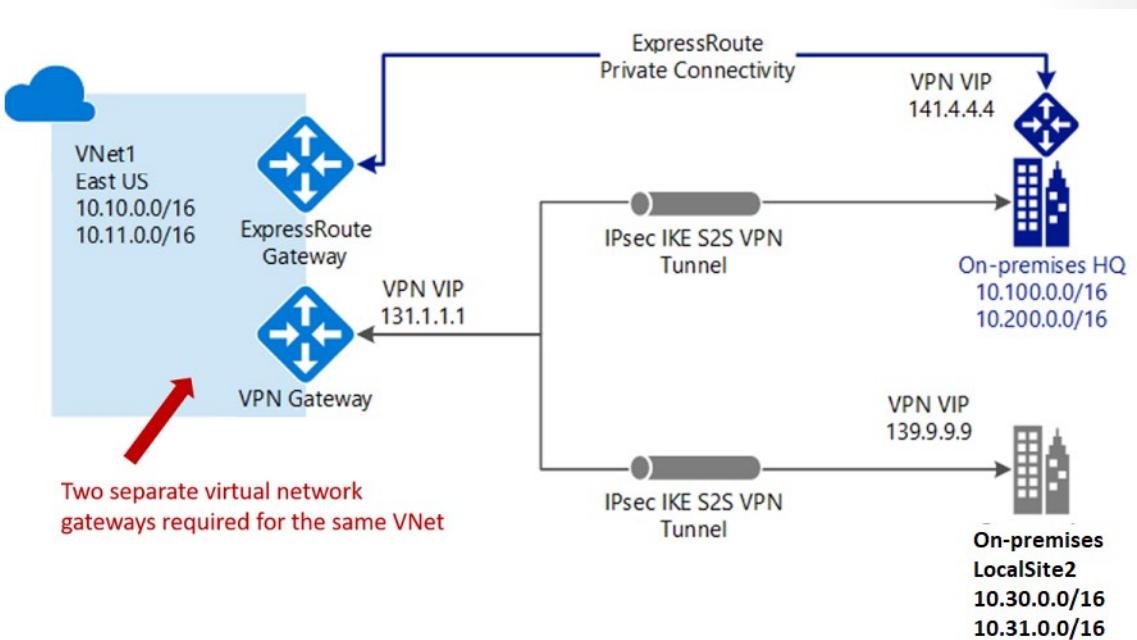
- **Unlimited data.** Billing is based on a monthly fee; all inbound and outbound data transfer is included free of charge.
- **Metered data.** Billing is based on a monthly fee; all inbound data transfer is free of charge. Outbound data transfer is charged per GB of data transfer. Data transfer rates vary by region.
- **ExpressRoute premium add-on.** This add-on includes increased routing table limits, increased number of VNets, global connectivity, and connections to Microsoft 365 and Dynamics 365.

## Coexist Site-to-Site and ExpressRoute

ExpressRoute is a direct, private connection from your WAN (not over the public Internet) to Microsoft Services, including Azure. Site-to-Site VPN traffic travels encrypted over the public Internet. Being able to configure Site-to-Site VPN and ExpressRoute connections for the same virtual network has several advantages.

You configure a Site-to-Site VPN as a secure failover path for ExpressRoute or use Site-to-Site VPNs to connect to sites that are not part of your network, but that are connected through ExpressRoute. Notice this configuration requires two virtual network gateways for the same virtual network, one using the gateway type *VPN*, and the other using the gateway type *ExpressRoute*.

## ExpressRoute and VPN Gateway coexisting connections example



## ExpressRoute connection models

You create a connection between your on-premises network and the Microsoft cloud in three different ways, Colocated at a cloud exchange, Point-to-point Ethernet Connection, and Any-to-any (IPVPN) Connection. Connectivity providers offer one or more connectivity models. You work with your connectivity provider to pick the model that works best for you.

### Colocated at a cloud exchange

If you are colocated in a facility with a cloud exchange, you order virtual cross-connections to the Microsoft cloud through the colocation provider's Ethernet exchange. Colocation providers offer either Layer 2 cross-connections, or managed Layer 3 cross-connections between your infrastructure in the colocation facility and the Microsoft cloud.

### Point-to-point Ethernet connections

You connect your on-premises datacenters/offices to the Microsoft cloud through point-to-point Ethernet links. Point-to-point Ethernet providers offer Layer 2 connections, or managed Layer 3 connections between your site and the Microsoft cloud.

### Any-to-any (IPVPN) networks

You integrate your WAN with the Microsoft cloud. IPVPN providers, typically Multiprotocol Label Switching (MPLS) VPN, offer any-to-any connectivity between your branch offices and datacenters. The Microsoft cloud can be interconnected to your WAN to make it appear just like any other branch office. WAN providers typically offer managed Layer 3 connectivity.

**Note:** Currently, the deployment options for S2S and ExpressRoute coexisting connections are only possible through PowerShell, and not the Azure portal.

## Compare Intersite Connection Options

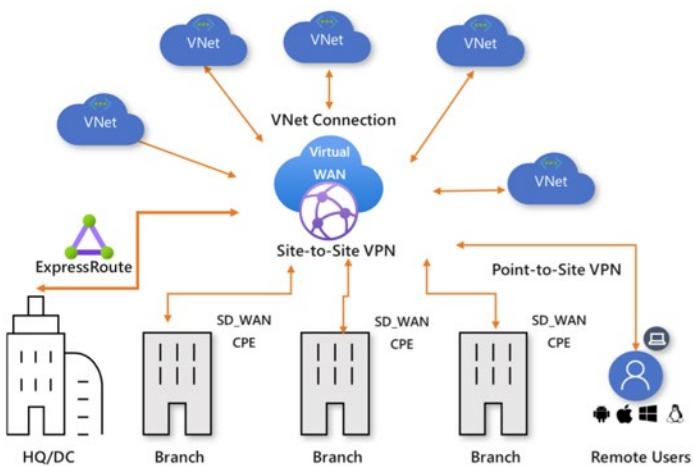
There are many intersite connection choices. This table summarizes how to make a selection.

| Connection                     | Azure Services Supported                             | Bandwidths                   | Protocols                     | Typical Use Case                                                                        |
|--------------------------------|------------------------------------------------------|------------------------------|-------------------------------|-----------------------------------------------------------------------------------------|
| Virtual network, point-to-site | Azure IaaS services, Azure Virtual Machines          | Based on the gateway SKU     | Active/passive                | Dev, test, and lab environments for cloud services and virtual machines.                |
| Virtual network, site-to-site  | Azure IaaS services, Azure Virtual Machines          | Typically < 1 Gbps aggregate | Active/passive, Active/active | Dev, test, and lab environments. Small-scale production workloads and virtual machines. |
| ExpressRoute                   | Azure IaaS and PaaS services, Microsoft 365 services | 50 Mbps up to 100 Gbps       | Active/active                 | Enterprise-class and mission-critical workloads. Big data solutions.                    |

## Determine Virtual WAN Uses

Azure Virtual WAN is a networking service that provides optimized and automated branch connectivity to, and through, Azure. Azure regions serve as hubs that you can choose to connect your branches to. You use the Azure backbone to connect branches and enjoy branch-to-VNet connectivity. There is a list of partners that support connectivity automation with Azure Virtual WAN VPN.

Azure Virtual WAN brings together many Azure cloud connectivity services such as site-to-site VPN, User VPN (point-to-site), and ExpressRoute into a single operational interface. Connectivity to Azure VNets is established by using virtual network connections. The global transit network architecture based on a hub-and-spoke connectivity model. The cloud hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'.



## Virtual WAN advantages

- **Integrated connectivity solutions in hub and spoke.** Automate site-to-site configuration and connectivity between on-premises sites and an Azure hub.
- **Automated spoke setup and configuration.** Connect your virtual networks and workloads to the Azure hub seamlessly.
- **Intuitive troubleshooting.** You can see the end-to-end flow within Azure, and then use this information to take required actions.

## Virtual WAN types

There are two types of virtual WANs: Basic and Standard.

| Virtual WAN type | Hub type | Available configurations                                                                                                   |
|------------------|----------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Basic</b>     | Basic    | Site-to-site VPN only                                                                                                      |
| <b>Standard</b>  | Standard | ExpressRoute, User VPN (P2S).<br>VPN (site-to-site), Inter-hub, and<br>VNet-to-VNet transiting through<br>the virtual hub. |

## Knowledge Check

Choose the best response for each question.

### Multiple choice

*Your company provides customers a virtual network in the cloud. You have dozens of Linux virtual machines in another virtual network. You need to install an Azure load balancer to direct traffic between the virtual networks. What should you do? Select one.*

- Install an external load balancer.
- Install an internal load balancer.
- Install a network load balancer.

### Multiple choice

*Your company has a popular regional web site. The company plans to move it to Azure and host it in the Canada East region. Ten Azure VMs have been configured to handle the web requests. The traffic should be evenly distributed across the machines. The machines should provide good performance even during peak times. Your solution should minimize complexity and ongoing costs. Which of the following would you select in this scenario? Select one.*

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

### Multiple choice

*What is the default distribution type for traffic through a load balancer? Select one.*

- Source IP affinity
- Five-tuple hash
- Three-tuple hash

### Multiple choice

*Which configuration is required to configure an internal load balancer?*

- Virtual machines should be in the same virtual network
- Virtual machines must be publicly accessible
- Virtual machines must be in an availability set

## Multiple choice

Which of the following statement about external load balancers is correct?

- They have a private, front-facing IP address.
- They don't have a listener IP address.
- They have a public IP address.

## Summary

Azure ExpressRoute can be used to connect your on-premises networks to the Microsoft cloud infrastructure. ExpressRoute works with an approved connectivity provider to establish the connections via a dedicated circuit.

Azure Virtual WAN can also be used to establish network connections. Azure Virtual WAN provides any-to-any connectivity, custom routing, and security.

You should now be able to:

- Identify features and usage cases for ExpressRoute.
- Coexist site-to-site and ExpressRoute networks.
- Identify features and usage cases for virtual WAN.

## Learn more

You can learn more by reviewing the following.

- **ExpressRoute documentation<sup>10</sup>**
- **Azure Virtual WAN documentation<sup>11</sup>**
- **Learn - Connect your on-premises network to the Microsoft global network by using ExpressRoute<sup>12</sup>**
- **Learn - Configure the network for your virtual machines<sup>13</sup>**
- **Learn - Introduction to Azure Virtual WAN<sup>14</sup>**

<sup>10</sup> <https://docs.microsoft.com/azure/expressroute/>

<sup>11</sup> <https://docs.microsoft.com/azure/virtual-wan/>

<sup>12</sup> <https://docs.microsoft.com/learn/modules/connect-on-premises-network-with-expressroute/>

<sup>13</sup> <https://docs.microsoft.com/learn/modules/configure-network-for-azure-virtual-machines/>

<sup>14</sup> <https://docs.microsoft.com/learn/modules/introduction-azure-virtual-wan/>

## Module 05 Lab

### Lab 05 - Implement Intersite Connectivity

#### Lab scenario

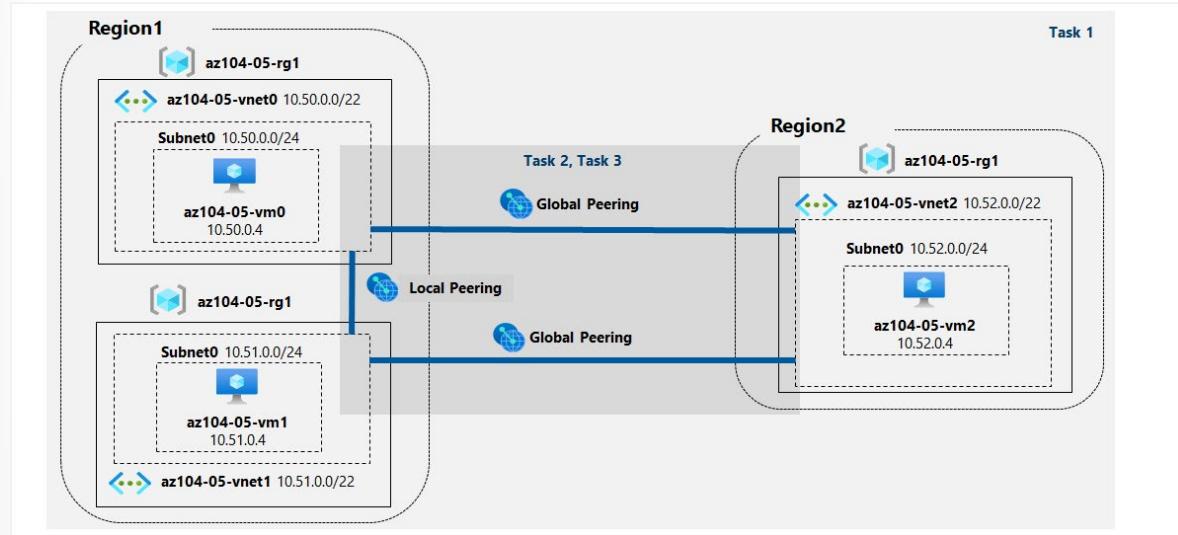
Contoso has its datacenters in Boston, New York, and Seattle offices connected via a mesh wide-area network links, with full connectivity between them. You need to implement a lab environment that will reflect the topology of the Contoso's on-premises networks and verify its functionality.

#### Objectives

In this lab, you will:

- Task 1: Provision the lab environment.
- Task 2: Configure local and global virtual network peering.
- Task 3: Test intersite connectivity.

#### Architecture Diagram



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Answers

## Multiple choice

You want to connect different VNets in the same region as well as different regions and decide to use VNet peering to accomplish this. Which of the following statements is not true about VNet peering? Select one.

- The virtual networks can only exist in the same azure cloud region.
- Network traffic between peered virtual networks is private.
- Peering is easy to configure and manage, requiring little to no downtime.

*Explanation*

*The virtual networks can exist in any Azure cloud region.*

## Multiple choice

You are configuring VNet Peering across two Azure two virtual networks, VNET1 and VNET2. You are configuring the VPN Gateways. You want VNET2 to be able to use to VNET1's gateway to get to resources outside the peering. What should you do? Select one.

- Select allow gateway transit on VNET1 and use remote gateways on VNET2.
- Select allow gateway transit on VNET2 and use remote gateways on VNET1.
- Select allow gateway transit and use remote gateways on both VNET1 and VNET2.

*Explanation*

*Select allow gateway transit on VNET1 and use remote gateways on VNET2. VNET1 will allow VNET2 to transit external resources, and VNET2 will expect to use a remote gateway.*

## Multiple choice

The traffic between virtual machines in peered virtual networks is routed ... Select one.

- directly through the Microsoft backbone infrastructure
- through a VPN gateway
- through the public Internet

*Explanation*

*The traffic between virtual machines in peered virtual networks is routed directly through the Microsoft backbone infrastructure.*

## Multiple choice

Your company is preparing to implement a Site-to-Site VPN to Microsoft Azure. You do all the following, except? Select one.

- Obtain a VPN device for the on-premises environment.
- Obtain a VPN device for the Azure environment.
- Create a virtual network gateway (VPN) and the local network gateway in Azure.

*Explanation*

*Obtain a VPN device for the Azure environment. Azure does not require a VPN device.*

**Multiple choice**

Your company is preparing to implement persistent connectivity to Microsoft Azure. The company has a single site, headquarters, which has an on-premises data center. The company requires the connectivity be persistent. Connectivity must provide for the entire on-premises site. You need to implement a connectivity solution to meet the requirements. What should you do? Select one.

- Implement a Site-to-Site VPN.
- Implement a Virtual Private Cloud (VPC).
- Implement a VNet-to-VNet VPN.

*Explanation*

*Implement a Site-to-Site VPN.*

**Multiple choice**

You are configuring a site-to-site VPN connection between your on-premises network and your Azure network. The on-premises network uses a Cisco ASA VPN device. Before starting the configuration, you ensure you have all the following, except? Select one.

- The shared access signature key for the recovery services vault.
- The shared key you provided when you created your site-to-site VPN connection.
- The public IP address of your virtual network gateway.

*Explanation*

*You only need the shared key and public IP address of the gateway.*

**Multiple choice**

Your VPN gateway works with ExpressRoute. Which VPN type should you select? Select one.

- Path-based
- Route-based
- SKU-based

*Explanation*

*Route-based. Typical route-based gateway scenarios include point-to-site, inter-virtual network, or multiple site-to-site connections. Route-based is also selected when you coexist with an ExpressRoute gateway or if you need to use IKEv2.*

**Multiple choice**

You are creating a connection between two virtual networks. Performance is a key concern. Which of the following will most influence performance? Select one.

- Ensuring you select a route-based VPN.
- Ensuring you select a policy-based VPN.
- Ensuring you select an appropriate Gateway SKU.

*Explanation*

*Select the appropriate Gateway SKU to ensure performance.*

**Multiple choice**

Your company provides customers a virtual network in the cloud. You have dozens of Linux virtual machines in another virtual network. You need to install an Azure load balancer to direct traffic between the virtual networks. What should you do? Select one.

- Install an external load balancer.
- Install an internal load balancer.
- Install a network load balancer.

*Explanation*

*Install an internal load balancer. Azure has two types of load balancers: public and internal. An internal load balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure.*

**Multiple choice**

Your company has a popular regional web site. The company plans to move it to Azure and host it in the Canada East region. Ten Azure VMs have been configured to handle the web requests. The traffic should be evenly distributed across the machines. The machines should provide good performance even during peak times. Your solution should minimize complexity and ongoing costs. Which of the following would you select in this scenario? Select one.

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

*Explanation*

*Azure Load Balancer. In this scenario, the requirements call for load balancing of a web site with minimal complexity and costs. The web site is in a single region, which rules out Azure Traffic Manager (which is geared toward a distributed web application). Azure CDN is complex and expensive, and it best suited for delivering static web content at various locations worldwide (with maximum performance). Azure Cloud Services are suited for applications and APIs, not for this scenario.*

**Multiple choice**

What is the default distribution type for traffic through a load balancer? Select one.

- Source IP affinity
- Five-tuple hash
- Three-tuple hash

*Explanation*

*Five-tuple hash. The hash includes Source IP, Source port, Destination IP, Destination port, and Protocol type.*

**Multiple choice**

Which configuration is required to configure an internal load balancer?

- Virtual machines should be in the same virtual network
- Virtual machines must be publicly accessible
- Virtual machines must be in an availability set

*Explanation*

*Virtual machines should be in the same virtual network. The virtual machines that you use a load balancer to distribute a load to must be in the same virtual network.*

**Multiple choice**

Which of the following statement about external load balancers is correct?

- They have a private, front-facing IP address.
- They don't have a listener IP address.
- They have a public IP address.

*Explanation*

*They have a public IP address. External load balancers have public IP addresses.*

## Module 6 Adminster Network Traffic

### Configure Network Routing and Endpoints

#### Introduction

#### Scenario

Your company recently suffered a security incident that exposed customer personal information. This resulted in the loss of customers' confidential data and confidence. The IT team has recommended implementing network virtual appliances.

You must ensure traffic is properly routed through the virtual appliances. You explore other security options like service endpoints and private links.

#### Skills measured

Configure routing methods and endpoints is part of **Exam AZ-104: Microsoft Azure Administrator<sup>1</sup>**.

Configure and manage virtual networking (25–30%)

Implement and manage virtual networking

- Configure user-defined network routes.
- Configure endpoints on subnets.
- Configure private endpoints.

#### Learning objectives

In this module, you will learn how to:

- Implement system routes and user-defined routes.
- Configure a custom route.

<sup>1</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

- Implement service endpoints.
- Identify features and usage cases for private links and endpoint services.

## Prerequisites

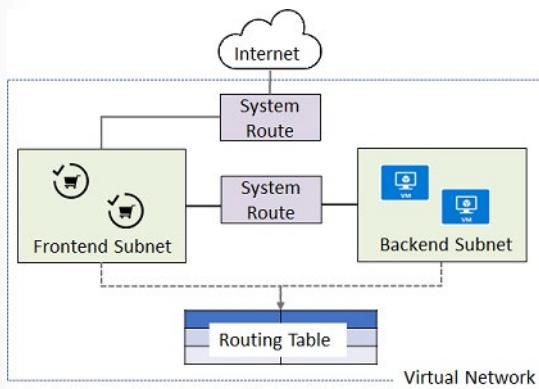
- Familiarity with network routing.

# Review System Routes

Azure uses **system routes** to direct network traffic between virtual machines, on-premises networks, and the Internet. The following situations are managed by these system routes:

- Traffic between VMs in the same subnet.
- Between VMs in different subnets in the same virtual network.
- Data flow from VMs to the Internet.
- Site-to-Site and ExpressRoute communication through the VPN gateway.

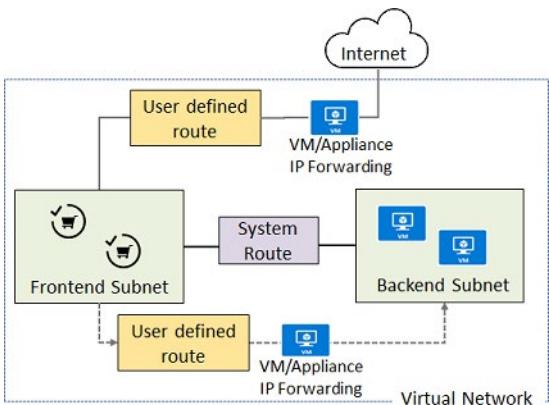
For example, consider this virtual network with two subnets. Communication between the subnets and from the frontend to the internet are all managed by Azure using the default system routes.



**Note:** Information about the system routes is recorded in a route table. A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network. Route tables are associated to subnets, and each packet leaving a subnet is handled based on the associated route table. Packets are matched to routes using the destination. The destination can be an IP address, a virtual network gateway, a virtual appliance, or the internet. If a matching route can't be found, then the packet is dropped.

# Identify User-Defined Routes

Azure automatically handles all network traffic routing. But, what if you want to do something different? For example, you may have a VM that performs a network function, such as routing, firewalling, or WAN optimization. You may want certain subnet traffic to be directed to this virtual appliance. For example, you might place an appliance between subnets or a subnet and the internet.



In these situations, you can configure user-defined routes (UDRs). UDRs control network traffic by defining routes that specify the next hop of the traffic flow. The hop can be a virtual network gateway, virtual network, internet, or virtual appliance.

Each route table can be associated to multiple subnets, but a subnet can only be associated to a single route table.

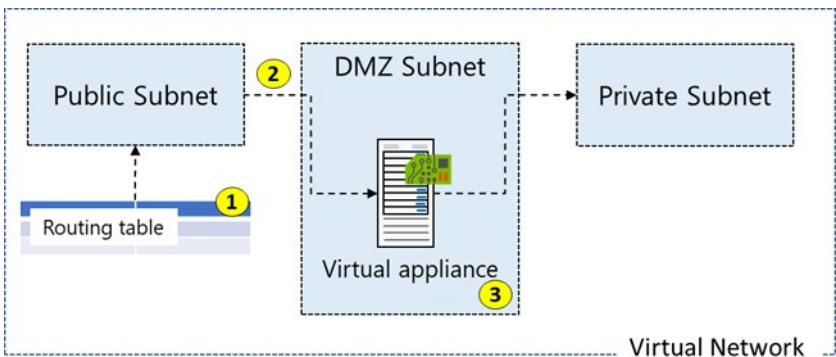
There are no charges for creating route tables in Microsoft Azure.

**Note:** Will you need to create custom routes?

## Examine a Routing Example

Let's review a specific network routing example. In this example, you have a virtual network that includes three subnets.

- The subnets are Private, DMZ, and Public. In the DMZ subnet, there is a network virtual appliance (NVA). NVAs are VMs that help with network functions like routing and firewall optimization.
- You want to ensure all traffic from the Public subnet goes through the NVA to the Private subnet.



## Create a Routing Table

Creating a routing table is straightforward. You provide **Name**, **Subscription**, **Resource Group**, and **Location**. You also decide to use **Virtual network gateway route propagation**.

**Create route table**

You can add routes to this table after it's created.

\* Name  
myRouteTablePublic

\* Subscription  
Visual Studio Enterprise

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

\* Location  
(US) West US

Virtual network gateway route propagation  
  Enabled

[Automation options](#)

Routes are automatically added to the route table for all subnets with Virtual network gateway propagation enabled. When you are using ExpressRoute, propagation ensures all subnets get the routing information.

## Create a Custom Route

For our example,

- The new route is named *ToPrivateSubnet*.
- The Private subnet is at 10.0.1.0/24.
- The route uses a virtual appliance. Notice the other choices for *Next hop type*: virtual network gateway, virtual network, internet, and none.
- The virtual appliance is located at 10.0.2.4.

**Add route**

myRouteTablePublic

Route name \*

ToPrivateSubnet ✓

Address prefix \* ⓘ

10.0.1.0/24 ✓

Next hop type ⓘ

Virtual network gateway ^

Virtual network gateway

Virtual network

Internet

Virtual appliance

None

In summary, this route applies to any address prefixes in 10.0.1.0/24 (private subnet). Traffic headed to these addresses will be sent to the virtual appliance with a 10.0.2.4 address.

## Associate the Route Table

The last step in our example is to associate the Public subnet with the new routing table. Each subnet can have zero or one route table associated to it.

**Add subnet**

VNet1

Name \*

Public ✓

Address range (CIDR block) \* ⓘ

10.0.1.0/24 ✓  
10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

NAT gateway ⓘ

None

Add IPv6 address space

Network security group

None

Route table

myRouteTablePublic ✓

**Note:** By default, using system routes traffic would go directly to the private subnet. However, with a user-defined route you can force the traffic through the virtual appliance.

**Note:** In this example, the virtual appliance shouldn't have a public IP address and IP forwarding should be enabled.

# Demonstration - Custom Routing Tables

In this demonstration, we will learn how to create a route table, define a custom route, and associate the route with a subnet.

**Note:** This demonstration requires a virtual network with at least one subnet.

## Create a routing table

1. Access the Azure portal.
2. Navigate to **Route tables**.
3. Select **+ Create**.
  - **Name:** *myRouteTablePublic*
  - **Subscription:** *select your subscription*
  - **Resource group:** *create or select a resource group*
  - **Region:** *select your location*
  - **Virtual network gateway route propagation:** *Enabled*
4. Select **Create**.
5. Wait for the new routing table to be deployed.

## Add a route

1. Select your new routing table, and then select **Routes**.
2. Select **+ Add**.
  - **Name:** *ToPrivateSubnet*
  - **Address prefix:** *10.0.1.0/24*
  - **Next hop type:** *Virtual appliance*
  - **Next hop address:** *10.0.2.4*
3. Read the information and ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.
4. Select **Create**.
5. Wait for the new route to be deployed.

## Associate a route table to a subnet

1. Navigate to the subnet you want to associate with the routing table.
2. Select **Route table**.
3. Select your new routing table, **myRouteTablePublic**.
4. **Save** your changes.

## Use PowerShell to view your routing information

1. Open the Cloud Shell.
2. View information about your new routing table.

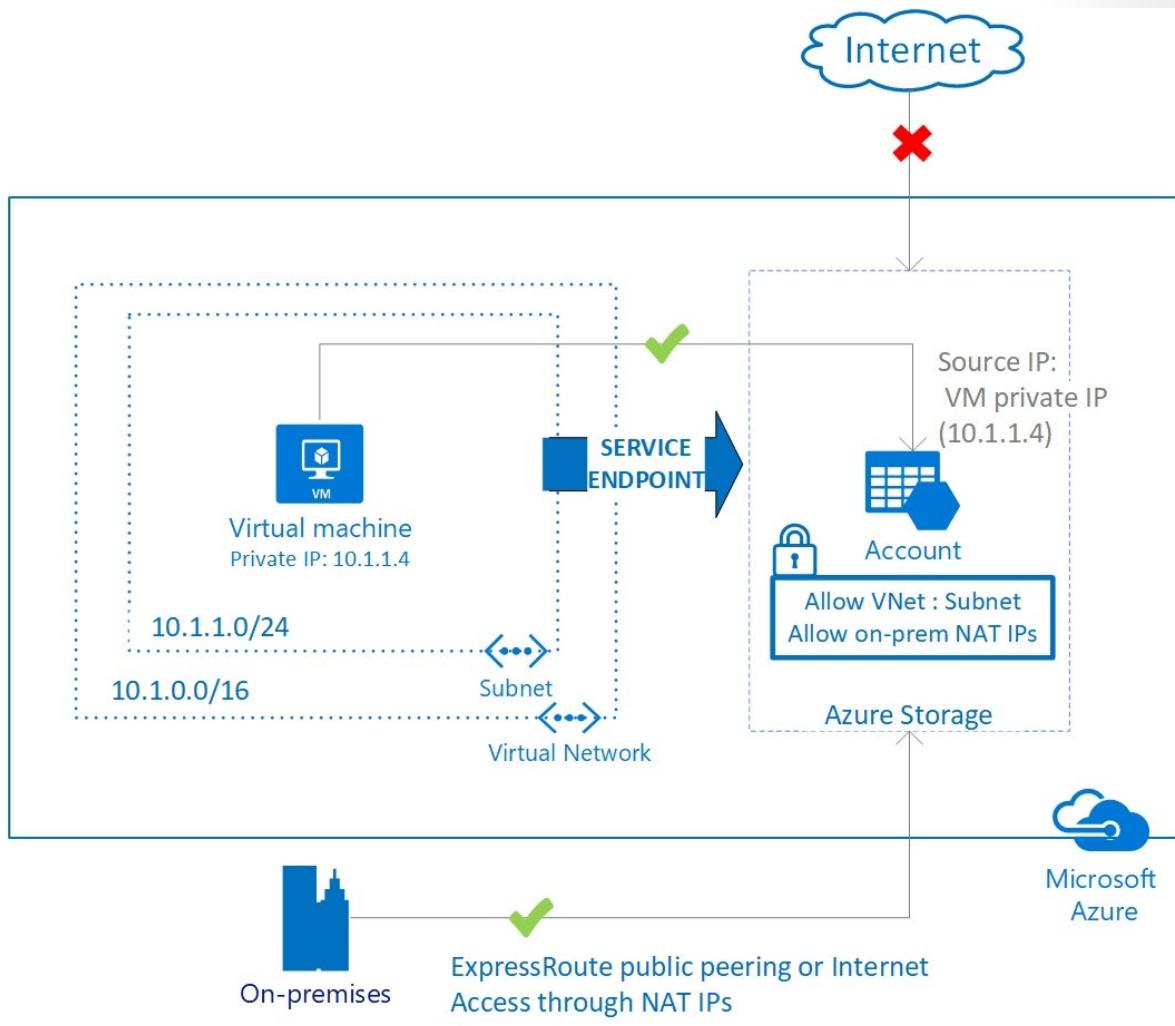
```
Get-AzRouteTable
```

- Verify the **Routes** and **Subnet** information is correct.

## Determine Service Endpoint Uses

A virtual network service endpoint provides the identity of your virtual network to the Azure service. Once service endpoints are enabled in your virtual network, you can secure Azure service resources to your virtual network by adding a virtual network rule to the resources.

Today, Azure service traffic from a virtual network uses public IP addresses as source IP addresses. With service endpoints, service traffic switches to use virtual network private addresses as the source IP addresses when accessing the Azure service from a virtual network. This switch allows you to access the services without the need for reserved, public IP addresses used in IP firewalls.



## Why use a service endpoint?

- Improved security for your Azure service resources.** VNet private address spaces can be overlapping and so, cannot be used to uniquely identify traffic originating from your VNet. Service endpoints secure Azure service resources to your virtual network by extending VNet identity to the service. When service endpoints are enabled in your virtual network, you secure Azure service resources to

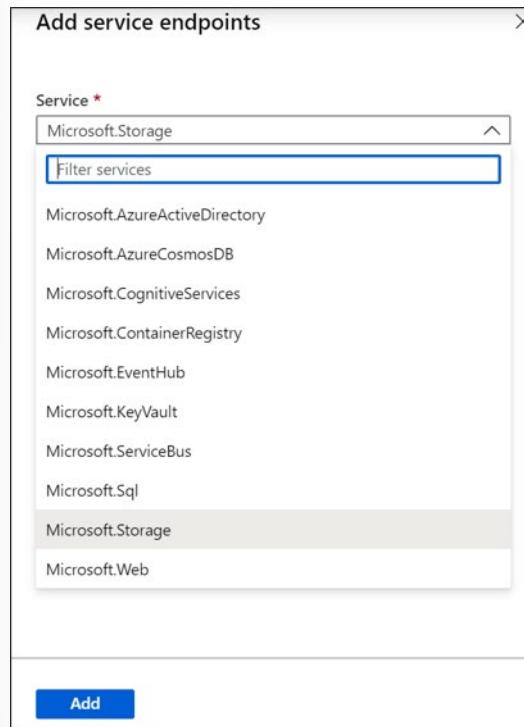
your virtual network by adding a virtual network rule. The rule improves security by fully removing public Internet access to resources, and allowing traffic only from your virtual network.

- **Optimal routing for Azure service traffic from your virtual network.** Today, any routes in your virtual network that force Internet traffic to your premises and/or virtual appliances, known as forced-tunneling, also force Azure service traffic to take the same route as the Internet traffic. Service endpoints provide optimal routing for Azure traffic.
- **Endpoints always take service traffic directly from your virtual network to the service on the Microsoft Azure backbone network.** Keeping traffic on the Azure backbone network allows you to continue auditing and monitoring outbound Internet traffic from your virtual networks, through forced-tunneling, without impacting service traffic. Learn more about user-defined routes and forced-tunneling.
- **Simple to set up with less management overhead.** You no longer need reserved, public IP addresses in your virtual networks to secure Azure resources through IP firewall. There are no NAT or gateway devices required to set up the service endpoints. Service endpoints are configured through the subnet. There is no additional overhead to maintaining the endpoints.

**Note:** With service endpoints, the virtual machine IP addresses switches from public to private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch. Ensure Azure service firewall rules allow for this switch before setting up service endpoints. You may also experience temporary interruption to service traffic from this subnet while configuring service endpoints.

## Determine Service Endpoint Services

It is easy to add a service endpoint to the virtual network. Several services are available including: Azure Active Directory, Azure Cosmos DB, EventHub, KeyVault, Service Bus, SQL, and Storage.



**Azure Storage.** Generally available in all Azure regions. This endpoint gives traffic an optimal route to the Azure Storage service. Each storage account supports up to 100 virtual network rules.

**Azure SQL Database and Azure SQL Data Warehouse.** Generally available in all Azure regions. A firewall security feature that controls whether the database server for your single databases and elastic pool in Azure SQL Database or for your databases in SQL Data Warehouse accepts communications that are sent from particular subnets in virtual networks.

**Azure Database for PostgreSQL server and MySQL.** Generally available in Azure regions where database service is available. Virtual Network (VNet) services endpoints and rules extend the private address space of a Virtual Network to your Azure Database for PostgreSQL server and MySQL server.

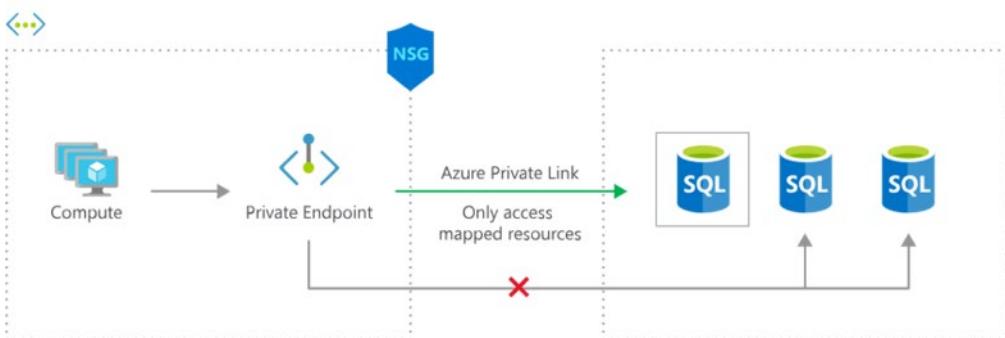
**Azure Cosmos DB.** Generally available in all Azure regions. You can configure the Azure Cosmos account to allow access only from a specific subnet of virtual network (VNet). By enabling Service endpoint to access Azure Cosmos DB on the subnet within a virtual network, the traffic from that subnet is sent to Azure Cosmos DB with the identity of the subnet and Virtual Network. Once the Azure Cosmos DB service endpoint is enabled, you can limit access to the subnet by adding it to your Azure Cosmos account.

**Azure Key Vault.** Generally available in all Azure regions. The virtual network service endpoints for Azure Key Vault allow you to restrict access to a specified virtual network. The endpoints also allow you to restrict access to a list of IPv4 (internet protocol version 4) address ranges. Any user connecting to your key vault from outside those sources is denied access.

**Azure Service Bus and Azure Event Hubs.** Generally available in all Azure regions. The integration of Service Bus with Virtual Network (VNet) service endpoints enables secure access to messaging capabilities from workloads like virtual machines that are bound to virtual networks, with the network traffic path being secured on both ends.

**Note:** Adding service endpoints can take up to 15 minutes to complete. Each service endpoint integration has its own Azure documentation page.

## Identify Private Link Uses



Azure Private Link provides private connectivity from a virtual network to Azure platform as a service (PaaS), customer-owned, or Microsoft partner services. It simplifies the network architecture and secures the connection between endpoints in Azure by eliminating data exposure to the public internet.

- **Private connectivity to services on Azure.** Traffic remains on the Microsoft network, with no public internet access. Connect privately to services running in other Azure regions. Private Link is global and has no regional restrictions.
- **Integration with on-premises and peered networks.** Access private endpoints over private peering or VPN tunnels from on-premises or peered virtual networks. Microsoft hosts the traffic, so you don't need to set up public peering or use the internet to migrate your workloads to the cloud.

- **Protection against data exfiltration for Azure resources.** Use Private Link to map private endpoints to Azure PaaS resources. When there is a security incident within your network, only the mapped resource would be accessible, eliminating the threat of data exfiltration.
- **Services delivered directly to your customers' virtual networks.** Privately consume Azure PaaS, Microsoft partner, and your own services in your virtual networks on Azure. Private Link works across Azure Active Directory (Azure AD) tenants to help unify your experience across services. Send, approve, or reject requests directly, without permissions or role-based access controls.

## How it works

Use Private Link to bring services delivered on Azure into your private virtual network by mapping it to a private endpoint. Or privately deliver your own services in your customers' virtual networks. All traffic to the service can be routed through the private endpoint, so no gateways, NAT devices, ExpressRoute or VPN connections, or public IP addresses are needed. Private Link keeps traffic on the Microsoft global network.

## Knowledge Check

Choose the best response for each question.

### Multiple choice

*Your company wants to redirect Internet traffic to your company's on-premises servers for packet inspection. Which of the following is not used for this? Select one.*

- User Defined Routes
- Forced Tunneling
- System Routes

### Multiple choice

*Why would you use a custom route in a virtual network? Select one.*

- To load balance the traffic within your virtual network.
- To connect to resources in another virtual network hosted in Azure.
- To control the flow of traffic within your Azure virtual network.

### Multiple choice

*When creating user-defined routes, you can specify any of these next hop types, except? Select one.*

- Internet
- Load Balancer
- Virtual Appliance

## Multiple choice

Your company needs to extend their private address space in Azure by providing a direct connection to your Azure resources. They implement which of the following? Select one.

- User-defined route
- Virtual appliance
- Virtual network endpoint

## Multiple choice

What is the main benefit of using a network virtual appliance?

- To control who can access Azure resources from the perimeter network.
- To control incoming traffic from the perimeter network and allow only traffic that meets security requirements to pass through.
- To control outbound access to the internet

## Summary and Resources

### Summary

Network routes control the flow of traffic through your network. You can customize these routes, implement service endpoints, and private links.

You should now be able to:

- Implement system routes and user-defined routes.
- Configure a custom route.
- Implement service endpoints.
- Identify features and usage cases for private links and endpoint services.

### Learn more

You can learn more by reviewing the following.

- **Virtual network traffic routing documentation<sup>2</sup>**
- **Learn - Manage and control traffic flow in your Azure deployment with routes<sup>3</sup>**

<sup>2</sup> <https://docs.microsoft.com/azure/virtual-network/virtual-networks-udr-overview>

<sup>3</sup> <https://docs.microsoft.com/learn/modules/control-network-traffic-flow-with-routes/>

# Configure Azure Load Balancer

## Introduction

### Scenario

Many apps need to be resilient to failure and scale easily when demand increases. You can address those needs by using Azure Load Balancer.

Suppose you work for a healthcare organization that's launching a new portal application in which patients can schedule appointments. The application has a patient portal and web application front end and a business tier database. The database is used by the front end to retrieve and save patient information.

The new portal needs to be available around the clock to handle failures. The portal must adjust to fluctuations in load by adding and removing resources to match the load. The organization needs a solution that distributes work to virtual machines across the system as virtual machines are added. The solution should detect failures and reroute jobs to virtual machines as needed. Improved resiliency and scalability helps ensure that patients can schedule appointments from any location.

You must distribute incoming network traffic across a group of back-end resources or services such as virtual machines (VMs). You must scale your applications while maintaining throughput and keeping response times low.

### Skills measured

Configuring load-balancing is part of **Exam AZ-104: Microsoft Azure Administrator<sup>4</sup>**.

Configure and manage virtual networking (25–30%)

Configure load balancing

- Configure an internal or public load balancer.
- Troubleshoot load-balancing.

### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for Azure load balancer.
- Implement public and internal Azure load balancers.
- Configure load balancer SKUs, backend pools, session persistence, and health probes.

### Prerequisites

None.

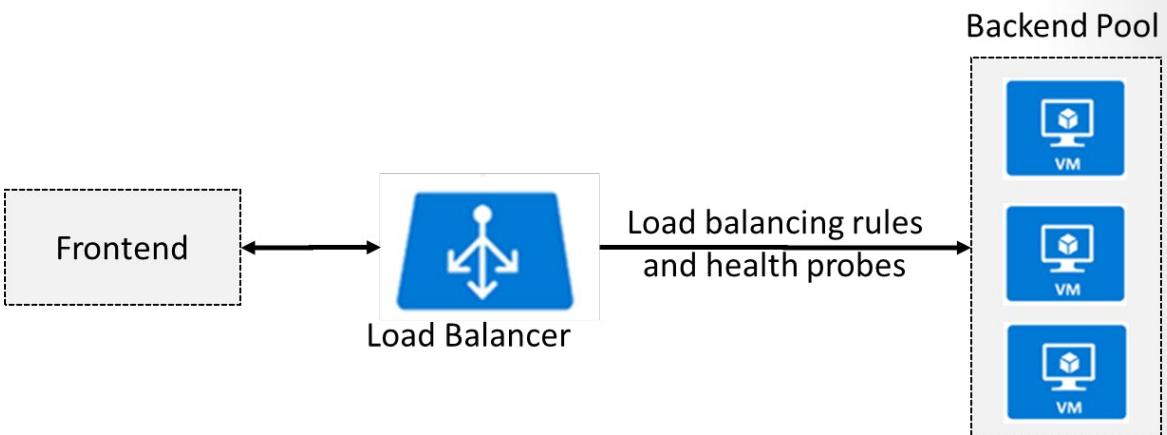
---

<sup>4</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

## Determine Azure Load Balancer Uses

The Azure Load Balancer delivers high availability and network performance to your applications. The load balancer distributes inbound traffic to backend resources using load-balancing rules and health probes.

- Load-balancing rules determine how traffic is distributed to the backend.
- Health probes ensure the resources in the backend are healthy.



The Load Balancer can be used for inbound and outbound scenarios and scales up to millions of TCP and UDP application flows.

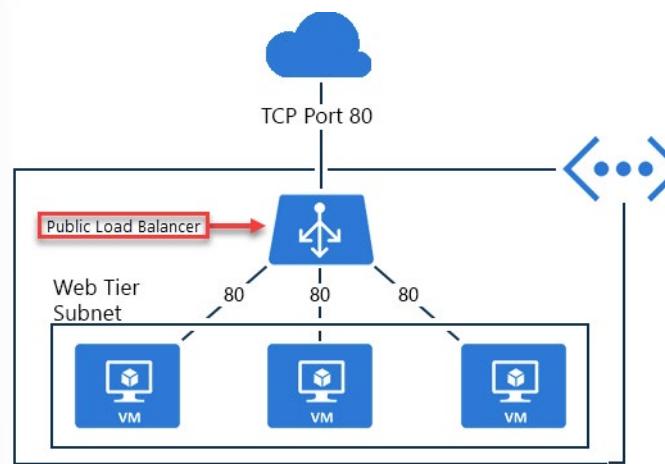
**Note:** Keep this diagram in mind since it covers the four components that must be configured for your load balancer: **Frontend IP configuration**, **Backend pools**, **Health probes**, and **Load-balancing rules**.

## Implement a Public Load Balancer

There are two types of load balancers: **public** and **internal**.

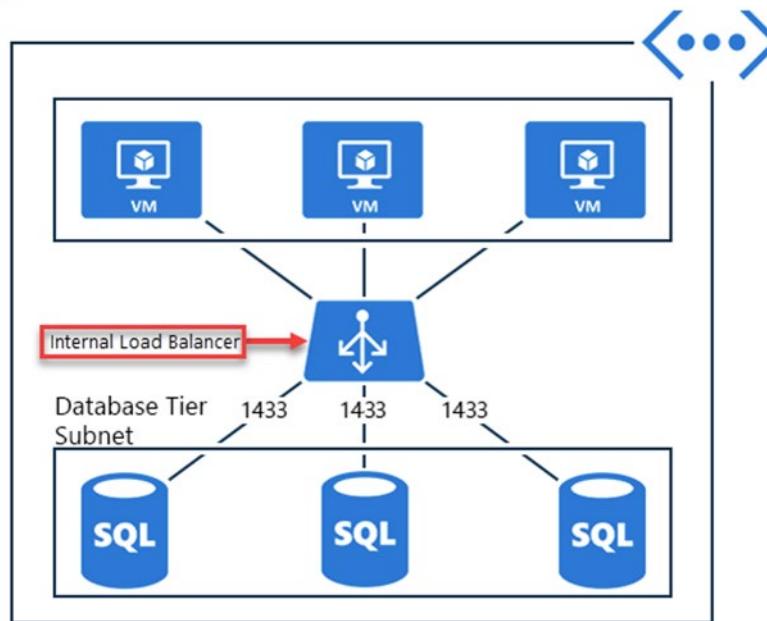
A public load balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the VM. Mapping is also provided for the response traffic from the VM. By applying load-balancing rules, you can distribute specific types of traffic across multiple VMs or services. For example, you can spread the load of incoming web request traffic across multiple web servers.

The diagram shows internet clients sending webpage requests to the public IP address of a web app on TCP port 80. Azure Load Balancer distributes the requests across the three VMs in the load-balanced set.



## Implement an Internal Load Balancer

An internal load balancer directs traffic to resources that are inside a virtual network or that use a VPN to access Azure infrastructure. Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint. Internal line-of-business applications run in Azure and are accessed from within Azure or from on-premises resources. For example, an internal load balancer could receive database requests that need to be distributed to backend SQL servers.



An internal load balancer enables the following types of load balancing:

- **Within a virtual network.** Load balancing from VMs in the virtual network to a set of VMs that reside within the same virtual network.
- **For a cross-premises virtual network.** Load balancing from on-premises computers to a set of VMs that reside within the same virtual network.

- **For multi-tier applications.** Load balancing for internet-facing multi-tier applications where the backend tiers are not internet-facing. The backend tiers require traffic load-balancing from the internet-facing tier.
- **For line-of-business applications.** Load balancing for line-of-business applications that are hosted in Azure without additional load balancer hardware or software. This scenario includes on-premises servers that are in the set of computers whose traffic is load-balanced.

**Note:** A public load balancer could be placed in front of the internal load balancer to create a multi-tier application.

## Determine Load Balancer SKUs

When you create an Azure Load Balancer, you select the type (Internal or Public) of load balancer. You also select the SKU. The load balancer supports both Basic and Standard SKUs, each differing in scenario scale, features, and pricing. The Standard Load Balancer is the newer Load Balancer product with an expanded and more granular feature set over Basic Load Balancer. It is a superset of Basic Load Balancer.

Instance details

Name \*  ✓

Region \*  ▼

Type \*  ⓘ  
 Internal  Public

SKU \*  ⓘ  
 Basic  Standard

Configure virtual network.

Virtual network \*  ⓘ  
 ▼

Subnet \*  ▼  
[Manage subnet configuration](#)

IP address assignment \*  
 Static  Dynamic

## Capabilities

| Feature             | Basic SKU           | Standard SKU                                                         |
|---------------------|---------------------|----------------------------------------------------------------------|
| Backend pools       | Up to 300 instances | Up to 1000 instances                                                 |
| Health probes       | HTTP, TCP           | HTTPS, HTTP, TCP                                                     |
| Availability zones  | Not available       | Zone-redundant and zonal frontends for inbound and outbound traffic. |
| Multiple front ends | Inbound only        | Inbound and outbound                                                 |

| Feature           | Basic SKU                      | Standard SKU                                                                                                                          |
|-------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Secure by default | Open by default. NSG optional. | Closed to inbound flows unless allowed by an NSG. Internal traffic from the virtual network to the internal load balancer is allowed. |
| SLA               | Not available                  | 99.99%                                                                                                                                |

**Note:** The Basic SKU can be upgraded to the Standard SKU. But, new designs and architectures should use the Standard Load Balancer.

## Create Backend Pools

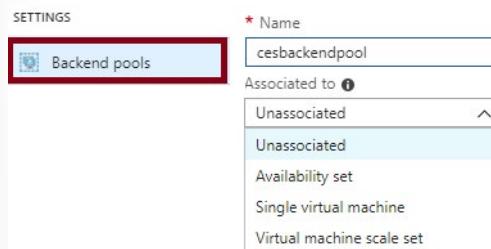
To distribute traffic, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer.



How you configure the backend pool depends on whether you are using the Standard or Basic SKU.

|                        | Standard SKU                                                                                        | Basic SKU                                                      |
|------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Backend pool endpoints | Any VM in a single virtual network, including a blend of VMs, availability sets, and VM scale sets. | VMs in a single availability set or virtual machine scale set. |

Backend pools are configured from the Backend Pool blade. For the Standard SKU you can connect to an Availability set, single virtual machine, or a virtual machine scale set.



**Note:** In the Standard SKU, you can have up to 1000 instances in the backend pool. In the Basic SKU, you can have up to 300 instances.

## Create Load Balancer Rules

A load balancer rule defines how traffic is distributed to the backend pool. The rule maps a given front-end IP and port combination to a set of back-end IP addresses and port combination. Before configuring the rule, create the front-end, back-end, and health probe. This diagram shows a rule that routes front-end

TCP connections to a set of backend web (port 80) servers. The rule uses a health probe that checks on HTTP port 80.

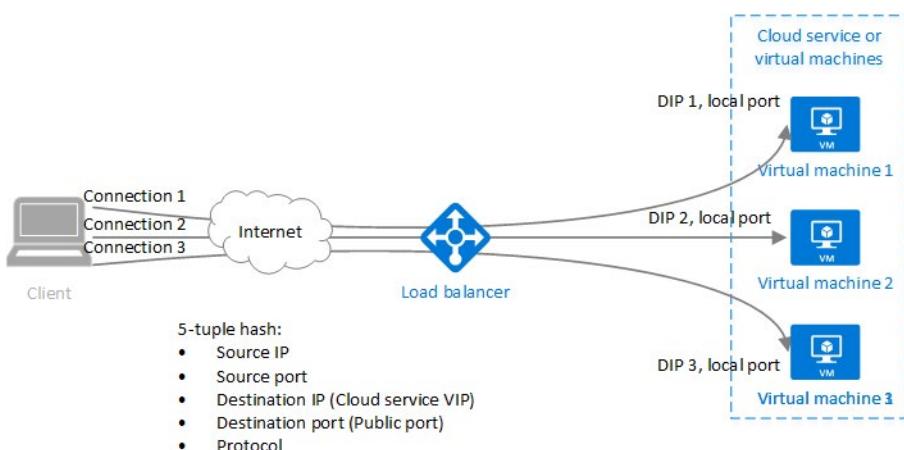
The screenshot shows the 'Add load balancing rule' configuration dialog. The fields are as follows:

- Name \***: lbr01
- IP Version \***: IPv4
- Frontend IP address \***: 10.1.0.4 (LoadBalancerFrontEnd)
- Protocol**: TCP
- Port \***: 80
- Backend port \***: 80
- Backend pool**: bep01
- Health probe**: hp01 (HTTP:80)
- Session persistence**: None
- Idle timeout (minutes)**: 4
- Floating IP (direct server return)**: Enabled

Load balancing rules can be used in combination with NAT rules. For example, you could use NAT from the load balancer's public address to TCP 3389 on a specific virtual machine. This allows remote desktop access from outside of Azure.

## Configure Session Persistence

By default, Azure Load Balancer distributes network traffic equally among multiple VM instances. The load balancer uses a five-tuple (source IP, source port, destination IP, destination port, and protocol type) hash to map traffic to available servers. It provides stickiness only within a transport session.



Session persistence specifies how traffic from a client should be handled. The default behavior (None) is that successive requests from a client may be handled by any virtual machine. You can change this behavior.

- **None (default)** specifies any virtual machine can handle the request.
- **Client IP** specifies that successive requests from the same client IP address will be handled by the same virtual machine.
- **Client IP and protocol** specifies that successive requests from the same client IP address and protocol combination will be handled by the same virtual machine.

**Note:** Keeping session persistence information is important in applications that use a shopping cart. Can you think of any other applications?

## Create Health Probes

A health probe allows the load balancer to monitor the status of your app. The health probe dynamically adds or removes VMs from the load balancer rotation based on their response to health checks. When a probe fails to respond, the load balancer stops sending new connections to the unhealthy instances.

There are two main ways to configure health probes **HTTP** and **TCP**.

The screenshot shows a configuration dialog for adding a health probe named 'hp01'. The fields are as follows:

- Name \***: hp01
- Protocol**: HTTP
- Port \***: 80
- Path \***: /
- Interval \***: 5 seconds
- Unhealthy threshold \***: 2 consecutive failures

**HTTP custom probe.** The load balancer regularly probes your endpoint (every 15 seconds, by default). The instance is healthy if it responds with an HTTP 200 within the timeout period (default of 31 seconds). Any status other than HTTP 200 causes the probe to fail. You can specify the port (Port), the URI for requesting the health status from the backend (URI), amount of time between probe attempts (Interval), and the number of failures that must occur for the instance to be considered unhealthy (Unhealthy threshold).

**TCP custom probe.** This probe relies on establishing a successful TCP session to a defined probe port. If the specified listener on the VM exists, the probe succeeds. If the connection is refused, the probe fails. You can specify the Port, Interval, and Unhealthy threshold.

**Note:** There is also a guest agent probe. This probe uses the guest agent inside the VM. It is not recommended when HTTP or TCP custom probe configurations are possible.

# Knowledge Check

Choose the best response for each question.

## Multiple choice

*Your company provides customers a virtual network in the cloud. You have dozens of Linux virtual machines in another virtual network. You need to install an Azure load balancer to direct traffic between the virtual networks. What should you do? Select one.*

- Install an external load balancer.
- Install an internal load balancer.
- Install a public load balancer.

## Multiple choice

*Your company has a popular regional web site. The company plans to move it to Microsoft Azure and host it in the Canada East region. The web team has established the following requirements for managing the web traffic: -Evenly distribute incoming web requests across a farm of 10 Azure VMs. -Support many incoming requests, including spikes during peak times. -Minimize complexity. -Minimize ongoing costs. Which of the following would you select for this scenario? Select one.*

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

## Multiple choice

*What is the default distribution type for traffic through a load balancer? Select one.*

- Source IP affinity
- Five-tuple hash
- Three-tuple hash

## Multiple choice

*Which configuration is required to configure an internal load balancer?*

- Virtual machines should be in the same virtual network.
- Virtual machines must be publicly accessible.
- Virtual machines must be in an availability set.

## Multiple choice

Which of the following statement about external load balancers is correct?

- They have a private, front-facing IP address.
- They don't have a listener IP address.
- They have a public IP address.

## Summary and Resources

### Summary

Many apps need to be resilient to failure and scale easily when demand increases. You can address those needs by using Azure Load Balancer.

You should now be able to:

- Identify features and usage cases for Azure load balancer.
- Implement public and internal Azure load balancers.
- Configure load balancer SKUs, backend pools, session persistence, and health probes.

### Learn more

You can learn more by reviewing the following.

- **Load Balancer documentation<sup>5</sup>**
- **Learn - Improve application scalability and resiliency by using Azure Load Balancer<sup>6</sup>**

---

<sup>5</sup> <https://docs.microsoft.com/azure/load-balancer/>

<sup>6</sup> <https://docs.microsoft.com/learn/modules/improve-app-scalability-resiliency-with-load-balancer/>

# Configure Azure Application Gateway

## Introduction

### Scenario

Imagine you work for the motor vehicle department of a governmental organization. The department runs several public websites that enable drivers to register their vehicles, and renew their driver's license online.

The vehicle registration website has been running on a single server, and has suffered multiple outages because of server failures. This has resulted in frustrated drivers trying to register their vehicles by month's end before their registrations expire.

You would like to improve resiliency by adding multiple web servers to its site, and distribute the load across them. You would also like to centralize their site on a single load-balancing service. This will simplify the URLs for site visitors.

### Skills measured

Configure the Azure Application Gateway is part of **Exam AZ-104: Microsoft Azure Administrator<sup>7</sup>**.

Configure and manage virtual networking (25–30%)

Configure load balancing

- Configure Azure Application gateway.

### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for Azure Application Gateway.
- Implement Azure Application Gateway, including selecting a routing method.
- Configure gateway features such as routing rules.

### Prerequisites

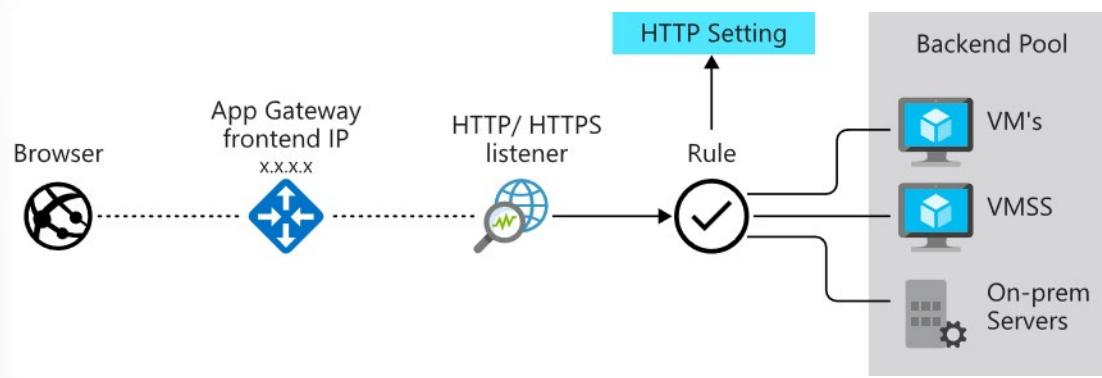
None.

## Implement Application Gateway

Application Gateway manages the requests that client applications send to a web app.

The Application Gateway uses application layer routing. Application layer routing routes traffic to a pool of web servers based on the URL of a request. The back-end pool can include Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers.

<sup>7</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>



The Application Gateway uses round robin to send load balance requests to the servers in each back-end pool. The Application Gateway provides session stickiness. Use session stickiness to ensure client requests in the same session are routed to the same back-end server.

Load-balancing works in the OSI Layer 7. Load-balancing requests use the routing parameters (host names and paths) in the Application Gateway rules. In comparison, the Azure Load Balancer, functions at the OSI Layer 4 level. This means the Azure Load Balancer distributes traffic based on the IP address of the target of a request.

## Additional features

- Support for the HTTP, HTTPS, HTTP/2 and WebSocket protocols.
- A web application firewall to protect against web application vulnerabilities.
- End-to-end request encryption.
- Autoscaling, to dynamically adjust capacity as your web traffic load change.

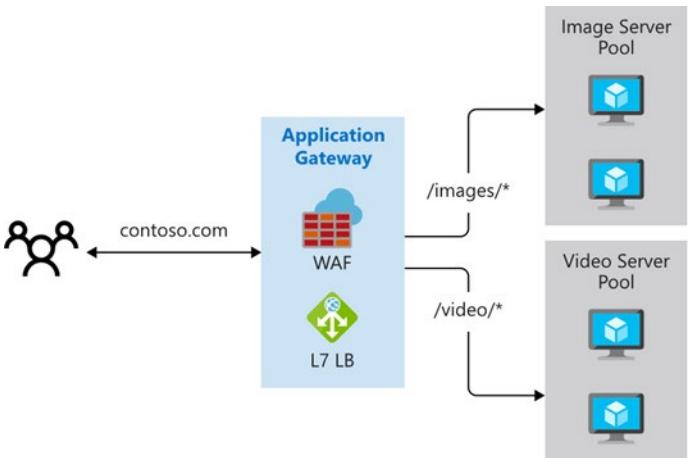
## Determine Application Gateway Routing

Clients send requests to your web apps to the IP address or DNS name of the gateway. The gateway routes requests to a selected web server in the back-end pool, using a set of rules configured for the gateway to determine where the request should go.

There are two primary methods of routing traffic, path-based routing and multiple site routing.

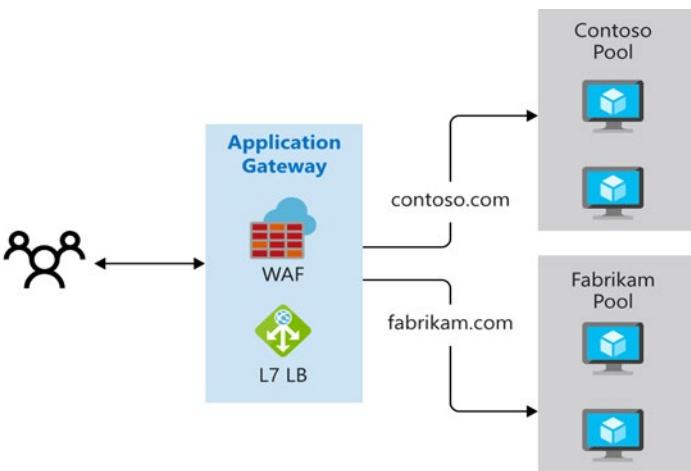
### Path-based routing

Path-based routing sends requests with different URL paths different pools of back-end servers. For example, you could direct requests with the path /video/\* to a back-end pool containing servers that are optimized to handle video streaming, and direct /images/\* requests to a pool of servers that handle image retrieval.



## Multiple site routing

Multiple site routing configures more than one web application on the same application gateway instance. In a multi-site configuration, you register multiple DNS names (CNAMEs) for the IP address of the Application Gateway, specifying the name of each site. Application Gateway uses separate listeners to wait for requests for each site. Each listener passes the request to a different rule, which can route the requests to servers in a different back-end pool. For example, you could direct all requests for `http://contoso.com` to servers in one back-end pool, and requests for `http://fabrikam.com` to another back-end pool. The following diagram shows this configuration.



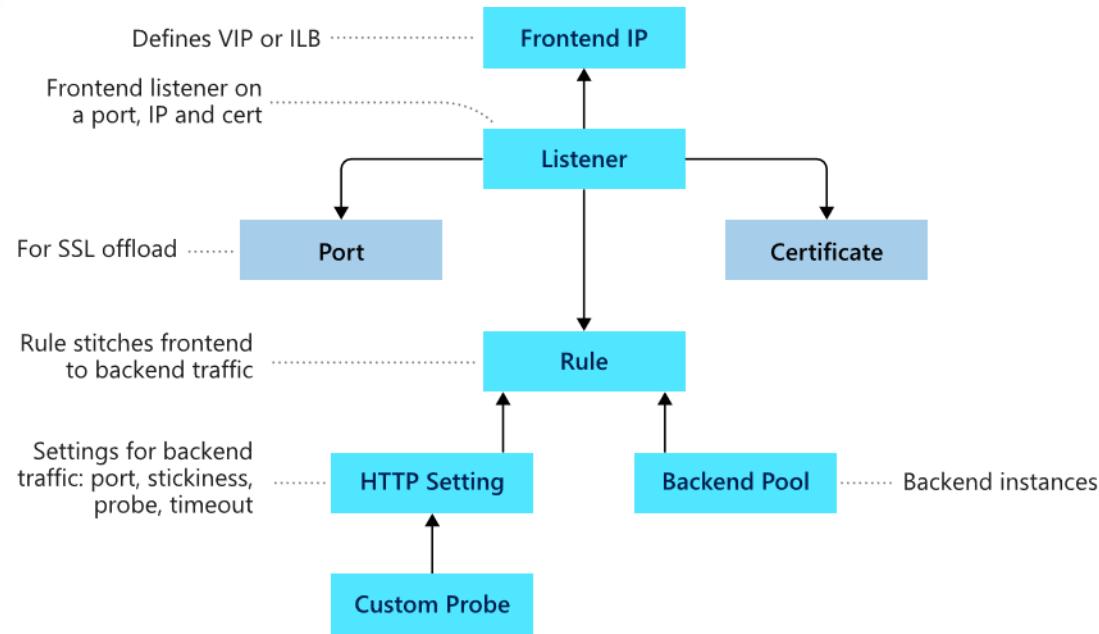
Multi-site configurations are useful for supporting multi-tenant applications, where each tenant has its own set of virtual machines or other resources hosting a web application.

## Other features

- **Redirection.** Redirection can be used to another site, or from HTTP to HTTPS.
- **Rewrite HTTP headers.** HTTP headers allow the client and server to pass parameter information with the request or the response.
- **Custom error pages.** Application Gateway allows you to create custom error pages instead of displaying default error pages. You can use your own branding and layout using a custom error page.

# Setup Application Gateway Components

Application Gateway has a series of components that combine to route requests to a pool of web servers and to check the health of these web servers.



## Front-end IP address

Client requests are received through a front-end IP address. You can configure Application Gateway to have a public IP address, a private IP address, or both. Application Gateway can't have more than one public and one private IP address.

## Listeners

Application Gateway uses one or more listeners to receive incoming requests. A listener accepts traffic arriving on a specified combination of protocol, port, host, and IP address. Each listener routes requests to a back-end pool of servers following routing rules that you specify. A listener can be Basic or Multi-site. A Basic listener only routes a request based on the path in the URL. A Multi-site listener can also route requests using the hostname element of the URL.

Listeners also handle TLS/SSL certificates for securing your application between the user and Application Gateway.

## Routing rules

A routing rule binds a listener to the back-end pools. A rule specifies how to interpret the hostname and path elements in the URL of a request, and then direct the request to the appropriate back-end pool. A routing rule also has an associated set of HTTP settings. These HTTP settings indicate whether (and how) traffic is encrypted between Application Gateway and the back-end servers. Other configuration information includes Protocol, Session stickiness, Connection draining, Request timeout period, and Health probes.

## Back-end pools

A back-end pool references a collection of web servers. You provide the IP address of each web server and the port on which it listens for requests when configuring the pool. Each pool can specify a fixed set of virtual machines, a virtual machine scale-set, an app hosted by Azure App Services, or a collection of on-premises servers. Each back-end pool has an associated load balancer that distributes work across the pool.

## Web application firewall

The web application firewall (WAF) is an optional component that handles incoming requests before they reach a listener. The web application firewall checks each request for many common threats, based on the Open Web Application Security Project (OWASP). Common threats include SQL-injection, Cross-site scripting, Command injection, HTTP request smuggling, HTTP response splitting, Remote file inclusion, Bots, crawlers, and scanners, and HTTP protocol violations and anomalies.

OWASP has defined a set of generic rules for detecting attacks. These rules are referred to as the Core Rule Set (CRS). The rule sets are under continuous review as attacks evolve in sophistication. WAF supports two rule sets, CRS 2.2.9 and CRS 3.0. CRS 3.0 is the default and more recent of these rule sets. If necessary, you can opt to select only specific rules in a rule set, targeting certain threats. Additionally, you can customize the firewall to specify which elements in a request to examine, and limit the size of messages to prevent massive uploads from overwhelming your servers.

WAF is enabled on your Application Gateway by selecting the WAF tier when you create a gateway.

## Health probes

Health probes determine which servers are available for load-balancing in a back-end pool. The Application Gateway uses a health probe to send a request to a server. When the server returns an HTTP response with a status code between 200 and 399, the server is considered healthy.

If you don't configure a health probe, Application Gateway creates a default probe that waits for 30 seconds before deciding that a server is unavailable.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Which criteria does Application Gateway use to route requests to a web server? Select one.*

- The hostname, port, and path in the URL of the request.
- The region in which the servers hosting the web application are located.
- The users authentication information.

## Multiple choice

*Which load balancing strategy does the Application Gateway implement? Select one.*

- Distributes requests to each available server in a backend pool in turn, round-robin.
- Distributes requests to the server in the backend pool with the lightest load.
- Polls each server in the backend pool in turn, and sends the request to the first server that responds.

## Multiple choice

*Your company has a website that allows users to customize their experience by downloading an app. Demand for the app has increased so you have added another virtual network with two virtual machines. These machines are dedicated to serving the app downloads. You need to ensure the additional download requests do not affect the website performance. Your solution must route all download requests to the two new servers you have installed. What action will you recommend? Select one.*

- Add a user-defined route.
- Create a local network gateway.
- Add an application gateway.

## Multiple choice

*You are deploying the Application Gateway and want to ensure incoming requests are checked for common security threats like cross-site scripting and crawlers. To address your concerns what should you do? Select one.*

- Install an internal load balancer
- Install Azure Firewall
- Install the Web Application Firewall

## Summary and Resources

### Summary

The Application Gateway provides load balancing and application routing capabilities across multiple web sites. Several routing methods are available including path-based routing. Also, the Application Gateway includes the Web Application Firewall with built-in security features.

You should now be able to:

- Identify features and usage cases for Azure Application Gateway.
- Implement Azure Application Gateway, including selecting a routing method.
- Configure gateway features such as routing rules.

## Learn more

You can learn more by reviewing the following.

- **What is Azure Application Gateway<sup>8</sup>.**
- **Learn - Load balance your web service traffic with Application Gateway<sup>9</sup>**
- **Learn - Introduction to Azure Web Application Firewall<sup>10</sup>**

---

<sup>8</sup> <https://docs.microsoft.com/azure/application-gateway/overview>

<sup>9</sup> <https://docs.microsoft.com/learn/modules/load-balance-web-traffic-with-application-gateway/>

<sup>10</sup> <https://docs.microsoft.com/en-us/learn/modules/introduction-azure-web-application-firewall/>

## Module 06 Lab

### Lab 06 - Implement Traffic Management

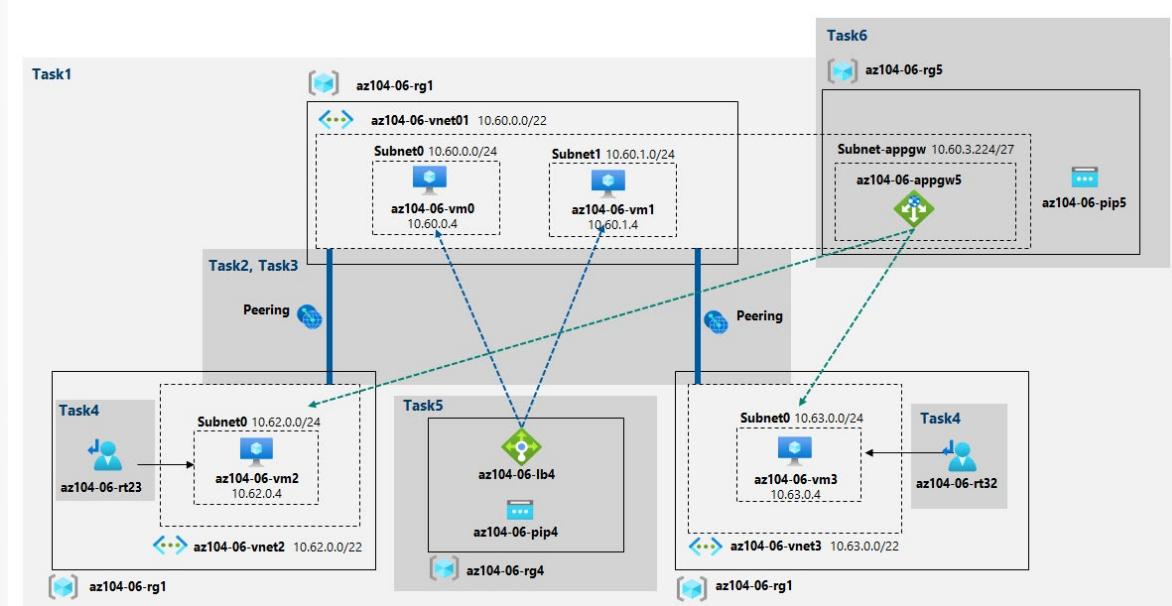
#### Lab scenario

You were tasked with testing managing network traffic targeting Azure virtual machines in the hub and spoke network topology, which Contoso considers implementing in its Azure environment (instead of creating the mesh topology, which you tested in the previous lab). This testing needs to include implementing connectivity between spokes by relying on user defined routes that force traffic to flow via the hub, as well as traffic distribution across virtual machines by using layer 4 and layer 7 load balancers. For this purpose, you intend to use Azure Load Balancer (layer 4) and Azure Application Gateway (layer 7).

#### Objectives

In this lab, you will:

- Task 1: Provision the lab environment.
- Task 2: Configure the hub and spoke network topology.
- Task 3: Test transitivity of virtual network peering.
- Task 4: Configure routing in the hub and spoke topology.
- Task 5: Implement Azure Load Balancer.
- Task 6: Implement Azure Application Gateway.



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Answers

## Multiple choice

Your company wants to redirect Internet traffic to your company's on-premises servers for packet inspection. Which of the following is not used for this? Select one.

- User Defined Routes
- Forced Tunneling
- System Routes

### Explanation

*System routes. Forced tunneling can redirect internet bound traffic back to the company's on-premises infrastructure. The redirection can be used to implement packet inspection or corporate audits. Forced tunneling in Azure is configured via virtual network user defined routes.*

## Multiple choice

Why would you use a custom route in a virtual network? Select one.

- To load balance the traffic within your virtual network.
- To connect to resources in another virtual network hosted in Azure.
- To control the flow of traffic within your Azure virtual network.

### Explanation

*To control the flow of traffic within your Azure virtual network. Custom routes are used to override the default Azure routing so that you can route traffic through a network virtual appliance.*

## Multiple choice

When creating user-defined routes, you can specify any of these next hop types, except? Select one.

- Internet
- Load Balancer
- Virtual Appliance

### Explanation

*Load balancer. The valid next hop choices are virtual appliance, virtual network gateway, virtual network, internet, and none.*

## Multiple choice

Your company needs to extend their private address space in Azure by providing a direct connection to your Azure resources. They implement which of the following? Select one.

- User-defined route
- Virtual appliance
- Virtual network endpoint

### Explanation

*Virtual network endpoint. Virtual network endpoints extend your private address space in Azure. Endpoints restrict the flow of traffic. As you enable service endpoints, Azure creates routes in the route table to direct this traffic.*

**Multiple choice**

What is the main benefit of using a network virtual appliance?

- To control who can access Azure resources from the perimeter network.
- To control incoming traffic from the perimeter network and allow only traffic that meets security requirements to pass through.
- To control outbound access to the internet

*Explanation*

*To control incoming traffic from the perimeter network and allow only traffic that meets security requirements to pass through. A network virtual appliance acts like a firewall. It checks all inbound and outbound traffic, and it secures your environment by allowing or denying the traffic.*

**Multiple choice**

Your company provides customers a virtual network in the cloud. You have dozens of Linux virtual machines in another virtual network. You need to install an Azure load balancer to direct traffic between the virtual networks. What should you do? Select one.

- Install an external load balancer.
- Install an internal load balancer.
- Install a public load balancer.

*Explanation*

*Install an internal load balancer. Azure has two types of load balancers: public and internal. An internal load balancer directs traffic only to resources that are inside a virtual network or that use a VPN to access Azure infrastructure.*

**Multiple choice**

Your company has a popular regional web site. The company plans to move it to Microsoft Azure and host it in the Canada East region. The web team has established the following requirements for managing the web traffic: -Evenly distribute incoming web requests across a farm of 10 Azure VMs. -Support many incoming requests, including spikes during peak times. -Minimize complexity. -Minimize ongoing costs. Which of the following would you select for this scenario? Select one.

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

*Explanation*

*Azure Load Balancer. In this scenario, the requirements call for load balancing of a web site with minimal complexity and costs.*

**Multiple choice**

What is the default distribution type for traffic through a load balancer? Select one.

- Source IP affinity
- Five-tuple hash
- Three-tuple hash

*Explanation*

*Five-tuple hash. The hash includes Source IP, Source port, Destination IP, Destination port, and Protocol type.*

**Multiple choice**

Which configuration is required to configure an internal load balancer?

- Virtual machines should be in the same virtual network.
- Virtual machines must be publicly accessible.
- Virtual machines must be in an availability set.

*Explanation*

*Virtual machines should be in the same virtual network. The virtual machines that you use a load balancer to distribute a load to must be in the same virtual network.*

**Multiple choice**

Which of the following statement about external load balancers is correct?

- They have a private, front-facing IP address.
- They don't have a listener IP address.
- They have a public IP address.

*Explanation*

*They have a public IP address. External load balancers have public IP addresses.*

**Multiple choice**

Which criteria does Application Gateway use to route requests to a web server? Select one.

- The hostname, port, and path in the URL of the request.
- The region in which the servers hosting the web application are located.
- The users authentication information.

*Explanation*

*The hostname, port, and path in the URL of the request.*

**Multiple choice**

Which load balancing strategy does the Application Gateway implement? Select one.

- Distributes requests to each available server in a backend pool in turn, round-robin.
- Distributes requests to the server in the backend pool with the lightest load.
- Polls each server in the backend pool in turn, and sends the request to the first server that responds.

*Explanation*

*The Application Gateway distributes requests to each available server in the backend pool using the round-robin method.*

**Multiple choice**

Your company has a website that allows users to customize their experience by downloading an app. Demand for the app has increased so you have added another virtual network with two virtual machines. These machines are dedicated to serving the app downloads. You need to ensure the additional download requests do not affect the website performance. Your solution must route all download requests to the two new servers you have installed. What action will you recommend? Select one.

- Add a user-defined route.
- Create a local network gateway.
- Add an application gateway.

*Explanation*

*Application gateway. Application Gateway lets you control the distribution of user traffic to your endpoints running in different datacenters around the world.*

**Multiple choice**

You are deploying the Application Gateway and want to ensure incoming requests are checked for common security threats like cross-site scripting and crawlers. To address your concerns what should you do? Select one.

- Install an internal load balancer
- Install Azure Firewall
- Install the Web Application Firewall

*Explanation*

*Install the Web Application Firewall. The web application firewall (WAF) is an optional component that handles incoming requests before they reach a listener. The web application firewall checks each request for many common threats, based on the Open Web Application Security Project (OWASP).*

# Module 7 Administer Azure Storage

## Configure Storage Accounts

### Introduction

#### Scenario

Most organizations have diverse requirements for their cloud-hosted data. Your company has documents, spreadsheets, and videos. This information needs to be securely shared across the organization and across geographical areas. The data must be quickly recovered if there is a datacenter failure.

You need to configure appropriate storage accounts for the data. You need to configure secure access and a storage replication strategy.

#### Skills measured

Configuring storage accounts is part of **Exam AZ-104: Microsoft Azure Administrator<sup>1</sup>**.

Implement and manage storage (15–20%)

Secure storage

- Create and configure storage accounts.
- Configure network access to storage accounts.

#### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for Azure storage accounts.
- Select between different types of storage and storage accounts.
- Select a storage replication strategy.

<sup>1</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

- Configure network access to storage accounts.
- Secure storage endpoints.

## Prerequisites

None.

# Implement Azure Storage

Azure Storage is Microsoft's cloud storage solution for modern data storage scenarios. Azure Storage offers a massively scalable object store for data objects, a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store. Azure Storage is:

- **Durable and highly available.** Redundancy ensures that your data is safe during transient hardware failures. You replicate data across datacenters or geographical regions for protection from local catastrophe or natural disaster. Data replicated remains highly available during an unexpected outage.
- **Secure.** All data written to Azure Storage is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data.
- **Scalable.** Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications.
- **Managed.** Microsoft Azure handles hardware maintenance, updates, and critical issues for you.
- **Accessible.** Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS. Microsoft provides SDKs for Azure Storage in various languages .NET, Java, Node.js, Python, PHP, Ruby, Go, and REST API. Azure Storage supports scripting in Azure PowerShell or Azure CLI. And the Azure portal and Azure Storage Explorer offer easy visual solutions for working with your data.

Azure Storage is a service that you can use to store files, messages, tables, and other types of information. You use Azure storage for applications like file shares. Developers use Azure storage for working data. Working data includes websites, mobile apps, and desktop applications. Azure storage is also used by IaaS virtual machines, and PaaS cloud services. You can generally think of Azure storage in three categories.

- **Storage for Virtual Machines.** Virtual machine storage includes disks and files. Disks are persistent block storage for Azure IaaS virtual machines. Files are fully managed file shares in the cloud.
- **Unstructured Data.** Unstructured data includes Blobs and Data Lake Store. Blobs are highly scalable, REST-based cloud object store. Data Lake Store is Hadoop Distributed File System (HDFS) as a service.
- **Structured Data.** Structured data includes Tables, Cosmos DB, and Azure SQL DB. Tables are a key/value, autoscaling NoSQL store. Cosmos DB is a globally distributed database service. Azure SQL DB is a fully managed database-as-a-service built on SQL.

General purpose storage accounts have two tiers: **Standard** and **Premium**.

- **Standard** storage accounts are backed by magnetic drives (HDD) and provide the lowest cost per GB. Use Standard storage for applications that require bulk storage or where data is infrequently accessed.
- **Premium** storage accounts are backed by solid-state drives (SSD) and offer consistent low-latency performance. Use Premium storage for Azure virtual machine disks with I/O-intensive applications, like databases.

**Note:** You can't convert a Standard storage account to a Premium storage account or vice versa. You must create a new storage account with the desired type and copy data, if applicable, to a new storage account.

# Explore Azure Storage Services

Azure Storage includes these data services, each of which is accessed through a storage account.

- **Azure Containers (Blobs):** A massively scalable object store for text and binary data.
- **Azure Files:** Managed file shares for cloud or on-premises deployments.
- **Azure Queues:** A messaging store for reliable messaging between application components.
- **Azure Tables:** A NoSQL store for schemaless storage of structured data.

## Container (blob) storage

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data. Blob storage is ideal for:

- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

Objects in Blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

## Azure Files

Azure Files enables you to set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol. That means that multiple VMs can share the same files with both read and write access. You can also read the files using the REST interface or the storage client libraries.

One thing that distinguishes Azure Files from files on a corporate file share is that you can access the files from anywhere in the world using a URL that points to the file and includes a shared access signature (SAS) token. You can generate SAS tokens; they allow specific access to a private asset for a specific amount of time.

File shares can be used for many common scenarios:

- Many on-premises applications use file shares. This feature makes it easier to migrate those applications that share data to Azure. If you mount the file share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with minimal, if any, changes.
- Configuration files can be stored on a file share and accessed from multiple VMs. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them, and that they use the same version.
- Diagnostic logs, metrics, and crash dumps are just three examples of data that can be written to a file share and processed or analyzed later.

At this time, Active Directory-based authentication and access control lists (ACLs) are not supported, but they will be at some time in the future. The storage account credentials are used to provide authentica-

tion for access to the file share. This means anybody with the share mounted will have full read/write access to the share.

## Queue storage

The Azure Queue service is used to store and retrieve messages. Queue messages can be up to 64 KB in size, and a queue can contain millions of messages. Queues are used to store lists of messages to be processed asynchronously.

For example, if you want your customers to be able to upload pictures, and you want to create thumbnails for each picture. You could have your customer wait for you to create the thumbnails while uploading the pictures. An alternative would be to use a queue. When the customer finishes the upload, write a message to the queue. Then have an Azure Function retrieve the message from the queue and create the thumbnails. Each of the processing parts can be scaled separately, giving you more control when tuning it for your usage.

## Table storage

Azure Table storage is now part of Azure Cosmos DB. In addition to the existing Azure Table storage service, there is a new Azure Cosmos DB Table API offering that provides throughput-optimized tables, global distribution, and automatic secondary indexes. Table storage is ideal for storing structured, non-relational data.

## Determine Storage Account Kinds

Azure Storage offers several kinds of storage accounts. Each kind supports different features and has its own pricing model. Consider these differences before you create a storage account to determine the kind of account that is best for your applications. The kinds of storage accounts are:

| Storage account             | Recommended usage                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Standard general-purpose v2 | Most scenarios including Blob, File, Queue, Table, and Data Lake Storage.                                                            |
| Premium block blobs         | Block blob scenarios with high transaction rates, or scenarios that use smaller objects or require consistently low storage latency. |
| Premium file shares         | Enterprise or high-performance file share applications.                                                                              |
| Premium page blobs          | Premium high-performance page blob scenarios.                                                                                        |

**Note:** All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest.

## Determine Replication Strategies

The data in your Azure storage account is always replicated to ensure durability and high availability. Azure Storage replication copies your data so that it is protected from planned and unplanned events ranging from transient hardware failures, network or power outages, massive natural disasters, and so on. You can choose to replicate your data within the same data center, across zonal data centers within the same region, and even across regions. Replication ensures that your storage account meets the Service-Level Agreement (SLA) for Storage even in the face of failures.

## Comparison of replication options

The following table provides a quick overview of the scope of durability and availability that each replication strategy will provide you for a given type of event (or event of similar impact).

|                                                                                                                 | LRS              | ZRS  | GRS/RA-GRS        | GZRS/RA-GZRS       |
|-----------------------------------------------------------------------------------------------------------------|------------------|------|-------------------|--------------------|
| <b>Node unavailability within a data center</b>                                                                 | Yes              | Yes  | Yes               | Yes                |
| <b>An entire data center (zonal or non-zonal) becomes unavailable</b>                                           | No               | Yes  | Yes               | Yes                |
| <b>A region-wide outage</b>                                                                                     | No               | No   | Yes               | Yes                |
| <b>Read access to your data (in a remote, geo-replicated region) in the event of region-wide unavailability</b> | No               | No   | Yes (with RA-GRS) | Yes (with RA-GZRS) |
| <b>Available in storage account types</b>                                                                       | GPv1, GPv2, Blob | GPv2 | GPv1, GPv2, Blob  | GPv2               |

## Locally redundant storage

LRS is the **lowest-cost replication option** and offers the least durability compared to other options. If a datacenter-level disaster (for example, fire or flooding) occurs, **all replicas may be lost or unrecoverable**.

Despite its limitations, LRS may be appropriate in these scenarios:

- When your application stores data that can be easily reconstructed if data loss occurs.
- When your data is constantly changing, for example a live feed, and storing the data is really not required.
- When your application is restricted to replicating data only within a country due to data governance requirements.

## Zone redundant storage

Zone Redundant Storage (ZRS) synchronously replicates your data across three (3) storage clusters in a single region. Each storage cluster is physically separated from the others and resides in its own availability zone. Each availability zone, and the ZRS cluster within it, is autonomous, with separate utilities and networking capabilities. Storing your data in a ZRS account ensures that you will be able access and manage your data if a zone becomes unavailable. ZRS provides excellent performance and low latency.

Here are a few of more things to know about ZRS:

- ZRS is not yet available in all regions.

- Changing to ZRS from another data replication option requires the physical data movement from a single storage stamp to multiple stamps within a region.
- ZRS may not protect your data against a regional disaster where multiple zones are permanently affected. Instead, ZRS offers resiliency for your data.

## Geo-redundant storage

Geo-redundant storage (GRS) **replicates your data to a secondary region** (hundreds of miles away from the primary location of the source data). GRS costs more than LRS, but GRS provides a higher level of durability for your data, **even if there is a regional outage**. GRS is designed to provide at least **99.999999999999% (16 9's) durability**. When your storage account has GRS enabled, then your data is durable even when there is a complete regional outage or a disaster where the primary region isn't recoverable.

For a storage account with GRS or RA-GRS enabled, all data is first replicated with locally redundant storage (LRS). An update is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the secondary region using GRS. When data is written to the secondary location, it's also replicated within that location using LRS. Both the primary and secondary regions manage replicas across separate fault domains and upgrade domains within a storage scale unit. The storage scale unit is the basic replication unit within the datacenter. Replication at this level is provided by LRS. If you opt for GRS, you have two related options to choose from:

- **GRS** replicates your data to another data center in a secondary region, but that data is available to be read only if Microsoft initiates a failover from the primary to secondary region.
- **Read-access geo-redundant storage (RA-GRS)** is based on GRS. RA-GRS replicates your data to another data center in a secondary region, and also provides you with the option to read from the secondary region. With RA-GRS, you can read from the secondary regardless of whether Microsoft initiates a failover from the primary to the secondary.

## Geo-zone redundant storage

Geo-zone-redundant storage (GZRS) **combines the high availability of zone-redundant storage with protection from regional outages as provided by geo-redundant storage**. Data in a GZRS storage account is replicated across three Azure availability zones in the primary region and also replicated to a secondary geographic region for protection from regional disasters. Each Azure region is paired with another region within the same geography, together making a regional pair.

With a GZRS storage account, you can continue to read and write data if an availability zone becomes unavailable or is unrecoverable. Additionally, your data is also durable when a complete regional outage or a disaster in which the primary region isn't recoverable. GZRS is designed to provide at least **99.999999999999% (16 9's) durability** of objects over a given year. GZRS also offers the same scalability targets as LRS, ZRS, GRS, or RA-GRS. You can optionally enable read access to data in the secondary region with read-access geo-zone-redundant storage (RA-GZRS).

Microsoft recommends using GZRS for applications requiring consistency, durability, high availability, excellent performance, and resilience for disaster recovery. Enable RA-GZRS for read access to a secondary region when there is a regional disaster.

## Access Storage

Every object that you store in Azure Storage has a unique URL address. The storage account name forms the subdomain of that address. The combination of subdomain and domain name, which is specific to each service, forms an endpoint for your storage account.

For example, if your storage account is named *mystorageaccount*, then the default endpoints for your storage account are:

- Container service: <http://mystorageaccount.blob.core.windows.net>
- Table service: <http://mystorageaccount.table.core.windows.net>
- Queue service: <http://mystorageaccount.queue.core.windows.net>
- File service: <http://mystorageaccount.file.core.windows.net>

The URL for accessing an object in a storage account is built by appending the object's location in the storage account to the endpoint. For example, to access *myblob* in the *mycontainer*, use this format: <http://mystorageaccount.blob.core.windows.net/mycontainer/myblob>.

## Configuring a Custom Domain

You can configure a custom domain for accessing blob data in your Azure storage account. As mentioned previously, the default endpoint for Azure Blob storage is <storage-account-name>.blob.core.windows.net. You can also use the web endpoint that's generated as a part of the static websites feature. If you map a custom domain and subdomain, such as www.contoso.com, to the blob or web endpoint for your storage account, your users can use that domain to access blob data in your storage account. There are two ways to configure this service: Direct CNAME mapping and an intermediary domain.

**Note:** Azure Storage does not yet natively support HTTPS with custom domains. You can currently Use Azure CDN to access blobs by using custom domains over HTTPS.

**Direct CNAME mapping** for example, to enable a custom domain for the blobs.contoso.com sub domain to an Azure storage account, create a CNAME record that points from blobs.contoso.com to the Azure storage account [storage account].blob.core.windows.net. The following example maps a domain to an Azure storage account in DNS:

| CNAME record      | Target                             |
|-------------------|------------------------------------|
| blobs.contoso.com | contosoblobs.blob.core.windows.net |

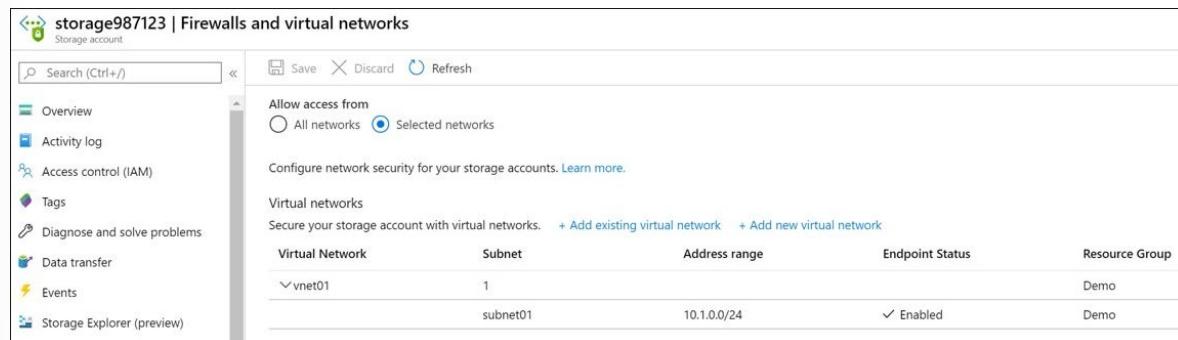
**Intermediary mapping with asverify** Mapping a domain that is already in use within Azure may result in minor downtime as the domain is updated. To avoid downtime, you can use the asverify subdomain to validate the domain. By prepending asverify to your own subdomain, you permit Azure to recognize your custom domain without modifying the DNS record for the domain. After you modify the DNS record for the domain, it will be mapped to the blob endpoint with no downtime.

The following examples maps a domain to the Azure storage account in DNS with the asverify intermediary domain:

| CNAME record               | Target                                      |
|----------------------------|---------------------------------------------|
| asverify.blobs.contoso.com | asverify.contosoblobs.blob.core.windows.net |
| blobs.contoso.com          | contosoblobs.blob.core.windows.net          |

## Secure Storage Endpoints

The steps necessary to restrict network access to Azure services varies across services. For accessing a storage account, you would use the **Firewalls and virtual networks** blade to add the virtual networks that will have access. Notice you can also configure to allow access to one or more public IP ranges.



The screenshot shows the 'storage987123 | Firewalls and virtual networks' blade. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Data transfer, Events, and Storage Explorer (preview). The main area has a search bar and buttons for Save, Discard, and Refresh. It shows the 'Allow access from' section with 'Selected networks' selected. Below that is a 'Virtual networks' section with a table:

| Virtual Network | Subnet | Address range | Endpoint Status | Resource Group |
|-----------------|--------|---------------|-----------------|----------------|
| vnet01          | 1      | subnet01      | 10.1.0.0/24     | Enabled        |

The 'Resource Group' column shows 'Demo' for the row.

- Firewalls and Virtual Networks restricts access to the Storage Account from specific Subnets on Virtual Networks or public IPs.
- Subnets and Virtual Networks must exist in the same Azure Region or Region Pair as the Storage Account.

**Note:** Be sure to test the service endpoint and verify the endpoint is limiting access as expected.

## Demonstration - Secure Storage Endpoints

In this demonstration, we will create a storage accounts, upload a file, and secure the file endpoint.

### Create a storage account in the portal

1. In the Azure portal, select **All services**. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select **Storage Accounts**.
2. On the Storage Accounts window that appears, choose **Add**.
3. Select the **subscription** in which to create the storage account.
4. Under the Resource group field, select **Create new**. Enter a name for your new resource group.
5. Enter a **name** for your storage account. The name you choose must be unique across Azure. The name also must be between 3 and 24 characters in length and can include numbers and lowercase letters only.
6. Select a **location** for your storage account or use the default location.
7. Leave these fields set to their default values:
  - Deployment model: **Resource Manager**
  - Performance: **Standard**
  - Account kind: **StorageV2 (general-purpose v2)**
  - Replication: **Locally redundant storage (LRS)**
  - Access tier: **Hot**
8. Select **Review + Create** to review your storage account settings and create the account.
9. Select **Create**.

10. If you have time, review the PowerShell and CLI code at the end of this demonstration.

#### **Upload a file to the storage account**

1. Within the Storage Account, create a **file share**, and **upload** a file.
2. For the Storage Account, use the **Shared Access Signature** blade to **Generate SAS and connection string**.
3. Use Storage Explorer and the connection string to access the file share.
4. Ensure you can view your uploaded file.

**Note:** This part of the demonstration requires a virtual network with a subnet.

#### **Create a subnet service endpoint**

1. Select your virtual network, and then select a subnet in the virtual network.
2. Under **Service Endpoints**, view the **Services** drop-down and the different services that can be secured with an endpoint.
3. Check the **Microsoft.Storage** option.
4. **Save** your changes.

#### **Secure the storage to the service endpoint**

1. Return to your **storage account**.
2. Select **Firewalls and virtual networks**.
3. Change to **Selected networks**.
4. Add existing virtual network, verify your subnet with the new service endpoint is listed.
5. **Save** your changes.

#### **Test the storage endpoint**

1. Return to the Storage Explorer.
2. **Refresh** the storage account.
3. You should now have an access error similar to this one:

```
This request is not authorized to perform this operation. RequestId:ae899621-e01a-00e8-12d5-c7876a000000 Time:2019-02-18T22:00:26.4551769Z
```

#### **Optional - Create a storage account using PowerShell**

Use the following code to create a storage account using PowerShell. Swap out the storage types and names to suit your requirements.

```
Get-AzLocation | select Location
$location = "westus"
$resourceGroup = "storage-demo-resource-group"
New-AzResourceGroup -Name $resourceGroup -Location $location
New-AzStorageAccount -ResourceGroupName $resourceGroup -Name "storagedemo"
-Location $location -SkuName Standard_LRS -Kind StorageV2
```

#### **Create a storage account using Azure CLI (optional)**

Use the following code to create a storage account using Azure CLI. Change the storage types and names to suit your requirements.

```
az group create --name storage-resource-group --location westus
az account list-locations --query "[].{Region:name}" --out table
az storage account create --name storagedemo --resource-group storage-re-
source-group --location westus --sku Standard_LRS --kind StorageV2
```

**Note:** If you plan to use the storage account in other scenarios be sure to return the account to **All networks** in the **Firewalls and virtual networks** blade.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Which of the following replicates your data to a secondary region, maintains six copies of your data, and is the default replication option? Select one.*

- Locally-redundant storage
- Read-access geo-redundant storage
- Zone-redundant storage

### Multiple choice

*You have two video files stored as blobs. One of the videos is business-critical and requires a replication policy that creates multiple copies across geographically diverse datacenters. The other video is non-critical, and a local replication policy is sufficient. Which of the following options would satisfy both data diversity and cost sensitivity consideration?*

- Create a single storage account that makes use of Local-redundant storage (LRS) and host both videos from here.
- Create a single storage account that makes use of Geo-redundant storage (GRS) and host both videos from here.
- Create two storage accounts. The first account makes use of Geo-redundant storage (GRS) and hosts the business-critical video content. The second account makes use of Local-redundant storage (LRS) and hosts the non-critical video content.

### Multiple choice

*The name of a storage account must be:*

- Unique within the containing resource group.
- Unique within your Azure subscription.
- Globally unique.

## Multiple choice

In a typical project, when would you create your storage account(s)?

- At the beginning, during project setup.
- After deployment, when the project is running.
- At the end, during resource cleanup.

## Multiple choice

A manufacturing company has several sensors that record time-relative data. Only the most recent data is useful. The company wants the lowest cost storage for this data. What is the best kind of storage account for them?

- LRS
- GRS
- ZRS

## Summary and Resources

### Summary

An Azure storage account contains all of your Azure Storage data objects. These data objects can be blobs, files, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data. The data is accessible from anywhere in the world over HTTP or HTTPS. Data in your Azure storage account is durable and highly available, secure, and massively scalable.

You should now be able to:

- Create and configure storage accounts.
- Configure network access to storage accounts.

### Learn more

You can learn more by reviewing the following.

- [Azure Storage documentation<sup>2</sup>](https://docs.microsoft.com/azure/storage/).
- [Learn - Create an Azure Storage account<sup>3</sup>](https://docs.microsoft.com/learn/modules/create-azure-storage-account/)
- [Learn - Make your application storage highly available with read-access geo-redundant storage<sup>4</sup>](https://docs.microsoft.com/learn/modules/ha-application-storage-with-grs/)
- [Learn - Provide disaster recovery by replicating storage data across regions and failing over to secondary location<sup>5</sup>](https://docs.microsoft.com/learn/modules/provide-disaster-recovery-by-replicating-storage-data-across-regions-and-failing-over-to-secondary-location/)

<sup>2</sup> <https://docs.microsoft.com/azure/storage/>

<sup>3</sup> <https://docs.microsoft.com/learn/modules/create-azure-storage-account/>

<sup>4</sup> <https://docs.microsoft.com/learn/modules/ha-application-storage-with-grs/>

<sup>5</sup> <https://docs.microsoft.com/learn/modules/provide-disaster-recovery-by-replicating-storage-data-across-regions-and-failing-over-to-secondary-location/>

# Configure Blob Storage

## Introduction

### Scenario

Azure Blob storage is a service for storing large amounts of unstructured object data, such as text or binary data. Your media company has an extensive library of video clips. The videos are accessed thousands of times a day.

The company relies on you to configure Blob storage. You use access tiers to reduce cost and improve performance. You develop a lifecycle management plan for the older videos. You configure object replication for failover.

### Skills measured

Configuring Blob storage is part of the **Exam AZ-104: Microsoft Azure Administrator<sup>6</sup>**.

Implement and manage storage (15–20%)

Configure Azure files and Azure Blob Storage

- Configure Azure Blob Storage.
- Configure storage tiers for Azure Blob storage.
- Configure Blob lifecycle management.

### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for Azure Blob storage.
- Configure Blob storage and Blob access tiers.
- Configure Blob lifecycle management rules.
- Configure Blob object replication.
- Upload and price Blob storage.

### Prerequisites

None.

## Implement Blob Storage

Azure Blob storage is a service that stores unstructured data in the cloud as objects/blobs. Blob storage can store any type of text or binary data, such as a document, media file, or application installer. Blob storage is also referred to as object storage.

Common uses of Blob storage include:

- Serving images or documents directly to a browser.

---

<sup>6</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

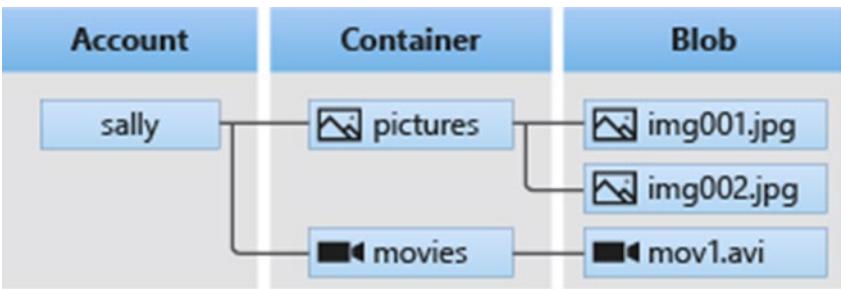
- Storing files for distributed access, such as installation.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

## Blob service resources

Blob storage offers three types of resources:

- The storage account
- Containers in the storage account
- Blobs in a container

The following diagram shows the relationship between these resources.



**Note:** Within the storage account, you can group as many blobs as needed in a container.

## Create Blob Containers

A container provides a grouping of a set of blobs. All blobs must be in a container. An account can contain an unlimited number of containers. A container can store an unlimited number of blobs. You can create the container in the Azure portal.

The screenshot shows the Azure portal's "New container" creation dialog. At the top, there are buttons for "+ Container" and "Change access level". The main area is titled "New container" and contains fields for "Name \*" (with "container01" entered) and "Public access level" (set to "Private (no anonymous access)". At the bottom are "OK" and "Cancel" buttons. To the right, a dropdown menu for "Public access level" is open, showing four options: "Private (no anonymous access)" (selected), "Private (no anonymous access)", "Blob (anonymous read access for blobs only)", and "Container (anonymous read access for containers and blobs)".

**Name:** The name may only contain lowercase letters, numbers, and hyphens, and must begin with a letter or a number. The name must also be between 3 and 63 characters long.

**Public access level:** Specifies whether data in the container may be accessed publicly. By default, container data is private to the account owner.

- Use **Private** to ensure there is no anonymous access to the container and blobs.
- Use **Blob** to allow anonymous public read access for blobs only.
- Use **Container** to allow anonymous public read and list access to the entire container, including the blobs.

**Note:** You can also create the Blob container with PowerShell using the **New-AzStorageContainer** command. How will you organize your Blob containers?

## Create Blob Access Tiers

Azure Storage provides different options for accessing block blob data (as shown in the screenshot), based on usage patterns. Each access tier in Azure Storage is optimized for a particular pattern of data usage. By selecting the correct access tier for your needs, you can store your block blob data in the most cost-effective manner.

### Access Tier

Optimize storage costs by placing your data in the appropriate access tier.



- **Hot.** The Hot tier is optimized for frequent access of objects in the storage account. Accessing data in the Hot tier is most cost-effective, while storage costs are higher. New storage accounts are created in the Hot tier by default.
- **Cool.** The Cool tier is optimized for storing large amounts of data that is infrequently accessed and stored for at least 30 days. Storing data in the Cool tier is more cost-effective, but accessing that data may be more expensive than accessing data in the Hot tier.
- **Archive.** The Archive tier is optimized for data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days. The Archive tier is the most cost-effective option for storing data, but accessing that data is more expensive than accessing data in the Hot or Cool tiers.

**Note:** When data usage changes, you can switch access tiers at any time.

# Add Blob Lifecycle Management Rules

## Add a rule

Details     Base blobs

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

+ Add if-then block

The screenshot shows the Azure portal's 'Add a rule' configuration page. At the top, there are two tabs: 'Details' (unchecked) and 'Base blobs' (checked). A note below explains that lifecycle management moves blobs to cooler tiers or deletes them based on defined rules, with the order from hot to cool storage, then archive, then deletion. An 'Add if-then block' button is present. The main area is divided into 'If' and 'Then' sections. In the 'If' section, 'Base blobs were' is set to 'Last modified' and 'More than (days ago)' is left empty. In the 'Then' section, 'Delete the blob' is selected, followed by 'Move to cool storage' (disabled), 'Move to archive storage' (disabled), and 'Delete the blob' again, which is described as the most efficient option if backing up a blob is not a priority.

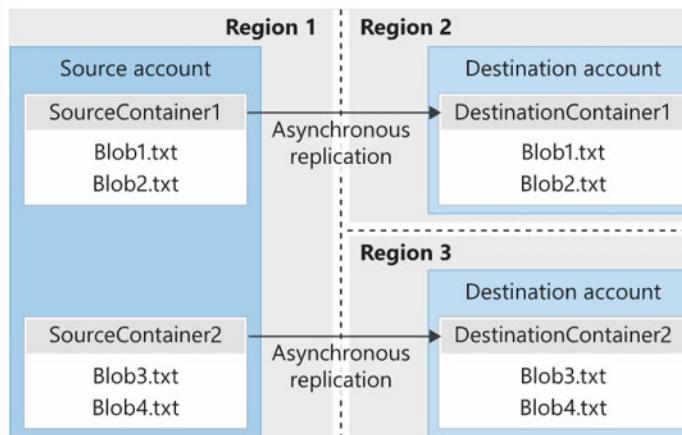
Data sets have unique lifecycles. Early in the lifecycle, people access some data often. But the need for access drops drastically as the data ages. Some data stays idle in the cloud and is rarely accessed once stored. Some data expires days or months after creation, while other data sets are actively read and modified throughout their lifetimes. Azure Blob storage lifecycle management offers a rich, rule-based policy for GPv2 and Blob storage accounts. Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's lifecycle.

The lifecycle management policy lets you:

- Transition blobs to a cooler storage tier (hot to cool, hot to archive, or cool to archive) to optimize for performance and cost.
- Delete blobs at the end of their lifecycles.
- Define rules to be run once per day at the storage account level.
- Apply rules to containers or a subset of blobs.

Consider a scenario where data gets frequent access during the early stages of the lifecycle, but only occasionally after two weeks. Beyond the first month, the data set is rarely accessed. In this scenario, hot storage is best during the early stages. Cool storage is most appropriate for occasional access. Archive storage is the best tier option after the data ages over a month. By adjusting storage tiers in respect to the age of data, you can design the least expensive storage options for your needs. To achieve this transition, lifecycle management policy rules are available to move aging data to cooler tiers.

# Determine Blob Object Replication



Object replication asynchronously copies block blobs in a container according to rules that you configure. The contents of the blob, any versions associated with the blob, and the blob's metadata and properties are all copied from the source container to the destination container.

## Scenarios

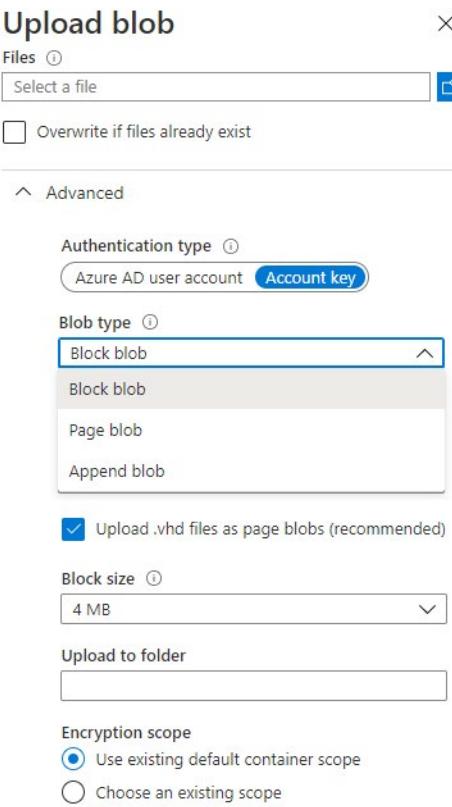
- **Minimizing latency.** Object replication can reduce latency for read requests by enabling clients to consume data from a region that is in closer physical proximity.
- **Increase efficiency for compute workloads.** With object replication, compute workloads can process the same sets of block blobs in different regions.
- **Optimizing data distribution.** You can process or analyze data in a single location and then replicate just the results to other regions.
- **Optimizing costs.** After your data has been replicated, you can reduce costs by moving it to the archive tier using life-cycle management policies.

## Considerations

- Object replication requires that blob versioning is enabled on both the source and destination accounts.
- Object replication doesn't support blob snapshots. Any snapshots on a blob in the source account are not replicated to the destination account.
- Object replication is supported when the source and destination accounts are in the hot or cool tier. The source and destination accounts may be in different tiers.
- When you configure object replication, you create a replication policy that specifies the source storage account and the destination account. A replication policy includes one or more rules that specify a source container and a destination container and indicate which block blobs in the source container will be replicated.

## Upload Blobs

A blob can be any type and size file. Azure Storage offers three types of blobs: *block blobs*, *page blobs*, and *append blobs*. You specify the blob type and access tier when you create the blob.



- **Block blobs (default)** consist of blocks of data assembled to make a blob. Most scenarios using Blob storage employ block blobs. Block blobs are ideal for storing text and binary data in the cloud, like files, images, and videos.
- **Append blobs** are like block blobs in that they are made up of blocks, but they are optimized for append operations, so they are useful for logging scenarios.
- **Page blobs** can be up to 8 TB in size and are more efficient for frequent read/write operations. Azure virtual machines use page blobs as OS and data disks.

**Note:** Once the blob has been created, its type cannot be changed.

## Blob upload tools

There are multiple methods to upload data to blob storage, including the following methods:

- **AzCopy** is an easy-to-use command-line tool for Windows and Linux that copies data to and from Blob storage, across containers, or across storage accounts.
- The **Azure Storage Data Movement library** is a .NET library for moving data between Azure Storage services. The AzCopy utility is built with the Data Movement library.
- **Azure Data Factory** supports copying data to and from Blob storage by using the account key, shared access signature, service principal, or managed identities for Azure resources authentications.
- **Blobfuse** is a virtual file system driver for Azure Blob storage. You can use blobfuse to access your existing block blob data in your Storage account through the Linux file system.
- **Azure Data Box Disk** is a service for transferring on-premises data to Blob storage when large datasets or network constraints make uploading data over the wire unrealistic. You can use Azure Data

Box Disk to request solid-state disks (SSDs) from Microsoft. You can then copy your data to those disks and ship them back to Microsoft to be uploaded into Blob storage.

- The **Azure Import/Export** service provides a way to export large amounts of data from your storage account to hard drives that you provide and that Microsoft then ships back to you with your data.

**Note:** And, you can always use Azure Storage Explorer.

## Determine Storage Pricing

All storage accounts use a pricing model for blob storage based on the tier of each blob. When using a storage account, the following billing considerations apply:

- **Performance tiers:** The storage tier determines the amount of data stored and the cost of storing the data. As the performance tier gets cooler, the per-gigabyte cost decreases.
- **Data access costs:** Data access charges increase as the tier gets cooler. For data in the cool and archive storage tier, you are charged a per-gigabyte data access charge for reads.
- **Transaction costs:** There is a per-transaction charge for all tiers. The charge increases as the tier gets cooler.
- **Geo-Replication data transfer costs:** This charge only applies to accounts with geo-replication configured, including GRS and RA-GRS. Geo-replication data transfer incurs a per-gigabyte charge.
- **Outbound data transfer costs:** Outbound data transfers (data that is transferred out of an Azure region) incur billing for bandwidth usage on a per-gigabyte basis. This billing is consistent with general-purpose storage accounts.
- **Changing the storage tier:** Changing the account storage tier from cool to hot incurs a charge equal to reading all the data existing in the storage account. However, changing the account storage tier from hot to cool incurs a charge equal to writing all the data into the cool tier (GPv2 accounts only).

## Demonstration - Blob Storage

In this demonstration, you will explore blob storage.

**Note:** This demonstration requires a storage account.

### Create a container

1. Navigate to a storage account in the Azure portal.
2. In the left menu for the storage account, scroll to the **Blob service** section, then select **Blobs**.
3. Select the **+ Container** button.
4. Type a **Name** for your new container. The container name must be lowercase, must start with a letter or number, and can include only letters, numbers, and the dash (-) character.
5. Set the level of public access to the container. The default level is Private (no anonymous access).
6. Select **OK** to create the container.

### Upload a block blob

1. In the Azure portal, navigate to the container you created in the previous section.
2. Select the container to show a list of blobs it contains. Since this container is new, it won't yet contain any blobs.
3. Select the **Upload** button to upload a blob to the container.

4. Expand the **Advanced** section.
5. Notice the **Authentication type**, **Blob type**, **Block size**, and the ability to **Upload to a folder**.
6. Notice the default **Authentication type** is SAS.
7. Browse your local file system to find a file to upload as a block blob and select **Upload**.
8. Upload as many blobs as you like in this way. You'll observe that the new blobs are now listed within the container.

#### Download a block blob

You can download a block blob to display in the browser or save to your local file system.

1. Navigate to the list of blobs that you uploaded in the previous section.
2. Right-click the blob you want to download and select **Download**.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Which of these changes between access tiers will happen immediately?*

- Hot to Cool
- Archive to Cool
- Archive to Hot

### Multiple choice

*You work for an open-source development company. You use Microsoft Azure for a variety of storage needs. Up to now, all the storage was used for internal purposes only. It is organized in block blobs. Each block blob is in its own container. Each container is set to default settings. In total, you have 50 block blobs. The company has decided to provide read access to the data in the block blobs, as part of releasing more information about their open-source development efforts. All block blobs must be readable by anonymous internet users. You need to configure the storage to meet the requirements. What should you do? Select one.*

- Create a new container, move all the blobs to the new container, and then set the public access level to Blob.
- Set the public access level to Blob on all the existing containers.
- Create a new access key for the storage account and then provide the connection string in the storage connectivity information to the public.

## Multiple choice

Your company provides cloud software to audit administrative access in Microsoft Azure resources. The software logs all administrative actions (including all clicks and text input) to log files. The software is about to be released from beta and the company is concerned about storage performance. You need to deploy a storage solution for the log files to maximize performance. What should you do? Select one.

- Deploy Azure Files using SMB 3.0.
- Deploy blob storage using block blobs.
- Deploy blob storage using append blobs.

## Multiple choice

Your company is building an app in Azure. The storage must be reachable programmatically through a REST API. The storage must be globally redundant. The storage must be accessible privately within the company's Azure environment. The storage must be optimal for unstructured data. Which type of Azure storage should you use for the app? Select one.

- Azure Table Storage
- Azure Blob Storage
- Azure File Storage

## Multiple choice

You are using blob storage. Which of the following is true? Select one.

- The cool access tier is for frequent access of objects in the storage account.
- The hot access tier is for storing large amounts of data that is infrequently accessed.
- You can switch between hot and cool performance tiers at any time.

## Summary and Resources

### Summary

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data. Unstructured data is data that doesn't adhere to a particular data model or definition, such as text or binary data.

You should now be able to:

- Identify features and usage cases for Azure Blob storage.
- Configure Blob storage and Blob access tiers.
- Configure Blob lifecycle management rules.
- Configure Blob object replication.
- Upload and price Blob storage.

## Learn more

You can learn more by reviewing the following.

- [Azure Blob storage documentation<sup>7</sup>](https://docs.microsoft.com/azure/storage/blobs/).
- [Object blob replication overview<sup>8</sup>](https://docs.microsoft.com/azure/storage/blobs/object-replication-overview)
- [Access tiers for Azure Blob Storage - hot, cool, and archive<sup>9</sup>](https://docs.microsoft.com/azure/storage/blobs/storage-blob-storage-tiers)
- [Learn - Optimize storage performance and costs using Blob storage tiers<sup>10</sup>](https://docs.microsoft.com/learn/modules/optimize-archive-costs-blob-storage/)
- [Learn - Gather metrics from your Azure Blob Storage containers<sup>11</sup>](https://docs.microsoft.com/learn/modules/gather-metrics-blob-storage/)

<sup>7</sup> <https://docs.microsoft.com/azure/storage/blobs/>

<sup>8</sup> <https://docs.microsoft.com/azure/storage/blobs/object-replication-overview>

<sup>9</sup> <https://docs.microsoft.com/azure/storage/blobs/storage-blob-storage-tiers>

<sup>10</sup> <https://docs.microsoft.com/learn/modules/optimize-archive-costs-blob-storage/>

<sup>11</sup> <https://docs.microsoft.com/learn/modules/gather-metrics-blob-storage/>

# Configure Storage Security

## Introduction

### Scenario

Your company has sensitive data including Personally Identifiable Information. The data is used internally and by external application developers.

You need to ensure the data is secured. You provide ways to grant secure access to the information.

### Skills measured

Providing secure access to Azure storage is part of **Exam AZ-104: Microsoft Azure Administrator<sup>12</sup>**.

Implement and manage storage (15–20%)

Secure storage

- Generate shared access signature (SAS) tokens.
- Manage access keys.
- Configure Azure AD authentication for a storage account.

### Learning objectives

In this module, you will learn how to:

- Configure shared access signatures including URI and SAS parameters.
- Configure storage service encryption.
- Implement customer-managed keys.
- Recommend opportunities to improve storage security.

### Prerequisites

None.

## Review Storage Security Strategies

Azure Storage provides a comprehensive set of security capabilities that together enable developers to build secure applications.

- **Encryption.** All data written to Azure Storage is automatically encrypted using Storage Service Encryption (SSE).
- **Authentication.** Azure Active Directory (Azure AD) and Role-Based Access Control (RBAC) are supported for Azure Storage for both resource management operations and data operations, as follows:
  - You can assign RBAC roles scoped to the storage account to security principals and use Azure AD to authorize resource management operations such as key management.

---

<sup>12</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

- Azure AD integration is supported for data operations on the Blob and Queue services.
- **Data in transit.** Data can be secured in transit between an application and Azure by using Client-Side Encryption, HTTPS, or SMB 3.0.
- **Disk encryption.** OS and data disks used by Azure virtual machines can be encrypted using Azure Disk Encryption.
- **Shared Access Signatures.** Delegated access to the data objects in Azure Storage can be granted using Shared Access Signatures.

## Authorization options

Every request made against a secured resource in the Blob, File, Queue, or Table service must be authorized. Authorization ensures that resources in your storage account are accessible only when you want them to be, and only to those users or applications to whom you grant access. Options for authorizing requests to Azure Storage include:

- **Azure Active Directory (Azure AD).** Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you can assign fine-grained access to users, groups, or applications via role-based access control (RBAC).
- **Shared Key.** Shared Key authorization relies on your account access keys and other parameters to produce an encrypted signature string that is passed on the request in the Authorization header.
- **Shared access signatures.** Shared access signatures (SAS) delegate access to a particular resource in your account with specified permissions and over a specified time interval.
- **Anonymous access to containers and blobs.** You can optionally make blob resources public at the container or blob level. A public container or blob is accessible to any user for anonymous read access. Read requests to public containers and blobs do not require authorization.

## Create Shared Access Signatures

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a SAS to clients who shouldn't have access to your storage account key. By distributing a SAS URI to these clients, you grant them access to a resource for a specified period of time. SAS is a secure way to share your storage resources without compromising your account keys.

The screenshot shows the 'Generate SAS token and URL' dialog. It includes fields for 'Signing method' (Account key selected), 'Signing key' (Key 1 selected), 'Permissions' (Read selected), 'Start and expiry date/time' (Start: 02/01/2021, Expiry: 02/02/2021), 'Allowed IP addresses' (example: 168.1.5.65 or 168.1.5.65-168.1....), and 'Allowed protocols' (HTTPS selected). A blue button at the bottom right says 'Generate SAS token and URL'.

A SAS gives you granular control over the type of access you grant to clients who have the SAS, including:

- An account-level SAS can delegate access to multiple storage services. For example, blob, file, queue, and table.
- An interval over which the SAS is valid, including the start time and the expiry time.
- The permissions granted by the SAS. For example, a SAS for a blob might grant read and write permissions to that blob, but not delete permissions.

**Note:** There are two types of SAS: **account** and **service**. The account SAS delegates access to resources in one or more of the storage services. The service SAS delegates access to a resource in just one of the storage services.

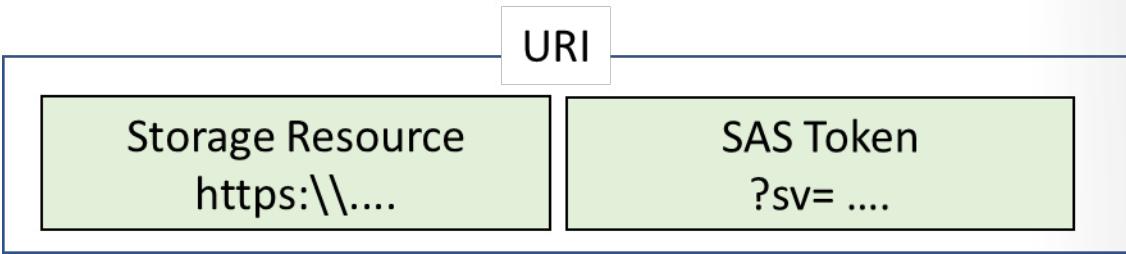
Optionally, you can also:

- Specify an IP address or range of IP addresses from which Azure Storage will accept the SAS. For example, you might specify a range of IP addresses belonging to your organization.
- The protocol over which Azure Storage will accept the SAS. You can use this optional parameter to restrict access to clients using HTTPS.

**Note:** A stored access policy can provide another level of control over service-level SAS on the server side. You can group shared access signatures and provide other restrictions by using policy.

## Identify URI and SAS Parameters

When you create your SAS, a URI is created using parameters and tokens. The URI consists of your Storage Resource URI and the SAS token.



Below is an example URI.

```
https://myaccount.blob.core.windows.net/?restype=service&comp=proper-
ties&sv=2015-04-05&ss=bf&srt=s&st=2015-04-29T22%3A18%3A26Z&se=2015-04-
30T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.5.60-168.1.5.70&spr=https
&sig=F%6GRVAZ5Cdj2Pw4txxxx
```

Each parameter has a specific meaning.

| Name                     | SAS portion                                                              | Description                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resource URI             | https://myaccount.blob.core.windows.net/?restype=service&comp=properties | The Blob service endpoint, with parameters for getting service properties (when called with GET) or setting service properties (when called with SET). |
| Storage services version | sv=2015-04-05                                                            | For storage services version 2012-02-12 and later, this parameter indicates the version to use.                                                        |
| Services                 | ss=bf                                                                    | The SAS applies to the Blob and File services                                                                                                          |
| Resource types           | srt=s                                                                    | The SAS applies to service-level operations.                                                                                                           |
| Start time               | st=2015-04-29T22%3A18%3A26Z                                              | Specified in UTC time. If you want the SAS to be valid immediately, omit the start time.                                                               |
| Expiry time              | se=2015-04-30T02%3A23%3A26Z                                              | Specified in UTC time.                                                                                                                                 |
| Resource                 | sr=b                                                                     | The resource is a blob.                                                                                                                                |
| Permissions              | sp=rw                                                                    | The permissions grant access to read and write operations.                                                                                             |
| IP Range                 | sip=168.1.5.60-168.1.5.70                                                | The range of IP addresses from which a request will be accepted.                                                                                       |
| Protocol                 | spr=https                                                                | Only requests using HTTPS are permitted.                                                                                                               |

| Name      | SAS portion                                            | Description                                                                                                                                                                  |
|-----------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Signature | sig=F%6GRVAZ5Cdj2Pw4tgU7II-STkWgn7bUkkAg8P6HESXwm-f%4B | Used to authenticate access to the blob. The signature is an HMAC computed over a string-to-sign and key using the SHA256 algorithm, and then encoded using Base64 encoding. |

## Demonstration - SAS in the Portal

In this demonstration, we will create a shared access signature.

**Note:** This demonstration requires a storage account, with a blob container, and an uploaded file.

### Create a SAS at the service level

1. Sign into the Azure portal.
2. Locate the storage account you want to work with and open it. Drill down to your blob container.
3. Click the file you would like to provide access to.
4. Select the **Generate SAS** tab.
5. Configure the shared access signature using the following parameters:
  - **Permissions:** Read
  - **Start and expiry date/time:** Today's date to start, 1 year out for expiry
  - **Allowed protocols:** HTTPS
  - **Signing key:** Key1
6. Copy the **Blob Server SAS URL** and paste the URL into a browser.
7. Verify the blob file displays.
8. Review the different URL parameters.

### Create a SAS at the account level

1. Return to your storage account.
2. Click **Shared access signature**.
3. Notice you can configure a variety of services, resource types, and permissions.
4. Click **Generate SAS and connection string**.
5. Review the connection string, SAS token, and URL information that is provided.

## Determine Storage Service Encryption

Azure **Storage Service Encryption** (SSE) for data at rest protects your data by ensuring your organizational security and compliance commitments are met.

SSE automatically encrypts your data before persisting it to Azure-managed Disks, Azure Blob, Queue, Table storage, or Azure Files, and decrypts the data before retrieval.

SES encryption, encryption at rest, decryption, and key management are transparent to users. All data written to the Azure storage platform is encrypted through 256-bit AES encryption, one of the strongest block ciphers available.

**Encryption**

Save  Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data in the storage account is encrypted using Microsoft Managed Keys. You may choose to bring your own key.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn More about Azure Storage Encryption](#)

Encryption type

Microsoft Managed Keys  
 Customer Managed Keys

**Note:** SSE is enabled for all new and existing storage accounts and cannot be disabled. Because your data is secured by default, you don't need to modify your code or applications.

## Create Customer Managed Keys

The Azure Key Vault can manage your encryption keys. You can create your own encryption keys and store them in a key vault, or you can use Azure Key Vault's APIs to generate encryption keys.

Customer-managed keys give you more flexibility and control. You can create, disable, audit, rotate, and define access controls.

Encryption type

Microsoft Managed Keys  
 Customer Managed Keys

**!** The storage account named 'storage987123' will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more about customer managed keys](#)

Encryption key

Enter key URI  
 Select from Key vault

Key vault and key \*

Key vault: keyvault987123  
Key: storagekey  
[Select a key vault and key](#)

**Note:** Customer-managed keys can be used with SSE. You can use either a new or existing key vault and key. The storage account and the key vault must be in the same region, but they can be in different subscriptions.

# Apply Storage Security Best Practices

## Risks

When you use shared access signatures in your applications, you should be aware of two potential risks.

- If a SAS is compromised, it can be used by anyone who obtains it.
- If a SAS provided to a client application expires and the application is unable to retrieve a new SAS from your service, then the application's functionality may be hindered.

## Recommendations

The following recommendations for using shared access signatures can help mitigate risks.

- **Always use HTTPS to create or distribute a SAS.** If a SAS is passed over HTTP and intercepted, an attacker could intercept and use the SAS. These man-in-the-middle attacks can compromise sensitive data or allow for data corruption by the malicious user.
- **Reference stored access policies where possible.** Stored access policies give you the option to revoke permissions without having to regenerate the storage account keys. Set the storage account key expiration date far out in the future.
- **Use near-term expiration times on an unplanned SAS.** In this way, even if a SAS is compromised, it's valid only for a short time. This practice is important if you can't reference a stored access policy. Near-term expiration times also limit the amount of data that can be written to a blob by limiting the time available to upload to it.
- **Have clients automatically renew the SAS if necessary.** Clients should renew the SAS well before the expiration date. Renewing early allows time for retries if the service providing the SAS is unavailable.
- **Be careful with SAS start time.** If you set the start time for a SAS to now, then due to clock skew (differences in current time according to different machines), failures may be observed intermittently for the first few minutes. In general, set the start time to be at least 15 minutes in the past. Or, don't set it at all, which will make it valid immediately in all cases. The same generally applies to expiry time as well - remember that you may observe up to 15 minutes of clock skew in either direction on any request. For clients using a REST version prior to 2012-02-12, the maximum duration for a SAS that does not reference a stored access policy is 1 hour, and any policies specifying longer term than that will fail.
- **Be specific with the resource to be accessed.** A security best practice is to provide a user with the minimum required privileges. If a user only needs read access to a single entity, then grant them read access to that single entity, and not read/write/delete access to all entities. This also helps lessen the damage if a SAS is compromised because the SAS has less power in the hands of an attacker.
- **Understand that your account will be billed for any usage, including that done with SAS.** If you provide write access to a blob, a user may choose to upload a 200-GB blob. If you've given them read access as well, they may choose to download it 10 times, incurring 2 TB in egress costs for you. Again, provide limited permissions to help mitigate the potential actions of malicious users. Use short-lived SAS to reduce this threat (but be mindful of clock skew on the end time).
- **Validate data written using SAS.** When a client application writes data to your storage account, keep in mind that there can be problems with that data. If your application requires that data be validated or authorized before it is ready to use, you should perform this validation after the data is written and before it is used by your application. This practice also protects against corrupt or malicious data.

being written to your account, either by a user who properly acquired the SAS, or by a user exploiting a leaked SAS.

- **Don't assume SAS is always the correct choice.** Sometimes the risks associated with a particular operation against your storage account outweigh the benefits of SAS. For such operations, create a middle-tier service that writes to your storage account after performing business rule validation, authentication, and auditing. Also, sometimes it's simpler to manage access in other ways. For example, if you want to make all blobs in a container publicly readable, you can make the container Public, rather than providing a SAS to every client for access.
- **Use Storage Analytics to monitor your application.** You can use logging and metrics to observe any spike in authentication failures due to an outage in your SAS provider service or to the inadvertent removal of a stored access policy.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*You use a Microsoft Azure storage account for storing large numbers of video and audio files. You create containers to store each type of file and want to limit access to those files for specific periods. Additionally, the files can only be accessed through shared access signatures (SAS). You need the ability to revoke access to the files and to change the period for which users can access the files. What should you do to accomplish this in the most simple and effective way? Select one.*

- Create an SAS for each user and delete the SAS when you want to prevent access.
- Implement stored access policies for each container to enable revocation of access or change of duration.
- Periodically regenerate the account key to control access to the files.

### Multiple choice

*You need to provide a contingent staff employee temporary read-only access to the contents of an Azure storage account container named media. It is important that you grant access while adhering to the security principle of least-privilege. What should you do? Select one.*

- Set the public access level to Container.
- Generate a shared access signature (SAS) token for the container.
- Configure a Cross-Origin Resource Sharing (CORS) rule for the storage account.

## Multiple choice

You are planning a delegation model for your Azure storage. The company has issued the following requirement for Azure storage access: -Apps in the non-production environment must have automated time-limited access. You need to configure storage access to meet the requirements. What should you do?

- Use shared access signatures for the non-production apps.
- Use access keys for the non-production apps.
- Use Stored Access Policies for the production apps..

## Multiple choice

You are planning a delegation model for your Azure storage. The company requires apps in the production environment to have unrestricted access to storage resources. You need to configure storage access to meet the requirements. What should you do?

- Use shared access signatures for the production apps.
- Use access keys for the production apps.
- Use Stored Access Policies for the production apps.

## Multiple choice

When configuring network access to your Azure Storage Account, what is the default network rule?

- To allow all connections from all networks
- To allow all connection from a private IP address range
- To deny all connections from all networks

## Multiple choice

Your organization has data stored in hard drives. It wants to move this data into a secure Azure storage solution. What solution would allow you to encrypt this data with minimal effort?

- Azure Disk Encryption.
- Azure Storage Service Encryption.
- Client-side encryption with Azure.

## Summary and Resources

### Summary

There are many options for securing Azure storage. These options include shared access signatures, storage service encryption, and customer-managed keys.

You should now be able to:

- Configure shared access signatures including URI and SAS parameters.
- Configure storage service encryption.
- Implement customer-managed keys.

- 
- Recommend opportunities to improve storage security.

## Learn more

You can learn more by reviewing the following.

- **What is a shared access signature?**<sup>13</sup>
- **Azure Storage encryption for data at rest**<sup>14</sup>
- **Learn - Secure your Azure Storage**<sup>15</sup>
- **Learn - Control access to Azure Storage with shared access signatures**<sup>16</sup>
- **Learn - Introduction to securing data at rest on Azure**<sup>17</sup>

---

<sup>13</sup> <https://docs.microsoft.com/azure/storage/common/storage-dotnet-shared-access-signature-part-1?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

<sup>14</sup> <https://docs.microsoft.com/azure/storage/common/storage-service-encryption>

<sup>15</sup> <https://docs.microsoft.com/learn/modules/secure-azure-storage-account/>

<sup>16</sup> <https://docs.microsoft.com/learn/modules/control-access-to-azure-storage-with-sas/>

<sup>17</sup> <https://docs.microsoft.com/learn/modules/secure-data-at-rest/>

# Configure Azure Files and File Sync

## Introduction

### Scenario

Your company has a large repository of documents used across the company. Offices are located in different geographical reasons, but need the most current versions of the documents.

You configure Azure File shares to provide a central location for the documents. You configure Azure File Sync to keep the information up to date across multiple offices.

### Skills measured

Configure Azure Files and Azure File Sync is part of **Exam AZ-104: Microsoft Azure Administrator<sup>18</sup>**.

Implement and manage storage (15–20%)

Configure Azure files and Azure Blob Storage

- Create an Azure file share.
- Create and configure Azure File Sync.

### Learning objectives

In this module, you will learn how to:

- Identify when to use Azure files versus Azure Blobs.
- Configure Azure file shares and file share snapshots.
- Identify features and usage cases of Azure File Sync.
- Identify File Sync components and configuration steps.

### Prerequisites

None.

## Compare Files to Blobs

**File storage<sup>19</sup>** offers shared storage for applications using the industry standard **SMB protocol<sup>20</sup>**.

Microsoft Azure virtual machines and cloud services can share file data across application components via mounted shares, and on-premises applications can also access file data in the share.

Applications running in Azure virtual machines or cloud services can mount a file storage share to access file data. This process is similar to how a desktop application would mount a typical SMB share. Any number of Azure virtual machines or roles can mount and access the File storage share simultaneously.

---

<sup>18</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

<sup>19</sup> <https://docs.microsoft.com/azure/storage/files/storage-files-introduction>

<sup>20</sup> <https://msdn.microsoft.com/library/windows/desktop/aa365233.aspx>

## Common uses of file storage

- **Replace and supplement.** Azure Files can be used to completely replace or supplement traditional on-premises file servers or NAS devices.
- **Access anywhere.** Popular operating systems such as Windows, macOS, and Linux can directly mount Azure File shares wherever they are in the world.
- **Lift and shift.** Azure Files makes it easy to "lift and shift" applications to the cloud that expect a file share to store file application or user data.
- **Azure File Sync.** Azure File shares can also be replicated with Azure File Sync to Windows Servers, either on-premises or in the cloud, for performance and distributed caching of the data where it's being used.
- **Shared applications.** Storing shared application settings, for example in configuration files.
- **Diagnostic data.** Storing diagnostic data such as logs, metrics, and crash dumps in a shared location.
- **Tools and utilities.** Storing tools and utilities needed for developing or administering Azure virtual machines or cloud services.

## Comparing Files and Blobs

Sometimes it is difficult to decide when to use file shares instead of blobs or disk shares. Take a minute to review this table that compares the different features.

| Feature            | Description                                                                                                                               | When to use                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Azure Files</b> | Provides an SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files.                       | You want to "lift and shift" an application to the cloud that already uses the native file system APIs to share data between it and other applications running in Azure. You want to store development and debugging tools that need to be accessed from many virtual machines. |
| <b>Azure Blobs</b> | Provides client libraries and a REST interface that allows unstructured data to be stored and accessed at a massive scale in block blobs. | You want your application to support streaming and random-access scenarios. You want to be able to access application data from anywhere.                                                                                                                                       |

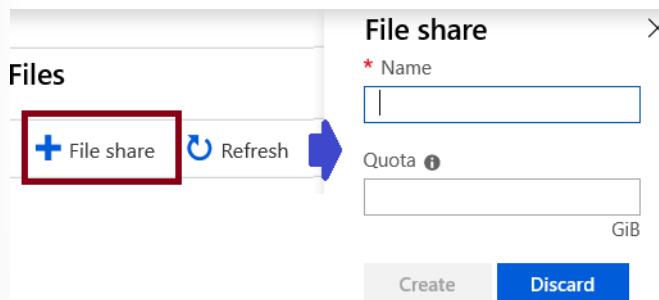
Other distinguishing features, when selecting Azure files.

- Azure files are true directory objects. Azure blobs are a flat namespace.
- Azure files are accessed through file shares. Azure blobs are accessed through a container.
- Azure files provide shared access across multiple virtual machines. Azure disks are exclusive to a single virtual machine.

**Note:** Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol. Azure File shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS.

## Manage File Shares

To access your files, you will need a storage account. After the storage account is created, provide the file share **Name** and the **Quota**. Quota refers to total size of files on the share.



## Mapping File Shares (Windows)

You can connect to your Azure file share with Windows or Windows Server. Just select **Connect** from your file share page.

Windows   Linux   macOS

Drive letter  ▼

To connect to this Azure file share from Windows, run these PowerShell commands from a normal (not elevated) PowerShell terminal:

```
$connectTestResult = Test-NetConnection -ComputerName storage987123.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
 # Save the password so the drive will persist on reboot
 cmd.exe /C "cmdkey /add:"storage987123.file.core.windows.net"
```

This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure [Point-to-Site \(P2S\) VPN](#), Azure [Site-to-Site \(S2S\) VPN](#), or [ExpressRoute](#) to tunnel SMB traffic to your Azure file share over a different port.

**Note:** Ensure port 445 is open. Azure Files uses SMB protocol. SMB communicates over TCP port 445. Also, ensure your firewall is not blocking TCP ports 445 from the client machine.

## Mounting File Shares (Linux)

Windows

Linux

macOS

## Mount point

cs4aa509d922cc7x4eb9x9ae

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

```
sudo mkdir /mnt/cs4aa509d922cc7x4eb9x9ae
if [! -d "/etc/smbcredentials"]; then
sudo mkdir /etc/smbcredentials
fi
if [! -f "/etc/smbcredentials/cs4aa509d922cc7x4eb9x9ae.lcred"];
then
```

In order to mount an Azure file share outside of the Azure region it is hosted in, such as on-premises or in a different Azure region, the OS must support the encryption functionality of SMB 3.0.

Azure file shares can be mounted in Linux distributions using the CIFS kernel client. File mounting can be done on-demand with the mount command or on-boot (persistent) by creating an entry in /etc/fstab.

## Secure Transfer Required

The secure transfer option enhances the security of your storage account by only allowing requests to the storage account by secure connection. For example, when calling REST APIs to access your storage accounts, you must connect using HTTPS. Any requests using HTTP will be rejected when *Secure transfer required* is enabled.

## Create File Share Snapshots

Azure Files provides the capability to take share snapshots of file shares. Share snapshots capture a point-in-time, read-only copy of your data.

|  Add snapshot  Refresh  Delete |                       |           |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------|--|
| Name                                                                                                                                                                                                                                                                                    | Date created          | Initiator |  |
| <input type="checkbox"/> 2020-03-12T00:58:38.0000000Z                                                                                                                                                                                                                                   | 3/11/2020, 8:58:38 PM | -         |  |

Share snapshot capability is provided at the file share level. Retrieval is provided at the individual file level, to allow for restoring individual files. You cannot delete a share that has share snapshots unless you delete all the share snapshots first.

Share snapshots are incremental in nature. Only the data that has changed after your most recent share snapshot is saved. Incremental snapshots minimizes the time required to create the share snapshot and saves on storage costs. Even though share snapshots are saved incrementally, you need to retain only the most recent share snapshot in order to restore the share.

## When to use share snapshots

- **Protection against application error and data corruption.** Applications that use file shares perform operations such as writing, reading, storage, transmission, and processing. When an application is

misconfigured or an unintentional bug is introduced, accidental overwrite or damage can happen to a few blocks. To help protect against these scenarios, you can take a share snapshot before you deploy new application code. When a bug or application error is introduced with the new deployment, you can go back to a previous version of your data on that file share.

- **Protection against accidental deletions or unintended changes.** Imagine that you're working on a text file in a file share. After the text file is closed, you lose the ability to undo your changes. In these cases, you then need to recover a previous version of the file. You can use share snapshots to recover previous versions of the file if it's accidentally renamed or deleted.
- **General backup purposes.** After you create a file share, you can periodically create a share snapshot of the file share to use it for data backup. A share snapshot, when taken periodically, helps maintain previous versions of data that can be used for future audit requirements or disaster recovery.

## Demonstration - File Shares

In this demonstration, we will work with files shares and snapshots.

**Note:** These steps require a storage account.

### Create a file share and upload a file

1. Access your storage account and click **Files**.
2. Click **+ File share** and give your new file share a **Name** and a **Quota**.
3. After your file share is created **Upload** a file.
4. Notice the ability to **Add a directory**, **Delete share**, and edit the **Quota**.

### Manage snapshots

1. Access your file share.
2. Select **Create Snapshot**.
3. Select **View Snapshots** and verify your snapshot was created.
4. Click the snapshot and verify it includes your uploaded file.
5. Click the file that is part of the snapshot and review the **File properties**.
6. Notice the choices to **Download** and **Restore** the snapshot file.
7. Access the file share and delete the file you previously uploaded.
8. **Restore** the file from the snapshot.

### Create a file share (PowerShell)

1. Gather the storage account name and the storage account key.

```
Get-AzStorageAccount | fl *name*
Get-AzStorageAccount -ResourceGroupName "YourResourceGroupName" -Name
"YourStorageAccountName"
```

2. Retrieve an access key for your storage account.

```
$storageAccountKeys = Get-AzStorageAccountKey -ResourceGroupName $resource-
GroupName -Name $storageAccountName
```

3. Create a context for your storage account and key. The context encapsulates the storage account name and account key.

```
$storageContext = New-AzStorageContext -StorageAccountName "YourStorageAc-
countName" -StorageAccountKey $storageAccountKeys[0].value
```

4. Create the file share. The name of your file share must be all lowercase.

```
$share = New-AzStorageShare "YourFileShareName" -Context $storageContext
```

### Mount a file share (PowerShell)

**Note:** Run the following commands from a regular (i.e. not an elevated) PowerShell session to mount the Azure file share. Remember to replace <your-resource-group-name>, <your-storage-account-name>, <your-file-share-name>, and desired-drive-letter with the proper information.

```
$resourceGroupName = "your-resource-group-name"
$storageAccountName = "your-storage-account-name"
$fileShareName = "your-file-share-name"

These commands require you to be logged into your Azure account, run
Login-AzAccount if you haven't
already logged in.
$storageAccount = Get-AzStorageAccount -ResourceGroupName $resourceGroupName
-Name $storageAccountName
$storageAccountKeys = Get-AzStorageAccountKey -ResourceGroupName $resource-
GroupName -Name $storageAccountName
$fileShare = Get-AzStorageShare -Context $storageAccount.Context | Where-Ob-
ject {
 $_.Name -eq $fileShareName -and $_.IsSnapshot -eq $false
}

if ($fileShare -eq $null) {
 throw [System.Exception]::new("Azure file share not found")
}

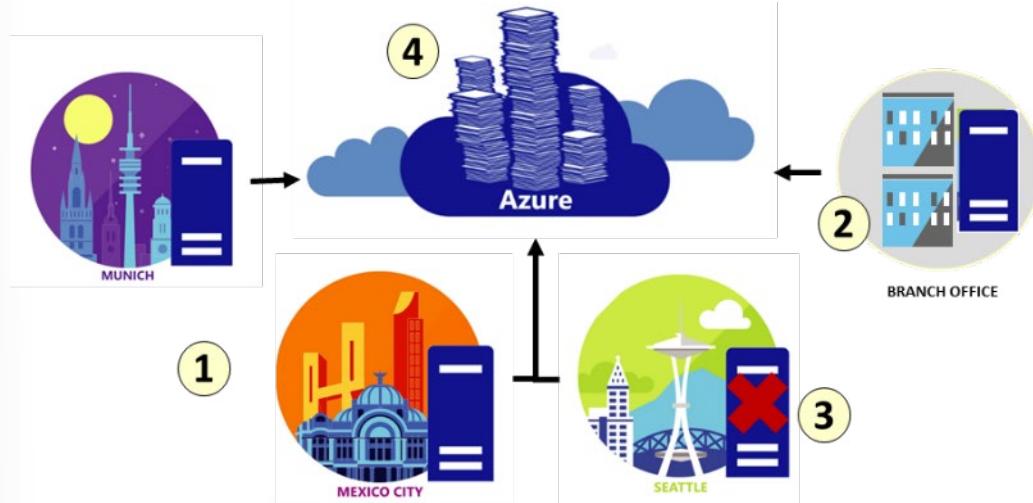
The value given to the root parameter of the New-PSDrive cmdlet is the
host address for the storage account,
storage-account.file.core.windows.net for Azure Public Regions. $fileShare.
StorageUri.PrimaryUri.Host is
used because non-Public Azure regions, such as sovereign clouds or Azure
Stack deployments, will have different
hosts for Azure file shares (and other storage resources).
$password = ConvertTo-SecureString -String $storageAccountKeys[0].Value
-AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -Argu-
mentList "AZURE\$($storageAccount.StorageAccountName)", $password
New-PSDrive -Name desired-drive-letter -PSPrinter FileSystem -Root
"\\"$(($fileShare.StorageUri.PrimaryUri.Host))\$($fileShare.Name)" -Credential
$credential -Persist
```

When finished, you can dismount the file share by running the following command:

```
Remove-PSDrive -Name desired-drive-letter
```

## Implement File Sync

Use **Azure File Sync** to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS. You can have as many caches as you need across the world.



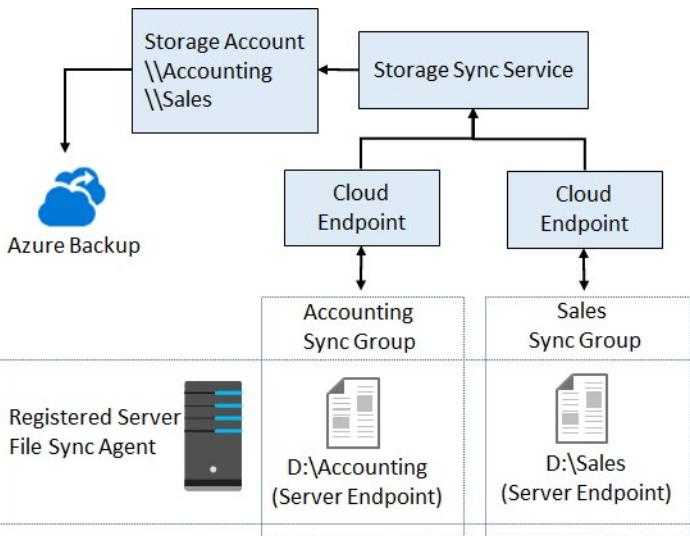
There are many uses and advantages to file sync.

1. **Lift and shift.** The ability to move applications that require access between Azure and on-premises systems. Provide write access to the same data across Windows Servers and Azure Files. This lets companies with multiple offices have a need to share files with all offices.
2. **Branch Offices.** Branch offices need to backup files, or you need to setup a new server that will connect to Azure storage.
3. **Backup and Disaster Recovery.** Once File Sync is implemented, Azure Backup will back up your on-premises data. Also, you can restore file metadata immediately and recall data as needed for rapid disaster recovery.
4. **File Archiving.** Only recently accessed data is located on local servers. Non-used data moves to Azure in what is called Cloud Tiering.

**Note:** Cloud tiering is an optional feature of Azure File Sync in which frequently accessed files are cached locally on the server while all other files are tiered to Azure Files based on policy settings. When a file is tiered, the Azure File Sync file system replaces the file locally with a pointer, or reparse point. The reparse point represents a URL to the file in Azure Files. When a user opens a tiered file, Azure File Sync seamlessly recalls the file data from Azure Files without the user needing to know that the file is actually stored in Azure. Cloud Tiering files will have greyed icons with an offline O file attribute to let the user know the file is only in Azure.

## Identify File Sync Components

To gain the most from Azure File Sync, it's important to understand the terminology.



**Storage Sync Service.** The Storage Sync Service is the top-level Azure resource for Azure File Sync. The Storage Sync Service resource is a peer of the storage account resource, and can similarly be deployed to Azure resource groups. A distinct top-level resource from the storage account resource is required because the Storage Sync Service can create sync relationships with multiple storage accounts via multiple sync groups. A subscription can have multiple Storage Sync Service resources deployed.

**Sync group.** A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. If for example, you have two distinct sets of files that you want to manage with Azure File Sync, you would create two sync groups and add different endpoints to each sync group. A Storage Sync Service can host as many sync groups as you need.

**Registered server.** The registered server object represents a trust relationship between your server (or cluster) and the Storage Sync Service. You can register as many servers to a Storage Sync Service instance as you want. However, a server (or cluster) can be registered with only one Storage Sync Service at a time.

**Azure File Sync agent.** The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share. The Azure File Sync agent has three main components:

- FileSyncSvc.exe: The background Windows service that is responsible for monitoring changes on server endpoints, and for initiating sync sessions to Azure.
- StorageSync.sys: The Azure File Sync file system filter, which is responsible for tiering files to Azure Files (when cloud tiering is enabled).
- PowerShell management cmdlets: PowerShell cmdlets that you use to interact with the Microsoft. StorageSync Azure resource provider. You can find these at the following (default) locations:
  - C:\\Program Files\\Azure\\StorageSyncAgent\\StorageSync.Management.PowerShell.Cmdlets.dll
  - C:\\Program Files\\Azure\\StorageSyncAgent\\StorageSync.Management.ServerCmdlets.dll

**Server endpoint.** A server endpoint represents a specific location on a registered server, such as a folder on a server volume. Multiple server endpoints can exist on the same volume if their namespaces do not overlap (for example, F:\\sync1 and F:\\sync2). You can configure cloud tiering policies individually for each server endpoint. You can create a server endpoint via a mountpoint. Note, mountpoints within the server endpoint are skipped. You can create a server endpoint on the system volume but, there are two limitations if you do so:

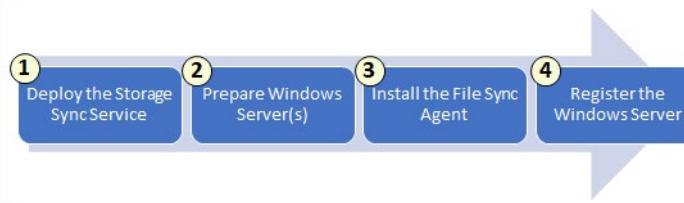
- Cloud tiering cannot be enabled.

- Rapid namespace restore (where the system quickly brings down the entire namespace and then starts to recall content) is not performed.

**Cloud endpoint.** A cloud endpoint is an Azure file share that is part of a sync group. The entire Azure file share syncs, and an Azure file share can be a member of only one cloud endpoint. Therefore, an Azure file share can be a member of only one sync group. If you add an Azure file share that has an existing set of files as a cloud endpoint to a sync group, the existing files are merged with any other files that are already on other endpoints in the sync group.

## Setup File Sync

There are several high-level steps for configuring File Sync.



1. **Deploy the Storage Sync Service.** The Storage Sync Service can be deployed from the Azure portal.

Home > Deploy Storage Sync

Deploy Storage Sync  X

\* Name: StorageSync1

\* Subscription: Visual Studio Enterprise

\* Resource group: ASH

Create new

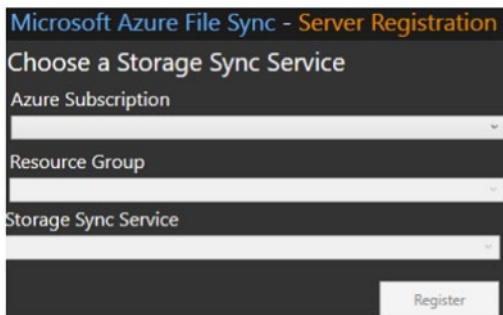
\* Location: South Central US

**Create** Automation options

You will need to provide Name, Subscription, Resource Group, and Location.

2. **Prepare Windows Server to use with Azure File Sync.** For each server that you intend to use with Azure File Sync, including server nodes in a Failover Cluster, you will need to configure the server. Preparation steps include temporarily disabling Internet Explorer Enhanced Security and ensuring you have latest PowerShell version.
3. **Install the Azure File Sync Agent.** The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share. The Azure File Sync agent installation package should install relatively quickly. We recommend that you keep the default installation path and that you enable Microsoft Update to keep Azure File Sync up to date.
4. **Register Windows Server with Storage Sync Service.** When the Azure File Sync agent installation is finished, the Server Registration UI automatically opens. Registering Windows Server with a Storage Sync Service establishes a trust relationship between your server (or cluster) and the Storage Sync

Service. Registration requires your Subscription ID, Resource Group, and Storage Sync Service (created



in step 1). A server (or cluster) can be registered with only one Storage Sync Service at a time.

**Note:** Once File Sync is configured you will need to configure file synchronization.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Your company is planning to store log data, crash dump files, and other diagnostic data for Azure VMs in Azure. Company administrators must be able to browse to the data in File Explorer. Access over SMB 3.0 must be supported. and the storage must support quotas. You need to choose the storage type to meet the requirements. Which storage type should you use? Select one.*

- Azure Files
- Table storage
- Blob storage

### Multiple choice

*Your company has a file server named FS01. The server has a single shared folder that users' access to shared files. The company wants to make the same files available from Microsoft Azure. Files deleted on either side (on-premises or cloud) should be automatically updated. You need to implement a solution to meet the requirements. What should you do? Select one.*

- Install and use AZCopy.
- Deploy Azure File Sync.
- Deploy storage tiering.

## Multiple choice

You've been asked by a local manufacturing company that runs dedicated software in their warehouse to keep track of stock. The software needs to run on machines in the warehouse, but the management team wants to access the output from the head office. The limited bandwidth available in the warehouse caused them problems in the past when they tried to use cloud-based solutions. You recommend that they use Azure Files. Which is the best method to sync the files with the cloud?

- Create an Azure Files share and directly mount shares on the machines in the warehouse.
- Use a machine in the warehouse to host a file share, install Azure File Sync, and share a drive with the rest of the warehouse.
- Install Azure File Sync on every machine in the warehouse and head office.

## Multiple choice

What is the Azure File Sync agent?

- It's installed on a server to enable Azure File Sync replication between the local file share and an Azure file share.
- It's installed on a server to set NTFS permissions on files and folders.
- It's installed on an Azure file share to control on-premises file and folder replication traffic.

## Multiple choice

In what order do you create the Azure resources needed to support Azure File Sync?

- Storage Sync Service, storage account, file share, and then the sync group.
- Storage account, file share, Storage Sync Service, and then the sync group.
- Storage account, file share, sync group, and then Storage Sync Service.

## Multiple choice

What is cloud tiering in Azure File Sync?

- It's a feature that archives infrequently accessed files to free up space on the local file share.
- It's a policy you create that prioritizes the sync order of file shares.
- It's a policy that sets the frequency at which the sync job runs.

## Multiple choice

What's the deployment process for Azure File Sync?

- Evaluate your on-premises system, create the Azure resources, install the Azure File Sync agent, register the on-premises server, and create the server endpoint.
- Create the Azure resources, install the Azure File Sync agent, register the on-premises server, and create the server endpoint.
- Evaluate your on-premises system, create the Azure resources, install the Azure File Sync agent on a virtual machine, register the on-premises server, and create the server endpoint.

# Summary and Resources

## Summary

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol. Azure File Sync is a service that allows you to cache several Azure file shares on an on-premises Windows Server or cloud VM.

You should now be able to:

- Identify when to use Azure files versus Azure Blobs.
- Configure Azure file shares and file share snapshots.
- Identify features and usage cases of Azure File Sync.
- Identify File Sync components and configuration steps.

## Learn more

You can learn more by reviewing the following.

- **Azure Files documentation<sup>21</sup>**
- **Planning for an Azure File Sync deployment<sup>22</sup>**
- **Learn - Store and share files in your app with Azure Files<sup>23</sup>**
- **Learn - Extend your on-premises file share capacity using Azure File Sync<sup>24</sup>**

<sup>21</sup> <https://docs.microsoft.com/azure/storage/files/>

<sup>22</sup> <https://docs.microsoft.com/azure/storage/files/storage-sync-files-planning>

<sup>23</sup> <https://docs.microsoft.com/learn/modules/store-and-share-with-azure-files/>

<sup>24</sup> <https://docs.microsoft.com/learn/modules/extend-share-capacity-with-azure-file-sync/>

# Configure Storage with Tools

## Introduction

### Scenario

Azure Administrators have many tools available for managing storage. You need to be efficient and select the best tool for the job.

### Skills measured

Storage management tools are part of **Exam AZ-104: Microsoft Azure Administrator<sup>25</sup>**.

Implement and manage storage (15–20%)

Manage storage

- Export from Azure job.
- Import into Azure job.
- Install and use Azure Storage Explorer.
- Copy data by using AZCopy.

### Learning objectives

In this module, you will learn how to:

- Configure and use Storage Explorer.
- Configure the Import and Export Service.
- Configure and use AZCopy.

### Prerequisites

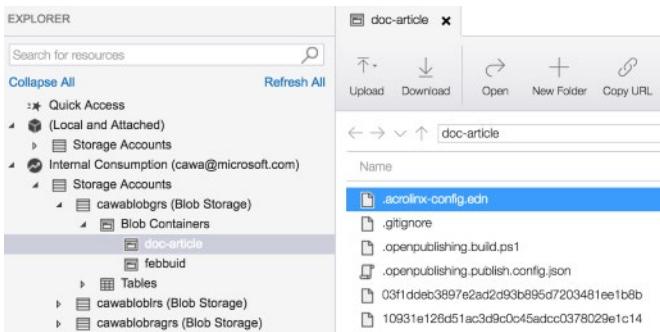
None.

## Use Storage Explorer

Azure Storage Explorer is a standalone app that makes it easy to work with Azure Storage data on Windows, macOS, and Linux. With Storage Explorer, you can access multiple accounts and subscriptions and manage all your storage content.

---

<sup>25</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>



To fully access resources after you sign in, Storage Explorer requires both management (Azure Resource Manager) and data layer permissions. This means that you need Azure Active Directory (Azure AD) permissions, which give you access to your storage account, the containers in the account, and the data in the containers.

## Connecting to storage

- Connect to storage accounts associated with your Azure subscriptions.
- Connect to storage accounts and services that are shared from other Azure subscriptions.
- Connect to and manage local storage by using the Azure Storage Emulator.



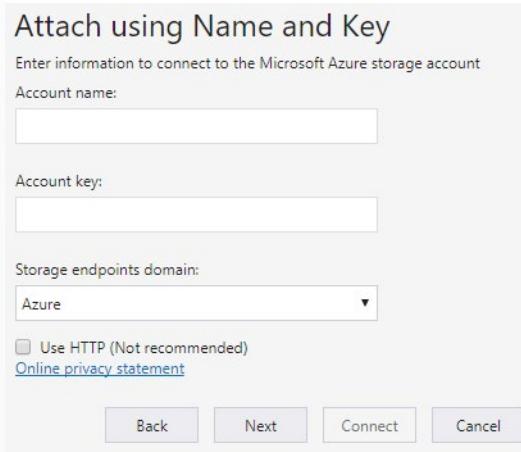
In addition, you can work with storage accounts in global and national Azure:

- **Connect to an Azure subscription.** Manage storage resources that belong to your Azure subscription.
- **Work with local development storage.** Manage local storage by using the Azure Storage Emulator.
- **Attach to external storage.** Manage storage resources that belong to another Azure subscription or that are under national Azure clouds by using the storage account's name, key, and endpoints (shown below.)
- **Attach a storage account by using an SAS.** Manage storage resources that belong to another Azure subscription by using a shared access signature (SAS).
- **Attach a service by using an SAS.** Manage a specific storage service (blob container, queue, or table) that belongs to another Azure subscription by using an SAS.

- **Connect to an Azure Cosmos DB account by using a connection string.** Manage Cosmos DB account by using a connection string.

## Accessing external storage accounts

As mentioned previously, Storage Explorer lets you attach to external storage accounts so that storage accounts can be easily shared. To create the connection you will need the storage **Account name** and **Account key**. In the portal, the account key is called **key1**.



To use a name and key from a national cloud, use the **Storage endpoints domain** drop-down to select **Other** and then enter the custom storage endpoint domain.

**Note:** Access keys provide access to the entire storage account. Store your access keys securely. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines.

## Use the Import and Export Service

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files. With the Azure Import/Export service, you supply your own disk drives and transfer data yourself.

## Usage Cases

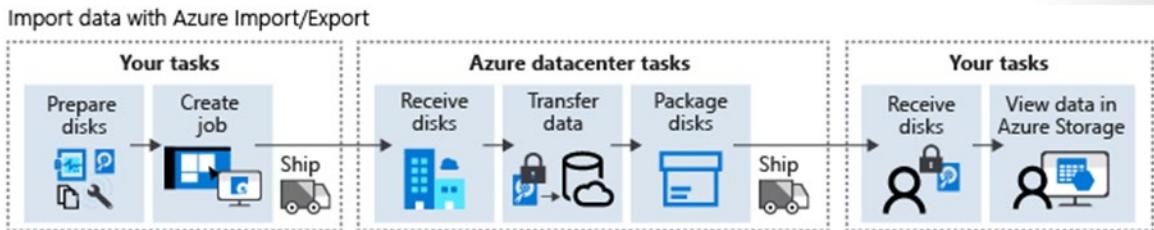
Consider using Azure Import/Export service when uploading or downloading data over the network is too slow or getting more network bandwidth is cost-prohibitive. Scenarios where this would be useful include:

- **Migrating data to the cloud.** Move large amounts of data to Azure quickly and cost effectively.
- **Content distribution.** Quickly send data to your customer sites.
- **Backup.** Take backups of your on-premises data to store in Azure blob storage.

- **Data recovery.** Recover large amount of data stored in blob storage and have it delivered to your on-premises location.

## Import Jobs

An Import job securely transfers large amounts of data to Azure Blob storage (block and page blobs) and Azure Files by shipping disk drives to an Azure datacenter. In this case, you will be shipping hard drives containing your data.



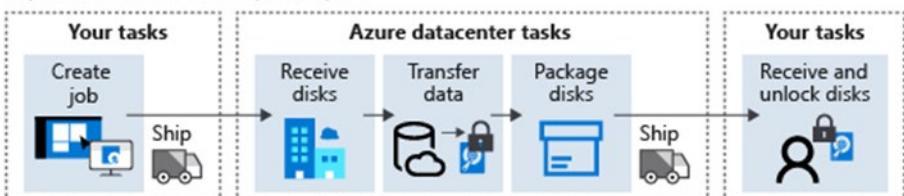
In order to perform an import, follow these steps:

- Create an Azure Storage account.
- Identify the number of disks that you will need to accommodate all the data that you want to transfer.
- Identify a computer that you will use to perform the data copy, attach physical disks that you will ship to the target Azure datacenter, and install the WAIimportExport tool.
- Run the WAIimportExport tool to copy the data, encrypt the drive with BitLocker, and generate journal files.
- Use the Azure portal to create an import job referencing the Azure Storage account. As part of the job definition, specify the destination address representing the Azure region where the Azure Storage account resides.
- Ship the disks to the destination that you specified when creating the import job and update the job by providing the shipment tracking number.
- Once the disks arrive at the destination, the Azure datacenter staff will carry out data copy to the target Azure Storage account and ship the disks back to you.

## Export Jobs

Export jobs transfer data from Azure storage to hard disk drives and ship to your on-premise sites.

Export data with Azure Import/Export



In order to perform an export, follow these steps:

- Identify the data in the Azure Storage blobs that you intend to export.
- Identify the number of disks that you will need to accommodate all the data you want to transfer.

- Use the Azure portal to create an export job referencing the Azure Storage account. As part of the job definition, specify the blobs you want to export, the return address, and your carrier account number. Microsoft will ship your disks back to you after the export process is complete.
- Ship the required number of disks to the Azure region hosting the storage account. Update the job by providing the shipment tracking number.
- Once the disks arrive at the destination, Azure datacenter staff will carry out data copy from the storage account to the disks that you provided, encrypt the volumes on the disks by using BitLocker, and ship them back to you. The BitLocker keys will be available in the Azure portal, allowing you to decrypt the content of the disks and copy them to your on-premises storage.

## Import/Export Tool (WAImpoerExport)

The **Azure Import/Export Tool** is the drive preparation and repair tool that you can use with the Microsoft Azure Import/Export service. You can use the tool for the following functions:

- Before creating an import job, you can use this tool to copy data to the hard drives you are going to ship to an Azure datacenter.
- After an import job has completed, you can use this tool to repair any blobs that were corrupted, were missing, or conflicted with other blobs.
- After you receive the drives from a completed export job, you can use this tool to repair any files that were corrupted or missing on the drives.

Import/Export service requires the use of internal SATA II/III HDDs or SSDs. Each disk contains a single NTFS volume that you encrypt with BitLocker when preparing the drive. To prepare a drive, you must connect it to a computer running a 64-bit version of the Windows client or server operating system and run the WAImpoerExport tool from that computer. The WAImpoerExport tool handles data copy, volume encryption, and creation of journal files. Journal files are necessary to create an import/export job and help ensure the integrity of the data transfer.

**Note:** You can create jobs directly from the Azure portal or you can accomplish this programmatically by using Azure Storage Import/Export REST API.

## Use AzCopy

An alternative method for transferring data is **AzCopy**. AzCopy v10 is the next-generation command-line utility for copying data to/from Microsoft Azure Blob and File storage, which offers a redesigned command-line interface and new architecture for high-performance reliable data transfers. Using AzCopy, you can copy data between a file system and a storage account, or between storage accounts.

## New features

Synchronize a file system to Azure Blob or vice versa. Ideal for incremental copy scenarios.

- Supports Azure Data Lake Storage Gen2 APIs.
- Supports copying an entire account (Blob service only) to another account.
- Account to account copy is now using the new Put from URL APIs. No data transfer to the client is needed which makes the transfer faster.
- List/Remove files and blobs in a given path.
- Supports wildcard patterns in a path, –include flags, and –exclude flags.

- Improved resiliency: every AzCopy instance will create a job order and a related log file. You can view and restart previous jobs and resume failed jobs. AzCopy will also automatically retry a transfer after a failure.
- General performance improvements.

## Authentication options

- **Azure Active Directory** (Supported for Blob and ADLS Gen2 services). Use .\azcopy login to sign in using Azure Active Directory. The user should have *Storage Blob Data Contributor* role assigned to write to Blob storage using Azure Active Directory authentication.
- **SAS tokens** (supported for Blob and File services). Append the SAS token to the blob path on the command line to use it.

## Getting started

AzCopy has a simple self-documented syntax. Here's how you can get a list of available commands:

```
AzCopy /?
```

The basic syntax for AzCopy commands is:

```
azcopy copy [source] [destination] [flags]
```

**Note:** AzCopy is available on Windows, Linux, and macOS.

## Demonstration - Storage Explorer

**Note:** If you have an older version of the Storage Explorer, be sure to upgrade.

**Note:** For the demonstration we will only configure a basic storage account connection.

In this demonstration, we will review several common Azure Storage Explorer tasks.

### Download and install Storage Explorer

**Note:** Storage Explorer is available through the portal, if you prefer to use that for the demonstration.

1. Download and install Azure Storage Explorer - <https://azure.microsoft.com/features/storage-explorer/>
2. After the installation, launch the tool.
3. Review the Release Notes and menu options.

### Connect to an Azure subscription

1. In Storage Explorer, select **Manage Accounts**, second icon top left. This will take you to the Account Management Panel.
2. The left pane now displays all the Azure accounts you've signed in to. To connect to another account, select **Add an account**.
3. If you want to sign into a national cloud or an Azure Stack, click on the Azure environment dropdown to select which Azure cloud you want to use.
4. Once you have chosen your environment, click the **Sign in...** button.

5. After you successfully sign in with an Azure account, the account and the Azure subscriptions associated with that account are added to the left pane.
6. Select the Azure subscriptions that you want to work with, and then select **Apply**.
7. The left pane displays the storage accounts associated with the selected Azure subscriptions.

**Note:** This next section requires an Azure storage account.

#### Attach an Azure storage account

1. Access the Azure portal, and your storage account.
2. Explore the choice for **Storage Explorer**.
3. Select **Access keys** and read the information about using the keys.
4. To connect in Storage Explorer, you will need the **Storage account name** and **Key1** information.
5. In Storage Explorer, **Add an account**.
6. Paste your account name in the Account name text box, paste your account key (the key1 value from the Azure portal) into the Account key text box, and then select **Next**.
7. Verify your storage account is available in the navigation pane. You may need to refresh the page.
8. Right-click your storage account and notice the choices including **Open in portal**, **Copy primary key**, and **Add to Quick Access**.

#### Generate a SAS connection string for the account you want to share

1. In **Storage Explorer**, right-click the storage account you want share, and then select **Get Shared Access Signature**.
2. Specify the time frame and permissions that you want for the account, and then click the **Create** button.
3. Next to the Connection String text box, select **Copy** to copy it to your clipboard, and then click **Close**.

#### Attach to a storage account by using a SAS Connection string

1. In **Storage Explorer**, open the **Connect Dialog**.
2. Choose **Use a connection string** and then click **Next**.
3. Paste your connection string into the **Connection string:** field. The **Display name:** field should populate. Click the **Next** button.
4. Verify the information is correct and select **Connect**.
5. After the storage account has successfully been attached, the storage account is displayed in the **Local and Attached** node with **(SAS)** appended to its name.

## Demonstration - AzCopy

In this demonstration, we will explore AzCopy.

#### Install the AzCopy tool

1. Download your version of AZCopy - **Get started with AZCopy<sup>26</sup>**
2. Install and launch the tool.

---

<sup>26</sup> <https://docs.microsoft.com/azure/storage/common/storage-use-azcopy-v10>

## Explore the help

1. View the help.

```
azcopy /?
```

2. Scroll to the top of the Help information and read about the **Common options**, like: source, destination, source key, and destination key.
3. Scroll down the **Samples** section. We will be trying several of these examples. Are any of these examples particularly interesting to you?

## Download a blob from Blob storage to the file system

**Note:** This example requires an Azure storage account with blob container and blob file. You will also need to capture parameters in a text editor like Notepad.

1. Access the Azure portal.
2. Access your storage account with the blob you want to download.
3. Select **Access keys** and copy the **Key Key1** value. This will be the *sourcekey*: value.
4. Drill down to the blob of interest, and view the file **Properties**.
5. Copy the **URL** information. This will be the *source*: value.
6. Locate a local destination directory. This will be the *dest*: value. A filename is also required.
7. Construct the command using your values.

```
azcopy /source:sourceURL /dest:destinationdirectoryandfilename /sourcekey:"key"
```

8. If you have errors, read them carefully and make corrections.
9. Verify the blob was downloaded to your local directory.

## Upload files to Azure blob storage

**Note:** The example continues from the previous example and requires a local directory with files.

1. The *source*: for the command will be a local directory with files.
2. The *dest*: will the blob URL used in the previous example. Be sure to remove the filename, just include the storage account and container.
3. The *destkey*: will the key used in the previous example.
4. Construct the command using your values.

```
azcopy /source:source /dest:destinationcontainer /destkey:key
```

5. If you have errors, read them carefully and make corrections.
6. Verify your local files were copied to the Azure container.
7. Notice there are switches to recurse subdirectories and pattern match.

## Knowledge Check

Choose the best response for each question.

### Multiple choice

*The manufacturing company's finance department wants to control how the data is being transferred to Azure Files. They want a graphical tool to manage the process, but they don't want to use the Azure portal. What tool do you recommend they use?*

- Azure Data Box
- Robocopy
- Azure Storage Explorer

### Multiple choice

*You have an existing storage account in Microsoft Azure. It stores unstructured data. You create a new storage account. You need to move half of the data from the existing storage account to the new storage account. What tool should you use? Select one.*

- Use the Azure portal
- Use the Robocopy command-line tool
- Use the AzCopy command-line tool

### Multiple choice

*You want to quickly upload the data in a collection of small files held in a local folder to blob storage. This is a one-off request. You don't want to overwrite blobs that have been modified in the last two days. Which tool should you use?*

- Azure CLI
- AzCopy
- Azure Storage Explorer

### Multiple choice

*You want to transfer a series of large files to blob storage. It may take several hours to upload each file, and you're concerned that if a transfer fails, it shouldn't have to restart from the beginning. Which tool is the most appropriate to do this task?*

- Azure CLI
- AzCopy
- Azure Storage Explorer

# Summary and Resources

## Summary

Azure provides several tools for working with the data in your storage accounts.

You should now be able to:

- Configure and use Storage Explorer.
- Configure the Import and Export Service.
- Configure and use AZCopy.

## Learn more

You can learn more by reviewing the following.

- **Get started with Storage Explorer<sup>27</sup>**
- **Azure Import and Export Service<sup>28</sup>**
- **Get started with AZCopy<sup>29</sup>**
- **Learn - Upload, download, and manage data with Azure Storage Explorer<sup>30</sup>**
- **Learn - Copy and move blobs from one container or storage account to another from the command line and in code<sup>31</sup>**
- **Learn - Monitor, diagnose, and troubleshoot your Azure storage<sup>32</sup>**
- **Learn - Export large amounts of data from Azure by using Azure Import/Export<sup>33</sup>**

<sup>27</sup> <https://docs.microsoft.com/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows>

<sup>28</sup> <https://azure.microsoft.com/documentation/articles/storage-import-export-service/>

<sup>29</sup> <https://docs.microsoft.com/azure/storage/common/storage-use-azcopy>

<sup>30</sup> <https://docs.microsoft.com/learn/modules/upload-download-and-manage-data-with-azure-storage-explorer/>

<sup>31</sup> <https://docs.microsoft.com/learn/modules/copy-blobs-from-command-line-and-code/>

<sup>32</sup> <https://docs.microsoft.com/learn/modules/monitor-diagnose-and-troubleshoot-azure-storage/>

<sup>33</sup> <https://docs.microsoft.com/learn/modules/export-data-with-azure-import-export/>

# Module 07 Lab

## Lab 07 - Manage Azure Storage

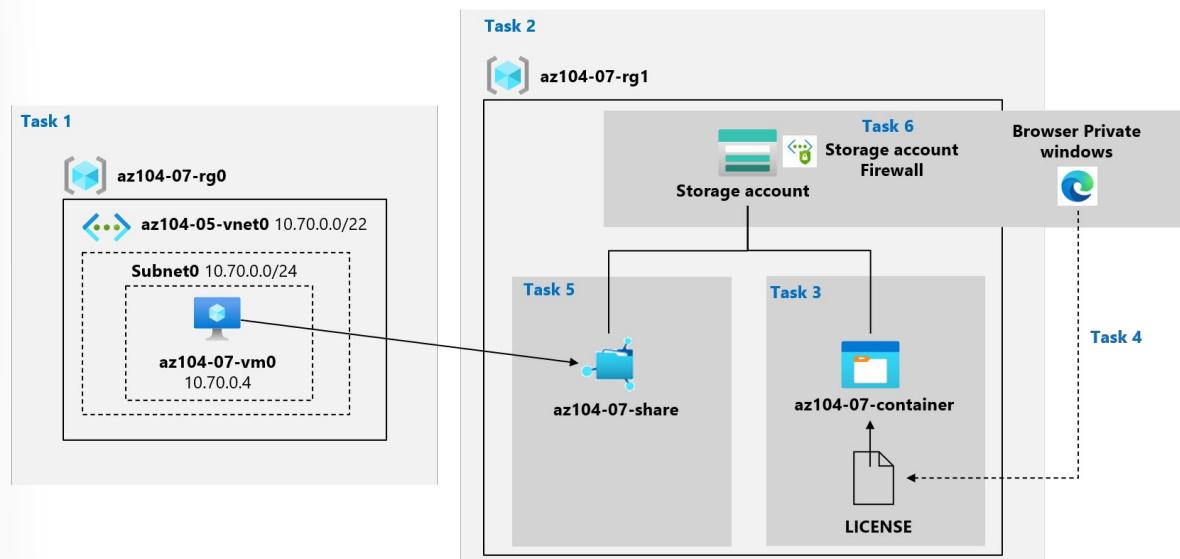
### Lab scenario

You need to evaluate the use of Azure storage for storing files residing currently in on-premises data stores. While majority of these files are not accessed frequently, there are some exceptions. You would like to minimize cost of storage by placing less frequently accessed files in lower-priced storage tiers. You also plan to explore different protection mechanisms that Azure Storage offers, including network access, authentication, authorization, and replication. Finally, you want to determine to what extent Azure Files service might be suitable for hosting your on-premises file shares.

### Objectives

In this lab, you will:

- Task 1: Provision the lab environment.
- Task 2: Create and configure Azure Storage accounts.
- Task 3: Manage blob storage.
- Task 4: Manage authentication and authorization for Azure Storage.
- Task 5: Create and configure an Azure Files shares.
- Task 6: Manage network access for Azure Storage.



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Answers

## Multiple choice

Which of the following replicates your data to a secondary region, maintains six copies of your data, and is the default replication option? Select one.

- Locally-redundant storage
- Read-access geo-redundant storage
- Zone-redundant storage

### Explanation

*Read-access geo-redundant storage (GRS) is the default replication option.*

## Multiple choice

You have two video files stored as blobs. One of the videos is business-critical and requires a replication policy that creates multiple copies across geographically diverse datacenters. The other video is non-critical, and a local replication policy is sufficient. Which of the following options would satisfy both data diversity and cost sensitivity consideration?

- Create a single storage account that makes use of Local-redundant storage (LRS) and host both videos from here.
- Create a single storage account that makes use of Geo-redundant storage (GRS) and host both videos from here.
- Create two storage accounts. The first account makes use of Geo-redundant storage (GRS) and hosts the business-critical video content. The second account makes use of Local-redundant storage (LRS) and hosts the non-critical video content.

### Explanation

*Create two storage accounts. The first account makes use of Geo-redundant storage (GRS) and hosts the business-critical video content. The second account makes use of Local-redundant storage (LRS) and hosts the non-critical video content. In general, increased diversity means an increased number of storage accounts. A storage account by itself has no financial cost. However, the settings you choose for the account do influence the cost of services in the account. Use multiple storage accounts to reduce costs.*

## Multiple choice

The name of a storage account must be:

- Unique within the containing resource group.
- Unique within your Azure subscription.
- Globally unique.

### Explanation

*Globally unique. The storage account name is used as part of the URI for API access, so it must be globally unique.*

**Multiple choice**

In a typical project, when would you create your storage account(s)?

- At the beginning, during project setup.
- After deployment, when the project is running.
- At the end, during resource cleanup.

*Explanation*

*At the beginning, during project setup. Storage accounts are stable for the lifetime of a project. It's common to create them at the start of a project.*

**Multiple choice**

A manufacturing company has several sensors that record time-relative data. Only the most recent data is useful. The company wants the lowest cost storage for this data. What is the best kind of storage account for them?

- LRS
- GRS
- ZRS

*Explanation*

*LRS. This option is the best because it's the lowest cost, the data is being continuously created, and data loss isn't an issue.*

**Multiple choice**

Which of these changes between access tiers will happen immediately?

- Hot to Cool
- Archive to Cool
- Archive to Hot

*Explanation*

*Hot to Cool. Changes between Hot and Cool, and to Archive, happen immediately.*

**Multiple choice**

You work for an open-source development company. You use Microsoft Azure for a variety of storage needs. Up to now, all the storage was used for internal purposes only. It is organized in block blobs. Each block blob is in its own container. Each container is set to default settings. In total, you have 50 block blobs. The company has decided to provide read access to the data in the block blobs, as part of releasing more information about their open-source development efforts. All block blobs must be readable by anonymous internet users. You need to configure the storage to meet the requirements. What should you do? Select one.

- Create a new container, move all the blobs to the new container, and then set the public access level to Blob.
- Set the public access level to Blob on all the existing containers.
- Create a new access key for the storage account and then provide the connection string in the storage connectivity information to the public.

*Explanation*

*Create a new container, move all the blobs to the new container, and then set the public access level to Blob. You should create a new container, move the existing blobs, and then set the public access level to Blob. In the future, when access changes are required, you can configure the single container (which would contain all blobs).*

**Multiple choice**

Your company provides cloud software to audit administrative access in Microsoft Azure resources. The software logs all administrative actions (including all clicks and text input) to log files. The software is about to be released from beta and the company is concerned about storage performance. You need to deploy a storage solution for the log files to maximize performance. What should you do? Select one.

- Deploy Azure Files using SMB 3.0.
- Deploy blob storage using block blobs.
- Deploy blob storage using append blobs.

*Explanation*

*Deploy blob storage using append blobs. Append blobs optimize append operations (writes adding onto a log file, for example). The company needs to write data to log files, most often appending data (until a new log file is generated).*

**Multiple choice**

Your company is building an app in Azure. The storage must be reachable programmatically through a REST API. The storage must be globally redundant. The storage must be accessible privately within the company's Azure environment. The storage must be optimal for unstructured data. Which type of Azure storage should you use for the app? Select one.

- Azure Table Storage
- Azure Blob Storage
- Azure File Storage

*Explanation*

*Azure Blob Storage. Azure Blob Storage is optimal for unstructured data and meets the requirements for the company's app.*

**Multiple choice**

You are using blob storage. Which of the following is true? Select one.

- The cool access tier is for frequent access of objects in the storage account.
- The hot access tier is for storing large amounts of data that is infrequently accessed.
- You can switch between hot and cool performance tiers at any time.

*Explanation*

*You can switch between performance tiers at any time. Changing the account storage tier from cool to hot incurs a charge equal to reading all the data existing in the storage account. However, changing the account storage tier from hot to cool incurs a charge equal to writing all the data into the cool tier (GPv2 accounts only).*

**Multiple choice**

You use a Microsoft Azure storage account for storing large numbers of video and audio files. You create containers to store each type of file and want to limit access to those files for specific periods. Additionally, the files can only be accessed through shared access signatures (SAS). You need the ability to revoke access to the files and to change the period for which users can access the files. What should you do to accomplish this in the most simple and effective way? Select one.

- Create an SAS for each user and delete the SAS when you want to prevent access.
- Implement stored access policies for each container to enable revocation of access or change of duration.
- Periodically regenerate the account key to control access to the files.

*Explanation*

*You should implement stored access policies which will let you change access based on permissions or duration by replacing the policy with a new one or deleting it altogether to revoke access. While Azure RMS would protect the files, there would be administrative complexity involved whereas stored access policies achieve the goal in the simplest way. Creating a SAS for each user would also involve a great amount of administrative overhead. Regenerating keys would prevent all users from accessing all files at the same time.*

**Multiple choice**

You need to provide a contingent staff employee temporary read-only access to the contents of an Azure storage account container named media. It is important that you grant access while adhering to the security principle of least-privilege. What should you do? Select one.

- Set the public access level to Container.
- Generate a shared access signature (SAS) token for the container.
- Configure a Cross-Origin Resource Sharing (CORS) rule for the storage account.

*Explanation*

*You should generate a SAS token for the container which provides access either to entire containers or blobs. You should not share the Etag with the contingent staff member. Azure uses Etags to control concurrent access to resources and do not deliver the appropriate security controls. Setting the public access level to Container would not conform to the principle of least privilege as the container now becomes open to public connections with no time limitation. CORS is a Hypertext Transfer Protocol (HTTP) mechanism that enables cross-domain resource access but does not provide security-based resource access control.*

**Multiple choice**

You are planning a delegation model for your Azure storage. The company has issued the following requirement for Azure storage access: -Apps in the non-production environment must have automated time-limited access. You need to configure storage access to meet the requirements. What should you do?

- Use shared access signatures for the non-production apps.
- Use access keys for the non-production apps.
- Use Stored Access Policies for the production apps..

*Explanation*

*Use shared access signatures for the non-production apps. Shared access signatures provide a way to provide more granular storage access than access keys. For example, you can limit access to "read only" and you can limit the services and types of resources. Shared access signatures can be configured for a specified amount of time, which meets the scenario's requirements.*

**Multiple choice**

You are planning a delegation model for your Azure storage. The company requires apps in the production environment to have unrestricted access to storage resources You need to configure storage access to meet the requirements. What should you do?

- Use shared access signatures for the production apps.
- Use access keys for the production apps.
- Use Stored Access Policies for the production apps.

*Explanation*

*Access keys provide unrestricted access to the storage resources, which is the requirement for production apps in this scenario.*

**Multiple choice**

When configuring network access to your Azure Storage Account, what is the default network rule?

- To allow all connections from all networks
- To allow all connection from a private IP address range
- To deny all connections from all networks

*Explanation*

*To allow all connections from all networks. The default network rule is to allow all connections from all networks.*

**Multiple choice**

Your organization has data stored in hard drives. It wants to move this data into a secure Azure storage solution. What solution would allow you to encrypt this data with minimal effort?

- Azure Disk Encryption.
- Azure Storage Service Encryption.
- Client-side encryption with Azure.

*Explanation*

*Azure Storage Service Encryption. Storage Service Encryption allows encryption on all data stored on storage accounts. Encryption is enabled by default.*

**Multiple choice**

Your company is planning to store log data, crash dump files, and other diagnostic data for Azure VMs in Azure. Company administrators must be able to browse to the data in File Explorer. Access over SMB 3.0 must be supported. and the storage must support quotas. You need to choose the storage type to meet the requirements. Which storage type should you use? Select one.

- Azure Files
- Table storage
- Blob storage

*Explanation*

Azure Files supports SMB 3.0, is reachable via File Explorer, and supports quotas. The other storage types do not support the requirements. While blob storage is good for unstructured data, it cannot be accessed over SMB 3.0.

**Multiple choice**

Your company has a file server named FS01. The server has a single shared folder that users' access to shared files. The company wants to make the same files available from Microsoft Azure. Files deleted on either side (on-premises or cloud) should be automatically updated. You need to implement a solution to meet the requirements. What should you do? Select one.

- Install and use AZCopy.
- Deploy Azure File Sync.
- Deploy storage tiering.

*Explanation*

In this scenario, only Azure File sync can keep FS01 and Azure synced up and maintaining the same data. While AZCopy can copy data, it isn't a sync solution to have both sources maintain the exact same files. Storage tiering is used for internal tiering (SSD and HDD, for example). While DFS Replication could fit here, DFS Namespace doesn't offer the replication component. Storage Explorer is a tool for managing different storage platforms.

**Multiple choice**

You've been asked by a local manufacturing company that runs dedicated software in their warehouse to keep track of stock. The software needs to run on machines in the warehouse, but the management team wants to access the output from the head office. The limited bandwidth available in the warehouse caused them problems in the past when they tried to use cloud-based solutions. You recommend that they use Azure Files. Which is the best method to sync the files with the cloud?

- Create an Azure Files share and directly mount shares on the machines in the warehouse.
- Use a machine in the warehouse to host a file share, install Azure File Sync, and share a drive with the rest of the warehouse.
- Install Azure File Sync on every machine in the warehouse and head office.

*Explanation*

Use a machine in the warehouse to host a file share, install Azure File Sync, and share a drive with the rest of the warehouse. This answer is the best because the low bandwidth means Azure File Sync will handle the updating and syncing of files efficiently over the low-bandwidth network.

**Multiple choice**

What is the Azure File Sync agent?

- It's installed on a server to enable Azure File Sync replication between the local file share and an Azure file share.
- It's installed on a server to set NTFS permissions on files and folders.
- It's installed on an Azure file share to control on-premises file and folder replication traffic.

*Explanation*

*It's installed on a server to enable Azure File Sync replication between the local file share and an Azure file share. Azure File Sync agent is a downloadable package that enables a Windows Server file share to be synced with an Azure file share.*

**Multiple choice**

In what order do you create the Azure resources needed to support Azure File Sync?

- Storage Sync Service, storage account, file share, and then the sync group.
- Storage account, file share, Storage Sync Service, and then the sync group.
- Storage account, file share, sync group, and then Storage Sync Service.

*Explanation*

*Storage account, file share, Storage Sync Service, and then the sync group. Create the storage account, and then create a file share within the storage account. Create the Storage Sync Service, and then create the sync group within the Storage Sync Service.*

**Multiple choice**

What is cloud tiering in Azure File Sync?

- It's a feature that archives infrequently accessed files to free up space on the local file share.
- It's a policy you create that prioritizes the sync order of file shares.
- It's a policy that sets the frequency at which the sync job runs.

*Explanation*

*It's a feature that archives infrequently accessed files to free up space on the local file share. Cloud tiering allows frequently accessed files to be cached on the local server. Infrequently accessed files are tiered, or archived, to the Azure file share according to the policy you create.*

**Multiple choice**

What's the deployment process for Azure File Sync?

- Evaluate your on-premises system, create the Azure resources, install the Azure File Sync agent, register the on-premises server, and create the server endpoint.
- Create the Azure resources, install the Azure File Sync agent, register the on-premises server, and create the server endpoint.
- Evaluate your on-premises system, create the Azure resources, install the Azure File Sync agent on a virtual machine, register the on-premises server, and create the server endpoint.

*Explanation*

*Evaluate your on-premises system, create the Azure resources, install the Azure File Sync agent, register the on-premises server, and create the server endpoint. Verify that your on-premises server's OS and file system are supported. Then create the required resources in Azure. On the local server, install the Azure File Sync agent and register the server. Finally, create the server endpoint in Azure.*

**Multiple choice**

The manufacturing company's finance department wants to control how the data is being transferred to Azure Files. They want a graphical tool to manage the process, but they don't want to use the Azure portal. What tool do you recommend they use?

- Azure Data Box
- Robocopy
- Azure Storage Explorer

*Explanation*

*Azure Storage Explorer. This option is the best if the finance department doesn't want to use the Azure portal.*

**Multiple choice**

You have an existing storage account in Microsoft Azure. It stores unstructured data. You create a new storage account. You need to move half of the data from the existing storage account to the new storage account. What tool should you use? Select one.

- Use the Azure portal
- Use the Robocopy command-line tool
- Use the AzCopy command-line tool

*Explanation*

*Use the AzCopy command-line tool. The key in this scenario is that you need to move data between storage accounts. The AzCopy tool can work with two different storage accounts. The other tools do not copy data between storage accounts. Alternatively, although not one of the answer choices, you can use Storage Explorer to copy data between storage accounts.*

**Multiple choice**

You want to quickly upload the data in a collection of small files held in a local folder to blob storage. This is a one-off request. You don't want to overwrite blobs that have been modified in the last two days. Which tool should you use?

- Azure CLI
- AzCopy
- Azure Storage Explorer

*Explanation*

*Azure CLI. The Azure CLI is great choice for one-off file transfers and can be used to check the last modified date.*

**Multiple choice**

You want to transfer a series of large files to blob storage. It may take several hours to upload each file, and you're concerned that if a transfer fails, it shouldn't have to restart from the beginning. Which tool is the most appropriate to do this task?

- Azure CLI
- AzCopy
- Azure Storage Explorer

*Explanation*

AzCopy. AzCopy is ideal for transferring large files as it can run in the background, and you can monitor the status AzCopy jobs.



## Module 8 Adminster Azure Virtual Machines

### Configure Virtual Machines

#### Introduction

#### Scenario

Suppose you work for a company doing consumer research and you're responsible for managing the on-premises servers. The servers you administer run all the company infrastructure, from web servers to databases. However, the hardware is aging and starting to struggle to keep up with some of the new data analysis applications being deployed to it. Rather than upgrade the hardware, the company has decided to deploy Azure virtual machines.

You are responsible for deploying the new virtual machines. Your deployment tasks will include correctly sizing the machines, selecting storage, and configuring networking.

#### Skills measured

Deploying virtual machine is part of **Exam AZ-104: Microsoft Azure Administrator<sup>1</sup>**.

Deploy and manage Azure compute resources (20–25%)

Configure VMs

- Move VMs from one resource group to another.
- Manage VM sizes.
- Add data disks.
- Configure networking.
- Redeploy VMs.

---

<sup>1</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

## Learning objectives

In this module, you will learn how to:

- Create a virtual machine planning checklist.
- Determine virtual machine locations and pricing models.
- Determine the correct virtual machine size.
- Configure virtual machine storage.

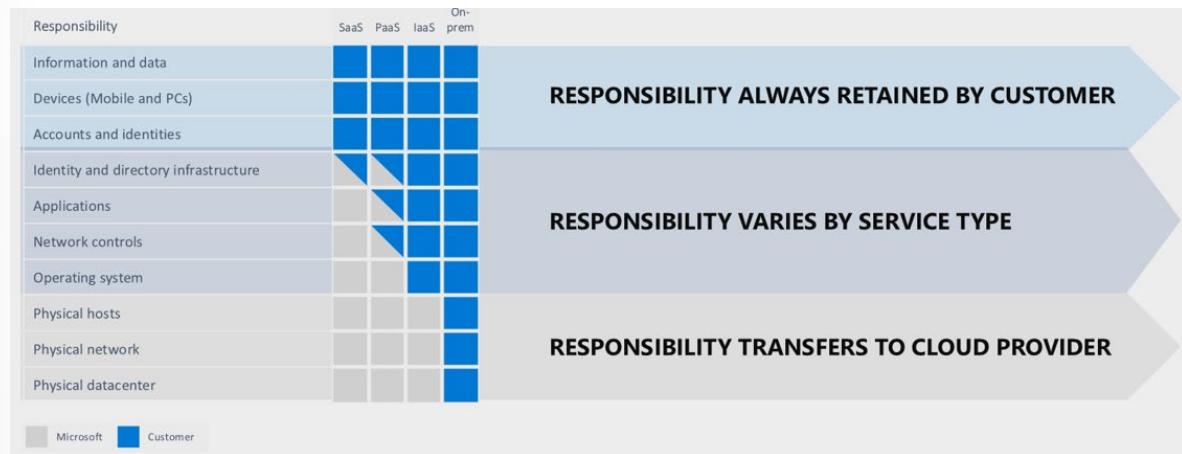
## Prerequisites

None.

## Review Cloud Services Responsibilities

Azure Virtual Machines is one of several types of on-demand, scalable computing resources that Azure offers. Typically, you'll choose a virtual machine if you need more control over the computing environment than the choices such as App Service or Cloud Services offer. Azure Virtual Machines provide you with an operating system, storage, and networking capabilities and can run a wide range of applications.

Virtual machines are part of the Infrastructure as a Service (IaaS) offering. IaaS is an instant computing infrastructure, provisioned and managed over the Internet. Quickly scale up and down with demand and pay only for what you use.



## IaaS business scenarios

- **Test and development.** Teams can quickly set up and dismantle test and development environments, bringing new applications to market faster. IaaS makes it quick and economical to scale up dev-test environments up and down.
- **Website hosting.** Running websites using IaaS can be less expensive than traditional web hosting.
- **Storage, backup, and recovery.** Organizations avoid the capital outlay for storage and complexity of storage management, which typically requires a skilled staff to manage data and meet legal and compliance requirements. IaaS is useful for handling unpredictable demand and steadily growing storage needs. It can also simplify planning and management of backup and recovery systems.

- **High-performance computing.** High-performance computing (HPC) on supercomputers, computer grids, or computer clusters helps solve complex problems involving millions of variables or calculations. Examples include earthquake and protein folding simulations, climate and weather predictions, financial modeling, and evaluating product designs.
- **Big data analysis.** Big data is a popular term for massive data sets that contain potentially valuable patterns, trends, and associations. Mining data sets to locate or tease out these hidden patterns requires a huge amount of processing power, which IaaS economically provides.
- **Extended Datacenter.** Add capacity to your datacenter by adding virtual machines in Azure instead of incurring the costs of physically adding hardware or space to your physical location. Connect your physical network to the Azure cloud network seamlessly.

**Note:** Are you using virtual machines in Azure? What scenarios are of interest to you?

## Plan Virtual Machines

Provisioning VMs to Azure requires planning.

- Start with the network
- Name the VM
- Decide the location for the VM
- Determine the size of the VM
- Understanding the pricing model
- Storage for the VM
- Select an operating system

### Start with the network

Virtual networks (VNets) are used in Azure to provide private connectivity between Azure Virtual Machines and other Azure services. VMs and services that are part of the same virtual network can access one another. By default, services outside the virtual network cannot connect to services within the virtual network. You can, however, configure the network to allow access to the external service, including your on-premises servers.

This latter point is why you should spend some time thinking about your network configuration. Network addresses and subnets are not trivial to change once you have them set up, and if you plan to connect your private company network to the Azure services, you will want to make sure you consider the topology before putting any VMs into place.

### Name the VM

One piece of information people often don't put much thought into is the name of the VM. The VM name is used as the computer name, which is configured as part of the operating system. You can specify a name of up to 15 characters on a Windows VM and 64 characters on a Linux VM.

This name also defines a manageable Azure resource, and it's not trivial to change later. That means you should choose names that are meaningful and consistent, so you can easily identify what the VM does. A good convention is to include the following information in the name:

| Element            | Example                    | Notes                                                                      |
|--------------------|----------------------------|----------------------------------------------------------------------------|
| Environment        | dev, prod, QA              | Identifies the environment for the resource                                |
| Location           | uw (US West), ue (US East) | Identifies the region into which the resource is deployed                  |
| Instance           | 01, 02                     | For resources that have more than one named instance (web servers, etc.)   |
| Product or Service | service                    | Identifies the product, application, or service that the resource supports |
| Role               | sql, web, messaging        | Identifies the role of the associated resource                             |

For example, `devusc-webvm01` might represent the first development web server hosted in the US South Central location.

## Decide the location for the VM

Azure has datacenters all over the world filled with servers and disks. These datacenters are grouped into geographic regions ('West US', 'North Europe', 'Southeast Asia', etc.) to provide redundancy and availability.

When you create and deploy a virtual machine, you must select a region where you want the resources (CPU, storage, etc.) to be allocated. The region lets you locate your VMs as close as possible to your users to improve performance and to meet any legal, compliance, or tax requirements.

## Considerations for the location

- **The location can limit your available options.** Each region has different hardware available and some configurations are not available in all regions.
- **There are price differences between locations.** If your workload isn't bound to a specific location, it can be very cost effective to check your required configuration in multiple regions to find the lowest price.

## Know the pricing options

There are two separate costs the subscription will be charged for every VM: compute and storage. By separating these costs, you scale them independently and only pay for what you need.

**Compute costs** - Compute expenses are priced on a per-hour basis but billed on a per-minute basis. For example, you are only charged for 55 minutes of usage if the VM is deployed for 55 minutes. You are not charged for compute capacity if you stop and deallocate the VM since this releases the hardware. The hourly price varies based on the VM size and OS you select. The cost for a VM includes the charge for the Windows operating system. Linux-based instances are cheaper because there is no operating system license charge.

**Storage costs** - You are charged separately for the storage the VM uses. The status of the VM has no relation to the storage charges. Even when a VM is stopped/deallocated, you are charged for the storage used by the disks.

You're able to choose from two payment options for compute costs:

1. **Consumption-based** - With the consumption-based option, you pay for compute capacity by the second. You're able to increase or decrease compute capacity on demand and start or stop at any time. Use this option if you run applications with short-term or unpredictable workloads that cannot be interrupted. For example, if you are doing a quick test, or developing an app in a VM, this would be the appropriate option.
2. **Reserved Virtual Machine Instances** - The Reserved Virtual Machine Instances (RI) option is an advance purchase of a virtual machine for one or three years in a specified region. The commitment is made up front, and in return, you get up to 72% price savings compared to pay-as-you-go pricing. RIs are flexible and can easily be exchanged or returned for an early termination fee. Use this option if the VM has to run continuously, or you need budget predictability, and you can commit to using the VM for at least a year.

## Determine Virtual Machine Sizing

Once you have the name and location set, you need to decide on the size of your VM. Rather than specify processing power, memory, and storage capacity independently, Azure provides different VM sizes that offer variations of these elements in different sizes. Azure provides a wide range of VM size options allowing you to select the appropriate mix of compute, memory, and storage for what you want to do.

The best way to determine the appropriate VM size is to consider the type of workload your VM needs to run. Based on the workload, you're able to choose from a subset of available VM sizes. Workload options are classified as follows on Azure:

| Series | Purpose                                    | Example Usage                                                                                                                                                                                                        |
|--------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A      | Entry-level economical VMs for dev or test | Development and test servers, low traffic web servers, small to medium databases, servers for proof-of-concepts, and code repositories.                                                                              |
| B      | Economical burstable VMs                   | Development and test servers, low-traffic web servers, small databases, micro services, servers for proof-of-concepts, build servers.                                                                                |
| D      | General purpose compute                    | Enterprise-grade applications, relational databases, in-memory caching, and analytics. The latest generations are ideal for applications that demand faster CPUs, better local disk performance, or higher memories. |

| Series    | Purpose                                             | Example Usage                                                                                                                                                                                                                                                              |
|-----------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dc        | Protect data in use                                 | Confidential querying in databases, creation of scalable confidential consortium networks, and secure multiparty machine learning algorithms. The DC-series VMs are ideal to build secure enclave-based applications to protect customers code and data while it's in use. |
| E         | Optimized for in-memory hyper-threaded applications | SAP HANA (E64s_v3 only), SAP S/4 HANA application layer, SAP NetWeaver application layer, SQL Hekaton, and other large in-memory business critical workloads.                                                                                                              |
| F         | Compute optimized virtual machines                  | Batch processing, web servers, analytics, and gaming.                                                                                                                                                                                                                      |
| G         | Memory and storage optimized virtual machines       | Large SQL and NoSQL databases, ERP, SAP, and data warehousing solutions.                                                                                                                                                                                                   |
| H         | High-Performance Computing virtual machines         | Fluid dynamics, finite element analysis, seismic processing, reservoir simulation, risk analysis, electronic design automation, rendering, Spark, weather modeling, quantum simulation, computational chemistry, heat transfer simulation.                                 |
| L         | Storage optimized virtual machines                  | NoSQL databases such as Cassandra, MongoDB, Cloudera, and Redis. Data warehousing applications and large transactional databases are great use cases as well.                                                                                                              |
| M and Mv2 | Memory optimized virtual machines                   | SAP HANA, SAP S/4 HANA, SQL Hekaton and other large in-memory business critical workloads requiring massive parallel compute power.                                                                                                                                        |
| N         | GPU enabled virtual machines                        | Simulation, deep learning, graphics rendering, video editing, gaming, and remote visualization.                                                                                                                                                                            |

## Resizing virtual machines

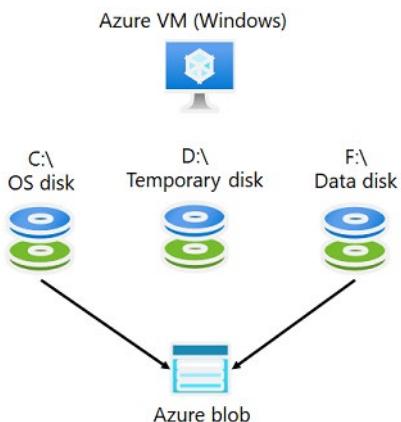
Azure allows you to change the VM size when the existing size no longer meets your needs. You can resize a VM if your current hardware configuration is allowed in the new size. This provides a fully agile and elastic approach to VM management.

When you stop and deallocate the VM, you can select any size available in your region.

**Note:** Be cautious when resizing production VMs. Resizing may require a restart that can cause a temporary outage or change configuration settings like the IP address.

## Determine Virtual Machine Storage

Just like any other computer, virtual machines in Azure use disks as a place to store an operating system, applications, and data. All Azure virtual machines have at least two disks – a Windows operating system disk (in the case of a Windows VM) and a temporary disk. Virtual machines also can have one or more data disks. All disks are stored as VHDs.



## Operating System Disks

Every virtual machine has one attached operating system disk. That OS disk has a pre-installed OS, which was selected when the VM was created. It's registered as a SATA drive and labeled as the C: drive by default.

## Temporary Disk

Every VM contains a temporary disk, which is not a managed disk. The temporary disk provides short-term storage for applications and processes and is intended to only store data such as page or swap files. Data on the temporary disk may be lost during a maintenance event or when you redeploy a VM. During a standard reboot of the VM, the data on the temporary drive should persist. However, there are cases where the data may not persist, such as moving to a new host. Therefore, any data on the temp drive should not be data that is critical to the system.

- On Windows virtual machines, this disk is labeled as the D: drive by default and it used for storing pagefile.sys.
- On Linux virtual machines, the disk is typically /dev/sdb and is formatted and mounted to /mnt by the Azure Linux Agent.

**Note:** Don't store data on the temporary disk. It provides temporary storage for applications and processes and is intended to only store data such as page or swap files.

## Data Disks

A data disk is a managed disk that's attached to a virtual machine to store application data, or other data you need to keep. Data disks are registered as SCSI drives and are labeled with a letter that you choose. Each data disk has a maximum capacity of 4,095 gibibytes (GiB). The size of the virtual machine determines how many data disks you can attach to it and the type of storage you can use to host the disks.

## Virtual Machine Storage Options

Azure Premium Storage delivers high-performance, low-latency disk support for virtual machines (VMs) with input/output (I/O)-intensive workloads. VM disks that use Premium Storage store data on solid-state drives (SSDs). To take advantage of the speed and performance of premium storage disks, you can migrate existing VM disks to Premium Storage.

In Azure, you can attach several premium storage disks to a VM. Using multiple disks gives your applications up to 256 TB of storage per VM. With Premium Storage, your applications can achieve 80,000 I/O operations per second (IOPS) per VM, and a disk throughput of up to 2,000 megabytes per second (MB/s) per VM. Read operations give you low latencies.

Azure offers two ways to create premium storage disks for VMs:

### Unmanaged disks

The original method is to use unmanaged disks. In an unmanaged disk, you manage the storage accounts that you use to store the virtual hard disk (VHD) files that correspond to your VM disks. VHD files are stored as page blobs in Azure storage accounts.

### Managed disks

An Azure-managed disk is a virtual hard disk (VHD). You can think of it like a physical disk in an on-premises server but, virtualized. Azure-managed disks are stored as page blobs, which are a random IO storage object in Azure. We call a managed disk 'managed' because it is an abstraction over page blobs, blob containers, and Azure storage accounts. With managed disks, all you have to do is provision the disk, and Azure takes care of the rest. When you select to use Azure-managed disks with your workloads, Azure creates and manages the disk for you. The available types of disks are Ultra Solid State Drives (SSD), Premium SSD, Standard SSD, and Standard Hard Disk Drives (HDD).

For the best performance for your application, we recommend that you migrate any VM disk that requires high IOPS to Premium Storage. If your disk does not require high IOPS, you can help limit costs by keeping it in standard Azure Storage. In standard storage, VM disk data is stored on hard disk drives (HDDs) instead of on SSDs.

**Note:** Managed disks are required for the single instance virtual machine SLA (99.95%).

## Create Virtual Machines in the Portal

When you are creating virtual machines in the portal, one of your first decisions is the image to use. Azure supports Windows and Linux operating systems. There are server and client platforms.



Additional images are available by searching the Marketplace.

After selecting your image, the portal will guide you through additional configuration information.

### Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

**Basic** - Project details, Administrator account, Inbound port rules

**Disks** - OS disk type, data disks

**Networking** - Virtual networks, load balancing

**Management** - Monitoring, Auto-shutdown, Back up

**Advanced** - Add additional configuration, agents, scripts, or applications via virtual machine extensions or cloud-init.

## Demonstration - Create Virtual Machines

In this demonstration, we will create and access a Windows virtual machine in the portal.

### Create the virtual machine

**Note:** These steps only cover a few virtual machine parameters. Feel free to explore and cover other areas. Note: These steps only cover a few virtual machine parameters. Feel free to explore and cover other areas.

1. Choose **Create a resource** in the upper left-hand corner of the Azure portal.
2. In the search box above the list of Azure Marketplace resources, search for **Windows Server 2016 Datacenter**. After locating the image, click **Create**.
3. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and then choose to **Create new** resource group. Type *myResourceGroup* for the name.
4. Under **Instance details**, type *myVM* for the **Virtual machine name** and choose *East US* for your **Location**. Leave the other defaults.

5. Under **Administrator account**, provide a username, such as *azureuser* and a password. The password must be at least 12 characters long and meet the defined complexity requirements.
6. Under **Inbound port rules**, choose **Allow selected ports** and then select **RDP (3389)** and **HTTP** from the drop-down.
7. Move to the **Management** tab, and under **Monitoring** turn **Off** Boot Diagnostics. This will eliminate validation errors.
8. Leave the remaining defaults and then select the **Review + create** button at the bottom of the page. Wait for the validation, then click **Create**.

### Connect to the virtual machine

Create a remote desktop connection to the virtual machine. These directions tell you how to connect to your VM from a Windows computer. On a Mac, you need to install an RDP client from the Mac App Store.

1. Select the **Connect** button on the virtual machine properties page.
2. In the **Connect to virtual machine** page, keep the default options to connect by DNS name over port 3389 and click **Download RDP file**.
3. Open the downloaded RDP file and select **Connect** when prompted.
4. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as *localhost\username*, enter password you created for the virtual machine, and then select **OK**.
5. You may receive a certificate warning during the sign-in process. Select **Yes** or **Continue** to create the connection.

### Install web server

1. To observe your VM in action, install the IIS web server. Open a PowerShell prompt on the VM and run the following command:

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

2. After IIS has installed, close the RDP connection to the VM.

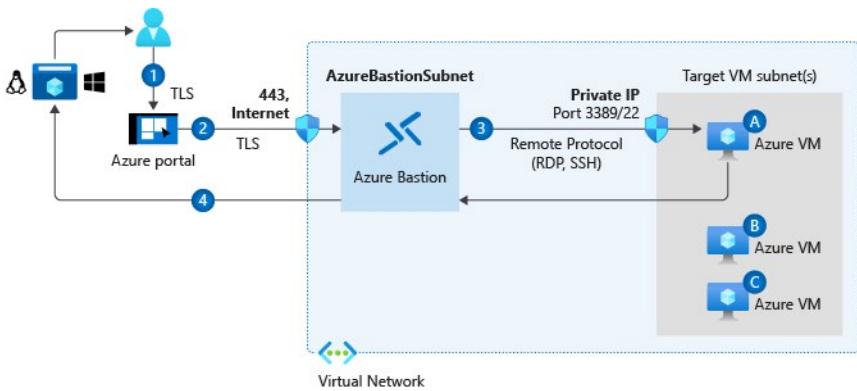
### View the IIS welcome page

1. In the portal, select the VM and in the overview of the VM, use the **Click to copy** button to the right of the public IP address to copy it and paste it into a browser tab.
2. The default IIS welcome page will open.

**Note:** When no longer needed, you can delete the resource group, virtual machine, and all related resources. To do so, select the resource group for the virtual machine, select **Delete**, then confirm the name of the resource group to delete.

## Connect to Virtual Machines

There are several ways to access your virtual machines in Azure.



## Windows-based virtual machines

You'll use the remote desktop client to connect to the Windows-based VM hosted on Azure. Most versions of Windows natively contain support for the remote desktop protocol (RDP).

## Linux-based virtual machines

To connect to a Linux-based VM, you need a secure shell protocol (SSH) client. For example, PuTTY which is a free and open-source terminal emulator, serial console and network file transfer application. PuTTY supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection. It can also connect to a serial port.

## Bastion Connections

The Azure Bastion service is a new fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over SSL. When you connect via Azure Bastion, your virtual machines do not need a public IP address.

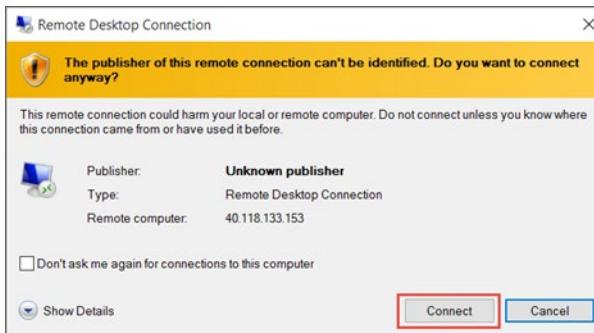
Bastion provides secure RDP and SSH connectivity to all VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world while still providing secure access using RDP/SSH. With Azure Bastion, you connect to the virtual machine directly from the Azure portal. You don't need an additional client, agent, or piece of software.

## Connect to Windows Virtual Machines

To manage an Azure Windows VM, you can use the same set of tools that you used to deploy it. However, you will also want to interact with an operating system (OS) running within the VM. The methods you can use to accomplish this are OS-specific and include the following options:

- **Remote Desktop Protocol (RDP)** allows you to establish a graphical user interface (GUI) session to an Azure VM that runs any supported version of Windows. The Azure portal automatically enables the **Connect button** on the Azure Windows VM blade if the VM is running and accessible via a public or private IP address, and if it accepts inbound traffic on TCP port 3389. After you click this button, the portal will automatically provision an RDP file, which you can either open or download. Opening the file initiates an RDP connection to the corresponding VM. You will get a warning that the RDP file is from an unknown publisher. Certificate warnings are expected. When connecting be sure to use

credentials for the virtual machine. The Azure PowerShell **Get-AzRemoteDesktopFile** cmdlet provides the same functionality.



- **Windows Remote Management (WinRM)** allows you to establish a command-line session to an Azure VM that runs any supported version of Windows. You can also use WinRM to run noninteractive Windows PowerShell scripts. WinRM facilitates additional session security by using certificates. You can upload a certificate that you intend to use to Azure Key Vault prior to establishing a session. The process of setting up WinRM connectivity includes the following, high-level steps:
  - Creating a key vault.
  - Creating a self-signed certificate.
  - Uploading the certificate to the key vault.
  - Identifying the URL of the certificate uploaded to the key vault.
  - Referencing the URL in the Azure VM configuration.

**Note:** By default, WinRM uses TCP port 5986. You can change the port. Ensure whatever port you are using is not blocked by network security group rules.

## Connect to Linux Virtual Machines

When you create a Linux VM, you can decide to authenticate with an **SSH public key** or **Password**.

A screenshot of the Azure portal's 'Create a Linux VM' form. It shows fields for 'Administrator account', 'Authentication type' (set to 'SSH public key'), 'Username', and 'SSH public key'. A tooltip for the 'SSH public key' field explains: 'Provide an RSA public key in the single-line format (starting with "ssh-rsa") or the multi-line PEM format. You can generate SSH keys using ssh-keygen on Linux and OS X, or PuTTYGen on Windows.' A green checkmark icon is next to the 'SSH public key' input field. At the bottom, there is a link 'Learn more about creating and using SSH keys in Azure'.

## SSH connections

SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections. SSH is the default connection protocol for Linux VMs hosted in Azure. Although SSH itself provides an encrypted connection, using passwords with SSH connections still leaves the VM vulnerable to brute-force

attacks or guessing of passwords. A more secure and preferred method of connecting to a VM using SSH is by using a public-private key pair, also known as SSH keys.

- The **public key** is placed on your Linux VM, or any other service that you wish to use with public-key cryptography.
- The **private key** remains on your local system. Protect this private key. Do not share it.

When you use an SSH client to connect to your Linux VM (which has the public key), the remote VM tests the client to make sure it possesses the private key. If the client has the private key, it's granted access to the VM.

Depending on your organization's security policies, you can reuse a single public-private key pair to access multiple Azure VMs and services. You do not need a separate pair of keys for each VM or service you wish to access.

Your public key can be shared with anyone, but only you (or your local security infrastructure) should possess your private key.

**Note:** Azure currently requires at least a 2048-bit key length and the SSH-RSA format for public and private keys.

## Demonstration - Connect to Linux Virtual Machines

In this demonstration, we will create a Linux machine and access the machine with SSL.

**Note:** Ensure port 22 is open for the connection to work.

### Create the SSH Keys

1. Download the PuTTY tool. This will include PuTTYgen - <https://putty.org/>.
2. Once installed, open the **PuTTYgen** program.
3. In the **Parameters** option group choose **RSA**.
4. Click the **Generate** button.
5. Move your mouse around the blank area in the window to generate some randomness.
6. Copy the text of the **Public key for pasting into authorized keys file**.
7. Optionally you can specify a **Key passphrase** and then **Confirm passphrase**. You will be prompted for the passphrase when you authenticate to the VM with your private SSH key. Without a passphrase, if someone obtains your private key, they can sign in to any VM or service that uses that key. We recommend you create a passphrase. However, if you forget the passphrase, there is no way to recover it.
8. Click **Save private key**.
9. Choose a location and filename and click **Save**. You will need this file to access the VM.

### Create the Linux machine and assign the public SSH key

1. In the portal create a Linux machine of your choice.
2. Choose **SSH Public Key** for the **Authentication type** (instead of **Password**).
3. Provide a **Username**.
4. Paste the public SSH key from PuTTY into the **SSH public key** text area. Ensure the key validates with a checkmark.

5. Create the VM. Wait for it to deploy.
6. Access the running VM.
7. From the **Overview** blade, click **Connect**.
8. Remember your login information including user and public IP address.

#### Access the server using SSH

1. Open the **PuTTY** tool.
2. Enter **username@publicIpAddress** where username is the value you assigned when creating the VM and publicIpAddress is the value you obtained from the Azure portal.
3. Specify **22** for the **Port**.
4. Choose **SSH** in the **Connection Type** option group.
5. Navigate to **SSH** in the Category panel, then click **Auth**.
6. Click the **Browse** button next to **Private key file for authentication**.
7. Navigate to the private key file saved when you generated the SSH keys and click **Open**.
8. From the main PuTTY screen click **Open**.
9. You will now be connected to your server command line.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*You are planning to deploy several Linux VMs in Azure. The security team issues a policy that Linux VMs must use an authentication system other than passwords. You need to deploy an authentication method for the Linux VMs to meet the requirement. Which authentication method should you use? Select one.*

- SSH key pair
- Access keys
- Shared access signature

### Multiple choice

*Your organization has a security policy that prohibits exposing SSH ports to the outside world. You need to connect to an Azure Linux virtual machine to install software. What should you do? Select one.*

- Configure the Bastion service
- Configure a Guest configuration on the virtual machine
- Create a custom script extension

## Multiple choice

*What is the effect of the default network security settings for a new virtual machine?*

- Neither outbound nor inbound requests are allowed.
- Outbound request is allowed. Inbound traffic is only allowed from within the virtual network.
- There are no restrictions: all outbound and inbound requests are allowed.

## Multiple choice

*You have several Linux virtual machines hosted in Azure. You will administer these VMs remotely over SSH from three dedicated machines in your corporate headquarters. Which of the following authentication methods would typically be considered best-practice for this situation?*

- Username and password
- Private key
- Private key with passphrase

## Multiple choice

*You want to run a network appliance on a virtual machine. Which workload option should you choose?*

- Compute optimized
- Memory optimized
- Storage optimized

# Summary and Resources

## Summary

Azure Virtual Machines (VM) is one of several types of on-demand, scalable computing resources that Azure offers. Typically, you choose a VM when you need more control over the computing environment than the other choices offer.

You should now be able to:

- Determine virtual machine names, locations and pricing models.
- Determine the correct virtual machine size.
- Configure virtual machine storage.
- Create a virtual machine in the Azure portal.
- Select a secure virtual machine connection method.
- Configure Windows and Linux virtual machine connections.

## Learn more

You can learn more by reviewing the following.

- [Azure Virtual Machine documentation<sup>2</sup>](https://docs.microsoft.com/azure/virtual-machines/)
- [Linux virtual machines documentation<sup>3</sup>](https://docs.microsoft.com/azure/virtual-machines/linux/)
- [Learn - Introduction to Azure virtual machines<sup>4</sup>](https://docs.microsoft.com/learn/modules/intro-to-azure-virtual-machines/)
- [Learn - Deploy Azure virtual machines from VHD templates<sup>5</sup>](https://docs.microsoft.com/learn/modules/deploy-vms-from-vhd-templates/)
- [Learn - Choose the right disk storage for your virtual machine workload<sup>6</sup>](https://docs.microsoft.com/learn/modules/choose-the-right-disk-storage-for-vm-workload/)
- [Learn - Add and size disks in Azure virtual machines<sup>7</sup>](https://docs.microsoft.com/learn/modules/add-and-size-disks-in-azure-virtual-machines/)
- [Learn - Create a Linux virtual machine in Azure<sup>8</sup>](https://docs.microsoft.com/learn/modules/create-linux-virtual-machine-in-azure/)
- [Learn - Create a Windows virtual machine in Azure<sup>9</sup>](https://docs.microsoft.com/learn/modules/create-windows-virtual-machine-in-azure/)
- [Learn - Connect to virtual machines through the Azure portal by using Azure Bastion<sup>10</sup>](https://docs.microsoft.com/learn/modules/connect-vm-with-azure-bastion/)

---

<sup>2</sup> <https://docs.microsoft.com/azure/virtual-machines/>

<sup>3</sup> <https://docs.microsoft.com/azure/virtual-machines/linux/>

<sup>4</sup> <https://docs.microsoft.com/learn/modules/intro-to-azure-virtual-machines/>

<sup>5</sup> <https://docs.microsoft.com/learn/modules/deploy-vms-from-vhd-templates/>

<sup>6</sup> <https://docs.microsoft.com/learn/modules/choose-the-right-disk-storage-for-vm-workload/>

<sup>7</sup> <https://docs.microsoft.com/learn/modules/add-and-size-disks-in-azure-virtual-machines/>

<sup>8</sup> <https://docs.microsoft.com/learn/modules/create-linux-virtual-machine-in-azure/>

<sup>9</sup> <https://docs.microsoft.com/learn/modules/create-windows-virtual-machine-in-azure/>

<sup>10</sup> <https://docs.microsoft.com/learn/modules/connect-vm-with-azure-bastion/>

# Configure Virtual Machine Availability

## Introduction

### Scenario

Managing virtual machines at scale can be challenging, especially when usage patterns vary and demands on applications fluctuate. You want to be able to adjust your virtual machine resources to match demands. At the same time, you want to keep the virtual machine configuration consistent to ensure application stability. Achieving these goals means you maintain throughput and responsiveness while minimizing the costs of continually running a large collection of virtual machines.

Your company website uses virtual machines and manages large workloads. The IT department wants to ensure the virtual machines can dynamically adjust to increases and decreases in workloads. They also want to ensure there is a business continuity plan to provide for highly available machines.

You need to deploy highly available virtual machines. You decide to use virtual machine scale sets and autoscale.

### Skills measured

High availability and scaling of virtual machine is part of **Exam AZ-104: Microsoft Azure Administrator<sup>11</sup>**.

Deploy and manage Azure compute resources (20–25%)

Configure VMs

- Configure high availability.
- Deploy and configure scale sets.

### Learning objectives

In this module, you will learn how to:

- Implement availability sets and availability zones.
- Implement update and fault domains.
- Implement virtual machine scale sets.
- Autoscale virtual machines.

### Prerequisites

None.

## Plan for Maintenance and Downtime

As an Azure administrator you must be prepared for planned and unplanned failures. There are three scenarios that can lead to your virtual machine in Azure being impacted: unplanned hardware maintenance, unexpected downtime, and planned maintenance.

<sup>11</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>



An **Unplanned Hardware Maintenance** event occurs when the Azure platform predicts that the hardware or any platform component associated to a physical machine, is about to fail. When the platform predicts a failure, it will issue an unplanned hardware maintenance event. Azure uses Live Migration technology to migrate the Virtual Machines from the failing hardware to a healthy physical machine. Live Migration is a VM preserving operation that only pauses the Virtual Machine for a short time, but performance might be reduced before and/or after the event.

**Unexpected Downtime** is when the hardware or the physical infrastructure for the virtual machine fails unexpectedly. Unexpected downtime can include local network failures, local disk failures, or other rack level failures. When detected, the Azure platform automatically migrates (heals) your virtual machine to a healthy physical machine in the same datacenter. During the healing procedure, virtual machines experience downtime (reboot) and in some cases loss of the temporary drive.

**Planned Maintenance** events are periodic updates made by Microsoft to the underlying Azure platform to improve overall reliability, performance, and security of the platform infrastructure that your virtual machines run on. Most of these updates are performed without any impact upon your Virtual Machines or Cloud Services.

**Note:** Microsoft does not automatically update your VM's OS or software. You have complete control and responsibility for that. However, the underlying software host and hardware are periodically patched to ensure reliability and high performance.

**Note:** What plans do you have to minimize the effect of downtime?

## Setup Availability Sets

An **Availability Set** is a logical feature used to ensure that a group of related VMs are deployed so that they aren't all subject to a single point of failure and not all upgraded at the same time during a host operating system upgrade in the datacenter. VMs placed in an availability set should perform an identical set of functionalities and have the same software installed.

Azure ensures that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or Azure software failure occurs, only a subset of your VMs are impacted. Your application stays up and continues to be available to your customers.

Availability Sets are an essential capability when you want to build reliable cloud solutions. Keep these general principles in mind.

- For redundancy, configure multiple virtual machines in an Availability Set.
- Configure each application tier into separate Availability Sets.
- Combine a Load Balancer with Availability Sets.
- Use managed disks with the virtual machines.

You create Availability Sets through the Azure portal in the disaster recovery section. Also, you can build Availability Sets using Resource Manager templates, scripting, or API tools.

Instance details

|                   |                                                |
|-------------------|------------------------------------------------|
| Name *            | <input type="text" value="avset01"/>           |
| Region *          | <input type="text" value="(US) East US"/>      |
| Fault domains     | <input type="text" value="2"/>                 |
| Update domains    | <input type="text" value="5"/>                 |
| Use managed disks | <input checked="" type="radio"/> Yes (Aligned) |

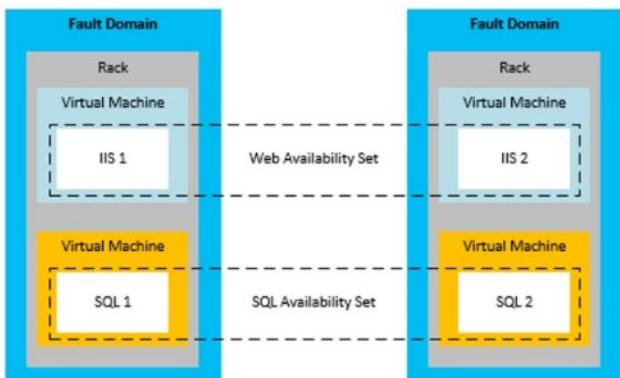
## Service Level Agreements

- For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time.
- For all Virtual Machines that have two or more instances deployed in the same Availability Set, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.95% of the time.
- For any Single Instance Virtual Machine using premium storage for all Operating System Disks and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 99.9%.

**Note:** You can create a virtual machine and an Availability Set at the same time. A VM can only be added to an Availability Set when it is created. To change the Availability Set, you need to delete and then recreate the virtual machine.

## Review Update and Fault Domains

Update Domains and Fault Domains helps Azure maintain high availability and fault tolerance when deploying and upgrading applications. Each virtual machine in an availability set is placed in one update domain and two fault domains.



## Update domains

An **upgrade domain (UD)** is a group of nodes that are upgraded together during the process of a service upgrade (rollout). An update domain allows Azure to perform incremental or rolling upgrades across a deployment. Each update domain contains a set of virtual machines and associated physical hardware that can be updated and rebooted at the same time. During planned maintenance, only one

update domain is rebooted at a time. By default, there are five (non-user-configurable) update domains, but you configure up to 20 update domains.

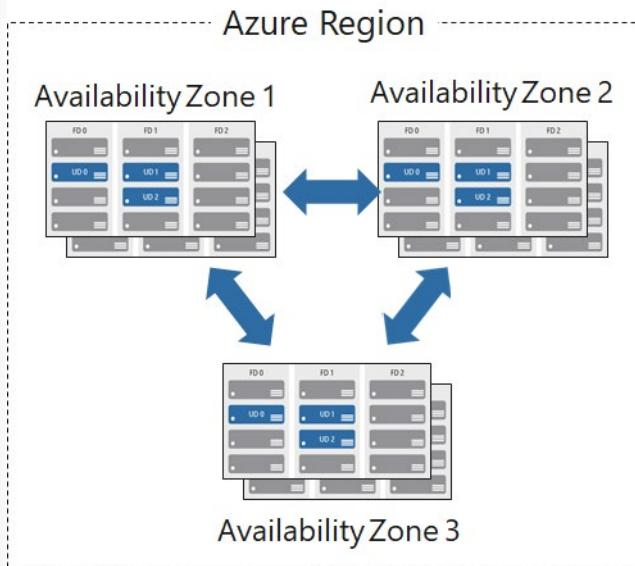
## Fault domains

A **fault domain (FD)** is a group of nodes that represent a physical unit of failure. A fault domain defines a group of virtual machines that share a common set of hardware, switches, that share a single point of failure. For example, a server rack serviced by a set of power or networking switches. VMs in an availability set are placed in at least two fault domains. Two fault domains mitigate against hardware failures, network outages, power interruptions, or software updates. Think of a fault domain as nodes belonging to the same physical rack.

**Note:** Placing your virtual machines into an availability set does not protect your application from operating system or application-specific failures. For that, you need to review other disaster recovery and backup techniques.

## Review Availability Zones

Availability Zones is a high-availability offering that protects your applications and data from datacenter failures.



## Considerations

- Availability Zones are unique physical locations within an Azure region.
- Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.
- To ensure resiliency, there's a minimum of three separate zones in all enabled regions.
- The physical separation of Availability Zones within a region protects applications and data from datacenter failures.
- Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure.

- With Availability Zones, Azure offers industry best 99.99% VM uptime SLA.

## Implementation

An Availability Zone in an Azure region is a combination of a fault domain and an update domain. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that VMs in different zones are not updated at the same time. Build high-availability into your application architecture by colocating your compute, storage, networking, and data resources within a zone and replicating in other zones.

Azure services that support Availability Zones fall into two categories:

- Zonal services.** Pin the resource to a specific zone (for example, virtual machines, managed disks, Standard IP addresses), or
- Zone-redundant services.** Platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

**Note:** To achieve comprehensive business continuity on Azure, build your application architecture using the combination of Availability Zones with Azure region pairs.

## Compare Vertical and Horizontal Scaling

Generally, there are two types of scaling: vertical scaling and horizontal scaling.

### Vertical scaling



Vertical scaling, also known as scale up and scale down, means increasing or decreasing virtual machine sizes in response to a workload. Vertical scaling makes the virtual machines more (scale up) or less (scale down) powerful. Vertical scaling can be useful when:

- A service built on virtual machines is under-utilized (for example at weekends). Reducing the virtual machine size can reduce monthly costs.
- Increasing virtual machine size to cope with larger demand without creating additional virtual machines.

## Horizontal scaling



Horizontal scaling, also referred to as scale out and scale in, where the number of VMs is altered depending on the workload. In this case, there is an increase (scale out) or decrease (scale in) in the number of virtual machine instances.

## Considerations

- Vertical scaling generally has more limitations. Vertical scaling dependent on the availability of larger hardware, which quickly hits an upper limit and can vary by region. Vertical scaling also usually requires a virtual machine to stop and restart.
- Horizontal scaling is more flexible in a cloud situation as it allows you to run potentially thousands of virtual machines to handle load.
- Reprovisioning means removing an existing virtual machine and replacing it with a new one. Do you need to retain your data?

## Implement Scale Sets

Virtual machine scale sets are an Azure Compute resource you can use to deploy and manage a set of **identical** VMs. With all VMs configured the same, virtual machine scale sets are designed to support true autoscale. No pre-provisioning of VMs is required. It is easier to build large-scale services targeting big compute, big data, and containerized workloads. As demand goes up more virtual machine instances can be added. As demand goes down virtual machines instances can be removed. The process can be manual or automated or a combination of both.

## Scale Set benefits

- All VM instances are created from the same base OS image and configuration. This approach lets you easily manage hundreds of VMs without additional configuration tasks or network management.
- Scale sets support the use of the Azure load balancer for basic layer-4 traffic distribution, and Azure Application Gateway for more advanced layer-7 traffic distribution and SSL termination.
- Scale sets are used to run multiple instances of your application. If one of these VM instances has a problem, customers continue to access your application through one of the other VM instances with minimal interruption.
- Customer demand for your application may change throughout the day or week. To match customer demand, scale sets can automatically increase the number of VM instances as application demand increases, then reduce the number of VM instances as demand decreases. This is known as autoscale.
- Scale sets support up to 1,000 VM instances. If you create and upload your own custom VM images, the limit is 600 VM instances.

## Create Scale Sets

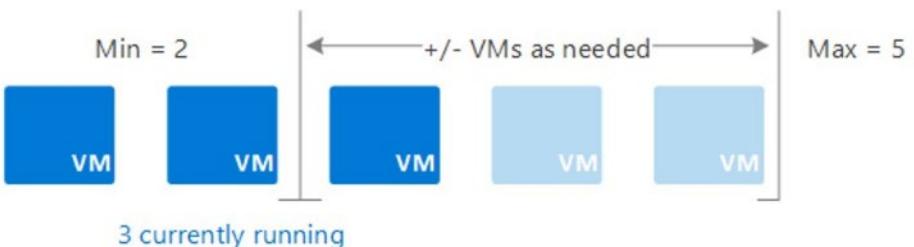
The screenshot shows the 'Create Scale Set' configuration page in the Azure portal. Key settings include:

- Initial instance count:** 2
- Size:** Standard D2s v3 (2 vcpus, 8 GiB memory (\$85.41/month))
- Azure Spot instance:** No (radio button selected)
- Use managed disks:** Yes (radio button selected)
- Allocation policy:**
  - Enable scaling beyond 100 instances: No (radio button selected)
  - Spreading algorithm: Max spreading (radio button selected)

- **Initial instance count.** Number of virtual machines in the scale set (0 to 1000).
- **Instance size.** The size of each virtual machine in the scale set.
- **Azure spot instance.** Low-priority VMs are allocated from Microsoft Azure's excess compute capacity. Spot instances enable several types of workloads to run at a reduced cost.
- **Use managed disks.** Managed disks hide the underlying storage accounts and instead shows the abstraction of a disk. Unmanaged disks expose the underlying storage accounts and VHD blobs.
- **Enable scaling beyond 100 instances.** If No, the scale set will be limited to one placement group with a max capacity of 100. If Yes, the scale set can span multiple placement groups. This allows for capacity to be up to 1,000 but changes the availability characteristics of the scale set.
- **Spreading algorithm.** We recommend deploying with max spreading for most workloads. This approach provides the best spreading.

## Implement Autoscale

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This means you can dynamically scale to meet changing demand.



## Autoscale benefits

- **Automatically adjust capacity.** Let's you create rules that define the acceptable performance for a positive customer experience. When those defined thresholds are met, autoscale rules act to adjust the capacity of your scale set.

- **Scale out.** If your application demand increases, the load on the VM instances in your scale set increases. If this increased load is consistent, rather than just a brief demand, you can configure autoscale rules to increase the number of VM instances in the scale set.
- **Scale in.** On an evening or weekend, your application demand may decrease. If this decreased load is consistent over a period of time, you can configure autoscale rules to decrease the number of VM instances in the scale set. This scale-in action reduces the cost to run your scale set as you only run the number of instances required to meet the current demand.
- **Schedule events.** Schedule events to automatically increase or decrease the capacity of your scale set at fixed times.
- **Less overhead.** Reduces the management overhead to monitor and optimize the performance of your application.

**Note:** Autoscale minimizes the number of unnecessary VM instances that run your application when demand is low, while customers continue to receive an acceptable level of performance as demand grows and additional VM instances are automatically added.

## Configure Autoscale

When you create a scale set you can enable Autoscale. You should also define a minimum, maximum, and default number of VM instances. When your autoscale rules are applied, these instance limits make sure that you do not scale out beyond the maximum number of instances or scale in beyond the minimum of instances.

The screenshot shows the 'Autoscale' configuration page in the Azure portal. It includes sections for 'Instance', 'Scaling', 'Scale out', and 'Scale in'. Key configuration parameters shown include:

- Instance:** Initial instance count: 2
- Scaling:** Scaling policy: Custom (selected)
- Scale out:** CPU threshold (%): 75, Duration in minutes: 10, Number of VMs to increase by: 1
- Scale in:** CPU threshold (%): 25, Number of VMs to decrease by: 1

- **Minimum number of VMs.** The minimum value for autoscale on this scale set.
- **Maximum number of VMs.** The maximum value for autoscale on this scale set.
- **Scale out CPU threshold.** The CPU usage percentage threshold for triggering the scale out autoscale rule.

- **Number of VMs to increase by.** The number of virtual machines to add to the scale set when the scale out autoscale rule is triggered.
- **Scale in CPU threshold.** The CPU usage percentage threshold for triggering the scale in autoscale rule.
- **Number of VMs to decrease by.** The number of virtual machines to remove to the scale set when the scale in autoscale rule is triggered.

## Demonstration - Virtual Machine Scaling

In this demonstration, we will explore virtual machine scaling options.

**Note:** This demonstration requires a virtual machine scale set. If you need help with this, review **Quick-start: Create a virtual machine scale set in the Azure portal**<sup>12</sup>.

**Note:** This demonstration is based on **Exercise - Configure a virtual machine scale set**<sup>13</sup>.

### Create a scale out rule

1. Access the Azure Portal select the virtual machine scale set you want to explore.
2. Under **Settings** select **Scaling**.
3. On the **Configuration** tab, review the purpose of scaling.
4. Review how **Manual scale** is used and discuss how to change the **Instance count**.
5. Select **Custom autoscale**.
  - Discuss how the default scale condition is executed when none of the other scale condition(s) match.
  - In the **Default** scale rule, discuss the difference between **Scale based on a metric** and **Scale to a specific instance count**.
6. Ensure that the **Scale mode** is set to **Scale based on a metric**. Then select **+ Add a rule**.
7. Create a rule with a Criteria and Action. The Criteria is when the CPU Percentage is over 75% for 10 minutes. The Action is to increase the instance count by 1.
  - Metric name: **Percentage CPU**
  - Operator: **Greater than**
  - Threshold: **75**
  - Duration: **10**
  - Operation: **Increase count by**
  - Instance count: **1**
8. After your rule is added, discuss how additional rules (like a scale in rule) could be used to optimize the deployment.

### Create a scale in rule

1. Ensure that the **Scale mode** is set to **Scale based on a metric**. Then select **+ Add a rule**.

<sup>12</sup> <https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/quick-create-portal>

<sup>13</sup> <https://docs.microsoft.com/en-us/learn/modules/build-app-with-scale-sets/5-exercise-configure-virtual-machine-scale-set>

2. Create a rule with a Criteria and Action. The Criteria is when the CPU Percentage is less than 50% for 10 minutes. The Action is to decrease the instance count by 1.
  - Metric name: **Percentage CPU**
  - Operator: **Less than**
  - Threshold: **50**
  - Duration: **10**
  - Operation: **Decrease count by**
  - Instance count: **1**
3. Your default scale condition now contains two scale rules. One rule scales the number of instances out. Another rule scales the number of instances back in.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Another IT administrator creates an Azure virtual machine scale set with 5 VMs. Later, you notice that the VMs are all running at max capacity with the CPU being fully consumed. However, additional VMs are not deploying in the scale set. You need to ensure that additional VMs are deployed when the CPU is 75% consumed. What should you do? Select one.*

- Enable the autoscale option.
- Increase the instance count.
- Add the scale set automation script to the library.

### Multiple choice

*You're part of the DevOps team for a large food delivery company. Friday night is typically your busiest time. Conversely, 7 AM on Wednesday is generally your quietest time. What should you implement? Select one.*

- autoscale
- metric-based rules
- schedule-based rules

## Multiple choice

Your company is preparing to deploy an application to Azure. The app is a self-contained unit that runs independently on several servers. The company is moving the app to the cloud to provide better performance. The team requests if the CPU across the servers goes above 85%, a new VM should be deployed. If the CPU across the servers drops below 15%, an Azure VM running the app should be decommissioned to reduce costs. You need to deploy a solution to meet the requirements while minimizing the administrative overhead to implement and manage the solution. What should you do? Select one.

- Deploy the app in a virtual machine scale set.
- Deploy the app in a virtual machine availability set.
- Deploy the app by using a resource manager template.

## Multiple choice

Your company is deploying a critical business application to Azure. The uptime of the application is of utmost importance. The application has two web servers, two application servers, and two database servers. Each VM in a tier must run on different hardware and uptime must be maximized. What should you do? Select one.

- Deploy 1 VM from each tier into one availability set and the remaining VMs into a separate availability set.
- Deploy the VMs from each tier into a dedicated availability set for the tier.
- Deploy the application and database VMs in one availability set and the web VMs into a separate availability set.

## Summary and Resources

### Summary

Azure provides several high availability options for virtual machines. These options include availability sets, availability zones, and virtual machine scale sets.

You should now be able to:

- Implement availability sets and availability zones.
- Implement update and fault domains.
- Implement virtual machine scale sets.
- Autoscale virtual machines.

### Learn more

You can learn more by reviewing the following.

- **Availability options for Azure Virtual Machines<sup>14</sup>**
- **Learn - Build a scalable application with virtual machine scale sets<sup>15</sup>**

<sup>14</sup> <https://docs.microsoft.com/azure/virtual-machines/availability>

<sup>15</sup> <https://docs.microsoft.com/learn/modules/build-app-with-scale-sets/>

- **Learn - Implement scale and high availability with Windows Server VM<sup>16</sup>**

---

<sup>16</sup> <https://docs.microsoft.com/learn/modules/implement-high-availability-of-windows-server-vms/>

# Configure Virtual Machine Extensions

## Introduction

### Scenario

Your company has created numerous scripts and processes to ensure virtual machines are updated. These scripts also run various configuration tasks.

You need to automate the process. Virtual machine extensions will allow you to avoid configuration drift.

### Skills measured

Automating virtual machine deployments is part of **Exam AZ-104: Microsoft Azure Administrator<sup>17</sup>**.

Deploy and manage Azure compute resources (20–25%)

Automate deployment of virtual machines (VMs) by using Azure Resource Manager templates

- Deploy virtual machine extensions.

### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for virtual machine extensions.
- Identify features and usage cases for custom script extensions.
- Identify features and usage cases for desired state configuration.

### Prerequisites

None.

## Implement Virtual Machine Extensions

Creating and maintaining virtual machines can be a lot of work, and much of it is repetitive, requiring the same steps each time. Fortunately, there are several ways to automate the tasks of creating, maintaining, and removing virtual machines. One way is to use a virtual machine **extension**.

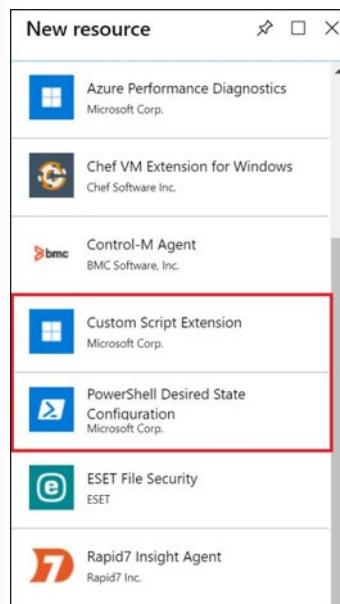
Azure virtual machine extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs. For example, if a virtual machine requires software installation, anti-virus protection, or a configuration script inside, a VM extension can be used. Extensions are all about managing your virtual machines.

Azure VM extensions can be:

- Managed with Azure CLI, PowerShell, Azure Resource Manager templates, and the Azure portal.
- Bundled with a new VM deployment or run against any existing system. For example, they can be part of a larger deployment, configuring applications on VM provision, or run against any supported extension operated systems post deployment.

<sup>17</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

There are different extensions for Windows and Linux machines and a large choice of first and third-party extensions.



## Implement Custom Script Extensions

Custom Script Extension(CSE) can be used to automatically launch and execute virtual machine customization tasks post configuration. Your script extension may perform simple tasks such as stopping the virtual machine or installing a software component. However, the script could be more complex and perform a series of tasks.

You can install the CSE from the Azure portal by accessing the virtual machines **Extensions** blade. Once the CSE resource is created, you will provide a PowerShell script file. Your script file will include the PowerShell commands you want to execute on the virtual machine. Optionally, you can pass in arguments, such as param1, param2. After the file is uploaded, it executes immediately. Scripts can be downloaded from Azure storage or GitHub, or provided to the Azure portal at extension run time.



You could also use the PowerShell **Set-AzVmCustomScriptExtension** command. This command requires the URI for the script in the blob container.

```
Set-AzVmCustomScriptExtension -FileUri https://scriptstore.blob.core.windows.net/scripts/Install_IIS.ps1 -Run "PowerShell.exe" -VmName vmName -ResourceGroupName resourceGroup -Location "location"
```

## Considerations

- **Timeout.** Custom Script extensions have 90 minutes to run. If your deployment exceeds this time, it is marked as a timeout. Keep this in mind when designing your script. Your virtual machine must be running to perform the tasks.
- **Dependencies.** If your extension requires networking or storage access, make sure that content is available.
- **Failure events.** Be sure to account for any errors that might occur when running your script. For example, running out of disk space, or security and access restrictions. What will the script do if there is an error?
- **Sensitive data.** Your extension may need sensitive information such as credentials, storage account names, and storage account access keys. How will you protect/encrypt this information?

**Note:** Can you think of any custom script extensions that you might want to create?

## Implement Desired State Configuration

Desired State Configuration (DSC) is a management platform in Windows PowerShell. DSC enables deploying and managing configuration data for software services and managing the environment in which these services run. DSC provides a set of Windows PowerShell language extensions, Windows PowerShell cmdlets, and resources that you can use to declaratively specify how you want your software environment to be configured. DSC also provides a means to maintain and manage existing configurations.

DSC centers around creating *configurations*. A configuration is an easy-to-read script that describes an environment made up of computers (nodes) with specific characteristics. These characteristics can be as simple as ensuring a specific Windows feature is enabled or as complex as deploying SharePoint. Use DSC when the CSE will not work for your application.

In this example, we are installing IIS on the localhost. The configuration is saved as a PS1 file.

```
configuration IISInstall
{
 Node "localhost"
 {
 WindowsFeature IIS
 {
 Ensure = "Present"
 Name = "Web-Server"
 } } }
```

The DSC script consists of a Configuration block, Node block, and one or more resource blocks.

- The **Configuration** block. This is the outermost script block. You define it by using the **Configuration** keyword and providing a name. In the example, the name of the configuration is *IISInstall*.
- One or more **Node** blocks. Node blocks define the computers or VMs that you are configuring. In the example, there is one Node block that targets a computer named "localhost".
- One or more resource blocks. Resource blocks configure the resource properties. In the example, there is one resource block that uses **WindowsFeature**. WindowsFeature indicates the name (Web-Server) of the role or feature that you want to ensure is added or removed. Ensure indicates if the role or feature is added. Your choices are Present and Absent.

**Note:** The Windows PowerShell DSC comes with a set of built-in configuration resources. For example, File Resource, Log Resource, and User Resource.

## Demonstration - Custom Script Extensions

In this demonstration, we will explore Custom Script Extensions.

**Note:** This scenario requires a Windows virtual machine in the running state.

### Verify the Web Server feature is available

1. Connect (RDP) to your Windows virtual machine and open a PowerShell prompt.
2. Run this command and verify the Web Server feature status is **Available** but not Installed.

```
Get-WindowsFeature -name Web-Server
```

### Create a PowerShell script file to install the Web Server

1. Create a file **Install\_IIS.ps1** on your local machine.
2. Edit the file and add this command:

```
Install-WindowsFeature -Name Web-Server
```

### Configure an Extension in the Portal to run the script

1. In the Azure Portal, access your virtual machine, and select **Extensions**.
2. Click **+ Add**. Take a minute to review the many different extensions that are available.
3. Locate the **Custom Script Extension** resource, select, and click **Create**.
4. Browse to your PowerShell script and upload the file. There will be a notification that the file was uploaded.
5. Click **OK**.
6. Select your **CustomScriptExtension**.
7. Click **View detailed status** and verify provisioning succeeded.

### Verify the Web Server was installed

1. Return to your virtual machine RDP session.
2. Verify the Web Server role was installed. This may take a couple of minutes.

```
Get-WindowsFeature -name Web-Server
```

**Note:** You could also use the PowerShell **Set-AzVmCustomScriptExtension** command to deploy the extension. You would need to upload the script to blob container and use the URI. We will do this in the next demonstration.

## Knowledge check

Choose the best response for each question.

## Multiple choice

*What is Azure Automation State Configuration?*

- A declarative management platform to configure, deploy, and control systems.
- A service used to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations, import DSC resources, and assign configurations to target nodes.
- A service that manages the state configuration on each destination, or node.

## Multiple choice

*A PowerShell DSC script \_\_\_\_\_.*

- contains the steps required to configure a virtual machine to get it into a specified state.
- can only be run in push mode.
- describes the desired state.

## Multiple choice

*Why should you use pull mode instead of push mode for DSC?*

- Pull mode is best for complex environments that need redundancy and scale.
- Pull mode is easy to set up and doesn't need its own dedicated infrastructure.
- Pull mode uses the local configuration manager (LCM) to make sure that the state on each node matches the state specified by the configuration.

# Summary and Resources

## Summary

Azure virtual machine (VM) extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs. For example, if a virtual machine requires software installation, anti-virus protection, or to run a script inside of it, a VM extension can be used.

You should now be able to:

- Identify features and usage cases for virtual machine extensions.
- Identify features and usage cases for custom script extensions.
- Identify features and usage cases for desired state configuration.

## Learn more

You can learn more by reviewing the following.

- **Virtual machine extensions and features for Windows<sup>18</sup>**
- **Virtual machine extensions and features for Linux<sup>19</sup>.**

<sup>18</sup> <https://docs.microsoft.com/azure/virtual-machines/extensions/features-windows?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json>

<sup>19</sup> <https://docs.microsoft.com/azure/virtual-machines/extensions/features-linux>

- **Learn - Automate the configuration of Windows Server IaaS Virtual Machines<sup>20</sup>**
- **Learn - Protect your virtual machine settings with Azure Automation State Configuration<sup>21</sup>**

---

<sup>20</sup> <https://docs.microsoft.com/learn/modules/automate-configuration-of-windows-server-iaas-virtual-machines/>

<sup>21</sup> <https://docs.microsoft.com/learn/modules/protect-vm-settings-with-dsc/>

# Module 08 Lab

## Lab 08 - Manage Virtual Machines

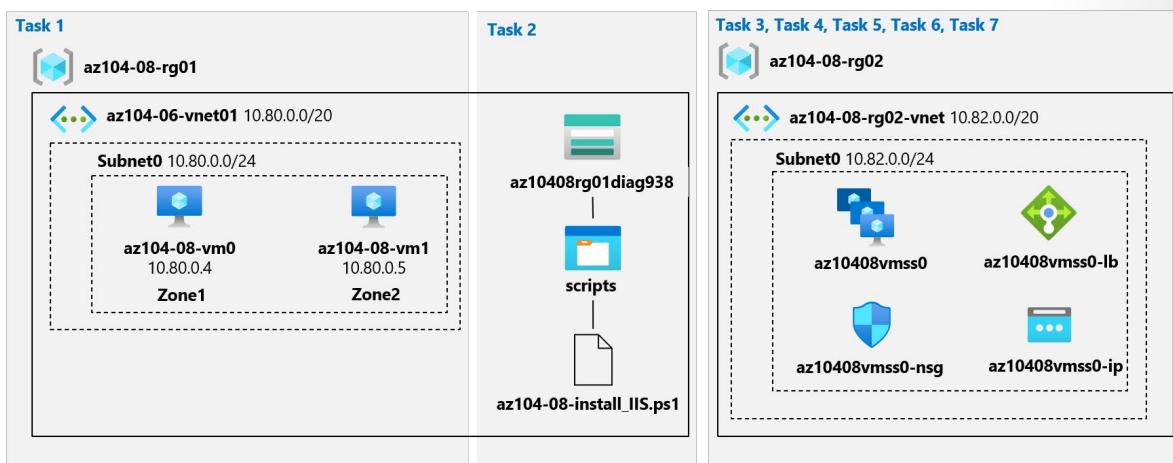
### Lab scenario

You were tasked with identifying different options for deploying and configuring Azure virtual machines. First, you need to determine different compute and storage resiliency and scalability options you can implement when using Azure virtual machines. Next, you need to investigate compute and storage resiliency and scalability options that are available when using Azure virtual machine scale sets. You also want to explore the ability to automatically configure virtual machines and virtual machine scale sets by using the Azure Virtual Machine Custom Script extension.

### Objectives

In this lab, you will:

- Task 1: Deploy zone-resilient Azure virtual machines by using the Azure portal and an Azure Resource Manager template.
- Task 2: Configure Azure virtual machines by using virtual machine extensions.
- Task 3: Scale compute and storage for Azure virtual machines.
- Task 4: Register the Microsoft.Insights and Microsoft.AlertsManagement resource providers
- Task 5: Deploy zone-resilient Azure virtual machine scale sets by using the Azure portal
- Task 6: Configure Azure virtual machine scale sets by using virtual machine extensions
- Task 7: Scale compute and storage for Azure virtual machine scale sets (optional)



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Answers

## Multiple choice

You are planning to deploy several Linux VMs in Azure. The security team issues a policy that Linux VMs must use an authentication system other than passwords. You need to deploy an authentication method for the Linux VMs to meet the requirement. Which authentication method should you use? Select one.

- SSH key pair
- Access keys
- Shared access signature

### Explanation

Azure supports two authentication methods for Linux VMs - passwords and SSH (via an SSH key pair). Access keys and shared access signatures are access methods for Azure storage, not for Azure VMs. In this scenario, you need to use an SSH key pair to meet the requirement.

## Multiple choice

Your organization has a security policy that prohibits exposing SSH ports to the outside world. You need to connect to an Azure Linux virtual machine to install software. What should you do? Select one.

- Configure the Bastion service
- Configure a Guest configuration on the virtual machine
- Create a custom script extension

### Explanation

Configure the Bastion service. The Azure Bastion service is a new fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP and SSH connectivity to your virtual machines directly in the Azure portal over SSL. When you connect via Azure Bastion, your virtual machines do not need a public IP address. Bastion provides secure RDP and SSH connectivity to all VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP and SSH ports to the outside world while still providing secure access using RDP and SSH. With Azure Bastion, you connect to the virtual machine directly from the Azure portal. You don't need an additional client, agent, or piece of software.

## Multiple choice

What is the effect of the default network security settings for a new virtual machine?

- Neither outbound nor inbound requests are allowed.
- Outbound request is allowed. Inbound traffic is only allowed from within the virtual network.
- There are no restrictions: all outbound and inbound requests are allowed.

### Explanation

Outbound request is allowed. Inbound traffic is only allowed from within the virtual network. Outbound requests are considered low risk, so they are allowed by default. Inbound traffic from within the virtual network is allowed. By placing a VM in a virtual network, the VM owner is implicitly opting-in to communication among the resources in the virtual network.

**Multiple choice**

You have several Linux virtual machines hosted in Azure. You will administer these VMs remotely over SSH from three dedicated machines in your corporate headquarters. Which of the following authentication methods would typically be considered best-practice for this situation?

- Username and password
- Private key
- Private key with passphrase

*Explanation*

*Private key with passphrase. Private key access with a passphrase is the most secure option. Even if an attacker acquires your private key, they will be unable to use it without the passphrase.*

**Multiple choice**

You want to run a network appliance on a virtual machine. Which workload option should you choose?

- Compute optimized
- Memory optimized
- Storage optimized

*Explanation*

*Compute optimized. Compute optimized virtual machines are designed to have a high CPU-to-memory ratio. Suitable for medium traffic web servers, network appliances, batch processes, and application servers.*

**Multiple choice**

Another IT administrator creates an Azure virtual machine scale set with 5 VMs. Later, you notice that the VMs are all running at max capacity with the CPU being fully consumed. However, additional VMs are not deploying in the scale set. You need to ensure that additional VMs are deployed when the CPU is 75% consumed. What should you do? Select one.

- Enable the autoscale option.
- Increase the instance count.
- Add the scale set automation script to the library.

*Explanation*

*When you have a scale set, you can enable automatic scaling with the autoscale option. When you enable the option, you define the parameters for when to scale. To meet the requirements of this scenario, you need to enable the autoscale option so that additional VMs are created when the CPU is 75% consumed. Note that the automation script is used to automate the deployment of scale sets and not related to automating the building of additional VMs in the scale set.*

**Multiple choice**

You're part of the DevOps team for a large food delivery company. Friday night is typically your busiest time. Conversely, 7 AM on Wednesday is generally your quietest time. What should you implement? Select one.

- autoscale
- metric-based rules
- schedule-based rules

*Explanation*

*Schedule-based rules. You can proactively schedule the scale set to deploy one or N number of additional instances to accommodate a spike in traffic and then scale back down when the spike ends.*

**Multiple choice**

Your company is preparing to deploy an application to Azure. The app is a self-contained unit that runs independently on several servers. The company is moving the app to the cloud to provide better performance. The team requests if the CPU across the servers goes above 85%, a new VM should be deployed. If the CPU across the servers drops below 15%, an Azure VM running the app should be decommissioned to reduce costs. You need to deploy a solution to meet the requirements while minimizing the administrative overhead to implement and manage the solution. What should you do? Select one.

- Deploy the app in a virtual machine scale set.
- Deploy the app in a virtual machine availability set.
- Deploy the app by using a resource manager template.

*Explanation*

*In this scenario, you should use a scale set for the VMs. Scale sets can scale up or down, based on defined criteria (such as the existing set of VMs using a large percentage of the available CPU). This meets the scenario's requirements.*

**Multiple choice**

Your company is deploying a critical business application to Azure. The uptime of the application is of utmost importance. The application has two web servers, two application servers, and two database servers. Each VM in a tier must run on different hardware and uptime must be maximized. What should you do? Select one.

- Deploy 1 VM from each tier into one availability set and the remaining VMs into a separate availability set.
- Deploy the VMs from each tier into a dedicated availability set for the tier.
- Deploy the application and database VMs in one availability set and the web VMs into a separate availability set.

*Explanation*

*An availability set should hold VMs in the same tier because that ensures that the VMs are not dependent on the same physical hardware. If you deploy VMs in a single tier across multiple availability sets, then you have a chance of a tier becoming unavailable due to a hardware issue. In this scenario, each tier should have a dedicated availability set (Web availability set, app availability set, database availability set).*

**Multiple choice**

What is Azure Automation State Configuration?

- A declarative management platform to configure, deploy, and control systems.
- A service used to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations, import DSC resources, and assign configurations to target nodes.
- A service that manages the state configuration on each destination, or node.

*Explanation*

*A service used to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations, import DSC resources, and assign configurations to target nodes.*

**Multiple choice**

A PowerShell DSC script \_\_\_\_\_.

- contains the steps required to configure a virtual machine to get it into a specified state.
- can only be run in push mode.
- describes the desired state.

*Explanation*

*Describes the desired state. A PowerShell DSC script is declarative. It describes the desired state but doesn't include the steps necessary to achieve that state.*

**Multiple choice**

Why should you use pull mode instead of push mode for DSC?

- Pull mode is best for complex environments that need redundancy and scale.
- Pull mode is easy to set up and doesn't need its own dedicated infrastructure.
- Pull mode uses the local configuration manager (LCM) to make sure that the state on each node matches the state specified by the configuration.

*Explanation*

*Pull mode is best for complex environments that need redundancy and scale. Each node automatically polls the pull server at regular intervals to get the latest configuration details. In push mode, an administrator manually sends the configurations toward the nodes.*



# Module 9 Administer PaaS Compute Options

## Configure Azure App Service Plans

### Introduction

#### Scenario

It's important to be able to scale a web app for these reasons:

- It enables the app to remain responsive during periods of high demand.
- It helps to save you money by reducing the resources required when demand drops.

Imagine that you work for a large chain of hotels. You have a website that customers can visit to make bookings and to view the details of bookings that they've previously made. At certain times of the year, the volume of traffic grows because customers are browsing hotels for summer vacations. At other times, traffic declines. These patterns are predictable.

You meet these goals providing scale up and down, and scale in and out. Your scaling choices depend on the App Service plan.

#### Skills measured

App Service plans and scaling are part of **Exam AZ-104: Microsoft Azure Administrator<sup>1</sup>**.

Deploy and manage Azure compute resources (20–25%)

Create and configure Azure App Service

- Create an App Service plan.
- Configure scaling settings in an App Service plan.

<sup>1</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

## Learning objectives

In this module, you will learn how to:

- Identify features and usage cases of the Azure App Service.
- Select an appropriate Azure App Service plan pricing tier.
- Scale the App Service Plan.
- Scale out the App Service Plan.

## Prerequisites

None.

# Implement Azure App Service Plans

In App Service, an app runs in an App Service plan. An App Service plan defines a set of compute resources for a web app to run. These compute resources are analogous to the server farm in conventional web hosting. One or more apps can be configured to run on the same computing resources (or in the same App Service plan).

When you create an App Service plan in a certain region (for example, West Europe), a set of compute resources is created for that plan in that region. Whatever apps you put into this App Service plan run on these compute resources as defined by your App Service plan. Each App Service plan defines:

- **Region** (West US, East US, etc.)
- **Number of VM instances**
- **Size of VM instances** (Small, Medium, Large)

## How the app runs and scales

In the Free and Shared tiers, an app receives CPU minutes on a shared VM instance and cannot scale out. In other tiers, an app runs and scales as follows.

When you create an app in App Service, it is put into an App Service plan. When the app runs, it runs on all the VM instances configured in the App Service plan. If multiple apps are in the same App Service plan, they all share the same VM instances. If you have multiple deployment slots for an app, all deployment slots also run on the same VM instances. If you enable diagnostic logs, perform backups, or run WebJobs, they also use CPU cycles and memory on these VM instances.

In this way, the App Service plan is the scale unit of the App Service apps. If the plan is configured to run five VM instances, then all apps in the plan run on all five instances. If the plan is configured for autoscaling, then all apps in the plan are scaled out together based on the autoscale settings.

## Considerations

Since you pay for the computing resources your App Service plan allocates, you can potentially save money by putting multiple apps into one App Service plan. You can continue to add apps to an existing plan as long as the plan has enough resources to handle the load. However, keep in mind that apps in the same App Service plan all share the same compute resources. To determine whether the new app has the necessary resources, you need to understand the capacity of the existing App Service plan, and the

expected load for the new app. Overloading an App Service plan can potentially cause downtime for your new and existing apps. Isolate your app into a new App Service plan when:

- The app is resource-intensive.
- You want to scale the app independently from the other apps in the existing plan.
- The app needs resources in a different geographical region.

## Determine App Service Plan Pricing

The pricing tier of an App Service plan determines what App Service features you get and how much you pay for the plan. There are a few categories of pricing tiers.

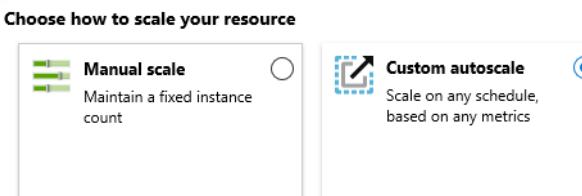
| Selected Feature         | Free     | Shared   | Basic              | Standard             | Premium                        | Isolated                                  |
|--------------------------|----------|----------|--------------------|----------------------|--------------------------------|-------------------------------------------|
| Usage                    | dev/test | dev/test | dedicated dev/test | production workloads | enhanced scale and performance | high performance, security, and isolation |
| Web, mobile, or API apps | 10       | 100      | Unlimited          | Unlimited            | Unlimited                      | Unlimited                                 |
| Disk space               | 1 GB     | 1 GB     | 10 GB              | 50 GB                | 250 GB                         | 1 TB                                      |
| Auto scale               | -        | -        | -                  | Supported            | Supported                      | Supported                                 |
| Deployment slots         | -        | -        | -                  | 5                    | 20                             | 20                                        |
| Max instances            | -        | -        | Up to 3            | Up to 10             | Up to 30                       | Up to 100                                 |

- **Free and Shared.** The Free and Shared service plans are base tiers that run on the same Azure VMs as other apps. Some apps may belong to other customers. These tiers are intended to be used only for development and testing purposes. There is no SLA provided for Free and Shared service plans. Free and Shared plans are metered on a per App basis.
- **Basic.** The Basic service plan is designed for apps that have lower traffic requirements, and don't need advanced auto scale and traffic management features. Pricing is based on the size and number of instances you run. Built-in network load-balancing support automatically distributes traffic across instances. The Basic service plan with Linux runtime environments supports Web App for Containers.
- **Standard.** The Standard service plan is designed for running production workloads. Pricing is based on the size and number of instances you run. Built-in network load-balancing support automatically distributes traffic across instances. The Standard plan includes auto scale that can automatically adjust the number of virtual machine instances running to match your traffic needs. The Standard service plan with Linux runtime environments supports Web App for Containers.
- **Premium.** The Premium service plan is designed to provide enhanced performance for production apps. The upgraded Premium plan, Premium v2, features Dv2-series VMs with faster processors, SSD storage, and double memory-to-core ratio compared to Standard. The new Premium plan also supports higher scale via increased instance count while still providing all the advanced capabilities found in the Standard plan. The first generation of Premium plan is still available for existing customers' scaling needs.
- **Isolated.** The Isolated service plan is designed to run mission critical workloads, that are required to run in a virtual network. The Isolated plan allows customers to run their apps in a private, dedicated environment in an Azure datacenter using Dv2-series VMs with faster processors, SSD storage, and

double the memory-to-core ratio compared to Standard. The private environment used with an Isolated plan is called the App Service Environment. The plan can scale to 100 instances with more available upon request.

## Scale Up and Scale Out the App Service

There are two methods for Web App scaling, **scale up** and **scale out**. Apps can be scaled manually or automatically (autoscale).



**Scale up.** Get more CPU, memory, disk space, and extra features like dedicated virtual machines (VMs), custom domains and certificates, staging slots, autoscaling, and more. You scale up by changing the pricing tier of the App Service plan that your app belongs to.

**Scale out:** Increase the number of VM instances that run your app. You can scale out to as many as 30 instances, depending on your pricing tier. App Service Environments in Isolated tier further increases your scale-out count to 100 instances. The scale instance count can be configured manually or automatically (autoscale). Autoscale is based on predefined rules and schedules.

### Changing your App Service plan (scale up)

Your App Service plan can be scaled up and down at any time. It is as simple as changing the pricing tier of the plan. You can choose a lower pricing tier at first and scale up later when you need more App Service features.

For example, you can start testing your web app in a Free App Service plan and pay nothing. When you want to add your custom DNS name to the web app, just scale your plan up to the Shared tier. Later, when you want to create an SSL binding, scale your plan up to Basic tier. When you want to have staging environments, scale up to Standard tier. When you need more cores, memory, or storage, scale up to a bigger VM size in the same tier.

The same works in the reverse. When you feel you no longer need the capabilities or features of a higher tier, you can scale down to a lower tier, which saves you money.

### Other considerations

- The scale settings take only seconds to apply and affect all apps in your App Service plan. They don't require you to change your code or redeploy your application.
- If your app depends on other services, such as Azure SQL Database or Azure Storage, you can scale up these resources separately. These resources aren't managed by the App Service plan.

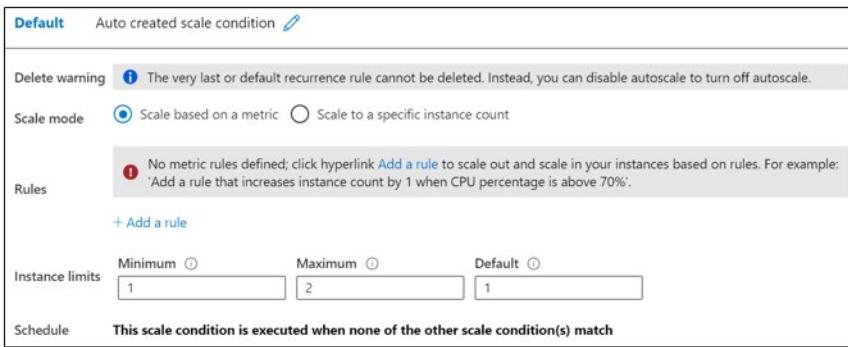
## Configure App Service Plan Scaling

Autoscale allows you to have the right amount of resources running to handle the load on your application. It allows you to add resources to handle increases in load and also save money by removing resources that are sitting idle. You specify a minimum and maximum number of instances to run and add or

remove VMs automatically based on a set of rules. When rule conditions are met, one or more autoscale actions are triggered.

## Autoscale settings

An autoscale setting is read by the autoscale engine to determine whether to scale up or down. Autoscale settings are grouped into profiles.



Rules include a trigger and a scale action (up or down). The trigger can be metric-based or time-based.

- **Metric-based.** Metric-based rules measure application load and add or remove VMs based on that load. For example, do this action when CPU usage is above 50%. Examples of metrics are CPU time, Average response time, and Requests.
- **Time-based.** Time-based (schedule-based) rules allow you to scale when you see time patterns in your load and want to scale before a possible load increase or decrease occurs. For example, trigger a webhook every 8am on Saturday in a given time zone.

## Considerations

- Having a minimum instance count makes sure your application is always running even under no load.
- Having a maximum instance count limits your total possible hourly cost.
- You can automatically scale between the minimum and maximum using rules you create.
- Ensure the maximum and minimum values are different and have an adequate margin between them.
- Always use a scale-out and scale-in rule combination that performs an increase and decrease.
- Choose the appropriate statistic for your diagnostics metric (Average, Minimum, Maximum and Total).
- Always select a safe default instance count. The default instance count is important because autoscale scales your service to that count when metrics are not available.
- Always configure autoscale notifications.

## Notification settings

A notification setting defines what notifications should occur when an autoscale event occurs based on satisfying the criteria of one of the autoscale setting's profiles. Autoscale can notify one or more email addresses or make calls to one or more webhooks.

# Demonstration - Create an App Service Plan

In this demonstration, we will create and work with Azure App Service plans.

## Create an App Service Plan

1. Sign-in to the [Azure portal](#)<sup>2</sup>.
2. Search for and select **App Service Plans**.
3. Click **+ Add** to create a new App Service plan.

| Setting          | Value                               |
|------------------|-------------------------------------|
| Subscription     | <b>Choose your subscription</b>     |
| Resource Group   | <b>myRGAppServices</b> (create new) |
| Name             | <b>AppServicePlan1</b>              |
| Operating System | <b>Windows</b>                      |
| Region           | <b>East US</b>                      |

4. Click **Review + Create** and then **Create**.
5. Wait for your new App Service plan to deploy.

## Review Pricing Tiers

1. Locate your new App Service plan.
2. Under **Settings**, click **Scale up (App Service Plan)**.
3. Notice there are three tiers: **Dev/Test**, **Production**, and **Isolated**.
4. Click each tier and review the included features and included hardware.
5. How do the tiers compare?

## Review autoscaling

1. Under **Settings** click **Scale out (App Service Plan)**.
2. Notice the default is **Manual scale**.
3. Notice you can specify an **instance count** depending on your App Service plan selection.
4. Click **Custom autoscale**.
5. Notice two scale modes: **Scale based on a metric** and **Scale to a specific instance count**.
6. Click **Add a rule** to automatically add an instance when the CPU percentages is greater than 80% for 10 minutes.

| Setting          | Value                    |
|------------------|--------------------------|
| Time aggregation | <b>Average</b>           |
| Metric name      | <b>CPU percentage</b>    |
| Operator         | <b>Greater than</b>      |
| Threshold        | <b>80</b>                |
| Duration         | <b>10 minutes</b>        |
| Operation        | <b>Increase count by</b> |
| Instance count   | <b>1</b>                 |

---

<sup>2</sup> <http://portal.azure.com/>

| Setting   | Value            |
|-----------|------------------|
| Cool down | <b>5 minutes</b> |

7. **Add** your rule changes.
8. Review the **Instance limits: Minimum, Maximum, and Default**.
9. Notice that you can add a **Schedule** and **Specify start/end dates** and **Repeat specific days**.
10. Do you see how you can create different App Service plans for your apps?

## Knowledge check

Choose the best response for each question.

### Multiple choice

*You are administering a production web app. The app requires scaling to five instances, 40GB of storage, and a custom domain name. Which App Service Plan should you select? Select one.*

- Basic
- Standard
- Premium

### Multiple choice

*Which of the following is not true of the App Service plan? Select one.*

- The App Service plan is a set of virtual server resources that run App Service apps.
- The App Service plan determines the performance characteristics of the virtual servers.
- The App Service plan hosts a single App Service web app.

### Multiple choice

*To get more CPU, memory, or disk space you should? Select one.*

- Scale up
- Scale out

### Multiple choice

*To configure an autoscale trigger based on average response time, you should select ... Select one.*

- Metric-based
- Time-based
- User-based

# Summary and Resources

## Summary

Your App Service plan can be scaled up and down at any time. Scaling lets you meet changing demands while effectively managing costs.

You should now be able to:

- Identify features and usage cases of the Azure App Service.
- Select an appropriate Azure App Service plan pricing tier.
- Scale the App Service Plan.
- Scale out the App Service Plan.

## Learn more

You can learn more by reviewing the following.

- **Azure App Service plan overview<sup>3</sup>**
- **Scale up an app in Azure App Service<sup>4</sup>**
- **Learn - Scale an App Service web app to efficiently meet demand with App Service scale up and scale out<sup>5</sup>**

---

<sup>3</sup> <https://docs.microsoft.com/azure/app-service/overview-hosting-plans>

<sup>4</sup> <https://docs.microsoft.com/azure/app-service/manage-scale-up>

<sup>5</sup> <https://docs.microsoft.com/learn/modules/app-service-scale-up-scale-out/>

# Configure Azure App Services

## Introduction

### Scenario

Imagine you're building a website for a new business, or you're running an existing web app on an aging on-premises server. Setting up a new server can be challenging. You need appropriate hardware, likely a server-level operating system, and a web hosting stack.

And once it's running, you need to maintain the server. And what happens if your website traffic increases? You may need to invest in additional hardware.

Hosting your web application using Azure App Service makes deploying and managing a web app much easier when compared to managing a physical server.

### Skills measured

Configuring the Azure App Service is part of **Exam AZ-104: Microsoft Azure Administrator<sup>6</sup>**.

Deploy and manage Azure compute resources (20–25%)

Create and configure Azure App Service

- Create an App Service.
- Secure an App Service.
- Configure custom domain names.
- Configure backup for an App Service.
- Configure networking settings.
- Configure deployment settings.

Monitor and back up Azure resources (10–15%)

Monitor resources by using Azure Monitor

- Configure Application Insights.

### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for the the Azure App Service.
- Create an App Service.
- Configure deployment settings, specifically deployment slots.
- Secure the App Service.
- Configure custom domain names
- Backup the App Service.
- Configure Application Insights.

<sup>6</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

## Prerequisites

None.

## Implement Azure App Services

Azure App Service brings together everything you need to create websites, mobile backends, and web APIs for any platform or device. Applications run and scale with ease on both Windows and Linux-based environments. There are many deployment choices.



## Reasons to use App Services

- **Multiple languages and frameworks.** App Service has first-class support for ASP.NET, Java, Ruby, Node.js, PHP, or Python. You can also run PowerShell and other scripts or executables as background services.
- **DevOps optimization.** Set up continuous integration and deployment with Azure DevOps, GitHub, BitBucket, Docker Hub, or Azure Container Registry. Promote updates through test and staging environments. Manage your apps in App Service by using Azure PowerShell or the cross-platform command-line interface (CLI).
- **Global scale with high availability.** Scale up or out manually or automatically. Host your apps anywhere in Microsoft's global datacenter infrastructure, and the App Service SLA promises high availability.
- **Connections to SaaS platforms and on-premises data.** Choose from more than 50 connectors for enterprise systems (such as SAP), SaaS services (such as Salesforce), and internet services (such as Facebook). Access on-premises data using Hybrid Connections and Azure Virtual Networks.
- **Security and compliance.** App Service is ISO, SOC, and PCI compliant. Authenticate users with Azure Active Directory or with social login (Google, Facebook, Twitter, and Microsoft). Create IP address restrictions and manage service identities.
- **Application templates.** Choose from an extensive list of application templates in the Azure Marketplace, such as WordPress, Joomla, and Drupal.
- **Visual Studio integration.** Dedicated tools in Visual Studio streamline the work of creating, deploying, and debugging.
- **API and mobile features.** App Service provides turn-key CORS support for RESTful API scenarios, and simplifies mobile app scenarios by enabling authentication, offline data sync, push notifications, and more.
- **Serverless code.** Run a code snippet or script on-demand without having to explicitly provision or manage infrastructure and pay only for the compute time your code actually uses.

## Create an App Service

When creating an App Service, you will need to specify a resource group and service plan. Then there are few other configuration choices. You may need to ask your developer for assistance in completing this information.

Instance Details

|                    |                                                                              |
|--------------------|------------------------------------------------------------------------------|
| Name *             | <input type="text" value="webappces1"/> .azurewebsites.net                   |
| Publish *          | <input checked="" type="radio"/> Code <input type="radio"/> Docker Container |
| Runtime stack *    | Select a runtime stack.                                                      |
| Operating System * | <input checked="" type="radio"/> Linux <input type="radio"/> Windows         |
| Region *           | Central US<br>Not finding your App Service Plan? Try a different region.     |

- **Name.** The name must be unique and will be used to locate your app. For example, webappces1.azurewebsites.net. You can map a custom domain name, if you prefer to use that instead.
- **Publish.** The App service can host either Code or a Docker Container.
- **Runtime stack.** The software stack to run the app, including the language and SDK versions. For Linux apps and custom container apps, you can also set an optional start-up command or file. Choices include: .NET Core, .NET Framework, Node.js, PHP, Python, and Ruby. Various versions of each are available.
- **Operating system.** Choices are Linux and Windows.
- **Region.** Your choice will affect app service plan availability.

## Application settings

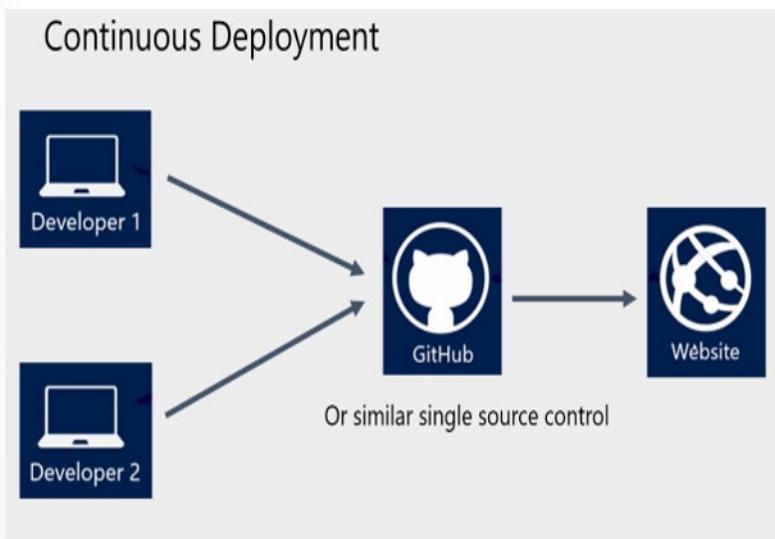
Once your app service is created, additional configuration information is available.

Certain configuration settings can be included in the developer's code or configurated in the app service. Here are a few interesting settings.

- **Always On.** Keep the app loaded even when there's no traffic. It's required for continuous WebJobs or for WebJobs that are triggered using a CRON expression.
- **ARR affinity.** In a multi-instance deployment, ensure that the client is routed to the same instance for the life of the session. You can set this option to Off for stateless application,
- **Connection strings.** Connection strings are encrypted at rest and transmitted over an encrypted channel.

## Explore Azure Container Instances Benefits

The Azure portal provides out-of-the-box continuous integration and deployment with Azure DevOps, GitHub, Bitbucket, FTP, or a local Git repository on your development machine. Connect your web app with any of the above sources and App Service will do the rest for you by auto-syncing code and any future changes on the code into the web app. Furthermore, with Azure DevOps, you can define your own build and release process that compiles your source code, runs the tests, builds a release, and finally deploys the release into your web app every time you commit the code. All that happens implicitly without any need to intervene.



## Automated deployment

Automated deployment, or continuous integration, is a process used to push out new features and bug fixes in a fast and repetitive pattern with minimal impact on end users. Azure supports automated deployment directly from several sources. The following options are available:

- **Azure DevOps:** You can push your code to Azure DevOps (previously known as Visual Studio Team Services), build your code in the cloud, run the tests, generate a release from the code, and finally, push your code to an Azure Web App.
- **GitHub:** Azure supports automated deployment directly from GitHub. When you connect your GitHub repository to Azure for automated deployment, any changes you push to your production branch on GitHub will be automatically deployed for you.
- **Bitbucket:** With its similarities to GitHub, you can configure an automated deployment with Bitbucket.

## Manual deployment

There are a few options that you can use to manually push your code to Azure:

- **Git:** App Service web apps feature a Git URL that you can add as a remote repository. Pushing to the remote repository will deploy your app.
- **CLI:** `webapp up` is a feature of the `az` command-line interface that packages your app and deploys it. Unlike other deployment methods, `az webapp up` can create a new App Service web app for you if you haven't already created one.

- **Zipdeploy:** Use curl or a similar HTTP utility to send a ZIP of your application files to App Service.
- **Visual Studio:** Visual Studio features an App Service deployment wizard that can walk you through the deployment process.
- **FTP/S:** FTP or FTPS is a traditional way of pushing your code to many hosting environments, including App Service.

## Create Deployment Slots

When you deploy your web app, web app on Linux, mobile back end, or API app to Azure App Service, you can use a separate deployment slot instead of the default production slot when you're running in the **Standard**, **Premium**, or **Isolated** App Service plan tier. Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot.

| NAME                                                                             | STATUS  | APP SERVICE PLAN  | TRAFFIC %                           |
|----------------------------------------------------------------------------------|---------|-------------------|-------------------------------------|
| webappces <span style="background-color: green; color: white;">PRODUCTION</span> | Running | ASP-webapprg-a247 | <div style="width: 100%;">100</div> |
| webappces-Staging                                                                | Running | ASP-webapprg-a247 | <div style="width: 0%;">0</div>     |

## Deployment slot advantages

Using separate staging and production slots has several advantages.

- You can validate app changes in a staging deployment slot before swapping it with the production slot.
- Deploying an app to a slot first and swapping it into production ensures that all instances of the slot are warmed up before being swapped into production. This eliminates downtime when you deploy your app. The traffic redirection is seamless, and no requests are dropped because of swap operations. This entire workflow can be automated by configuring Auto Swap when pre-swap validation is not needed.
- After a swap, the slot with previously staged app now has the previous production app. If the changes swapped into the production slot are not as you expected, you can perform the same swap immediately to get your “last known good site” back.

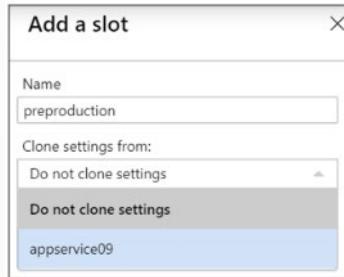
Auto swap streamlines Azure DevOps scenarios where you want to deploy your app continuously with zero cold starts and zero downtime for customers of the app. When auto swap is enabled from a slot into production, every time you push your code changes to that slot, App Service automatically swaps the app into production after it's warmed up in the source slot. Auto swap isn't currently supported in web apps on Linux.

**Note:** Each App Service plan mode supports a different number of deployment slots.

## Add Deployment Slots

New deployment slots can be empty or cloned. When you clone a configuration from another deployment slot, the cloned configuration is editable. Some configuration elements follow the content across a swap (not slot specific), whereas other configuration elements stay in the same slot after a swap (slot specific). Deployment slot settings fall into three categories.

- Slot-specific app settings and connection strings, if applicable.
- Continuous deployment settings, if enabled.
- App Service authentication settings, if enabled.



### **Settings that are swapped:**

- General settings, such as framework version, 32/64-bit, web sockets
- App settings (can be configured to stick to a slot)
- Connection strings (can be configured to stick to a slot)
- Handler mappings
- Public certificates
- WebJobs content
- Hybrid connections \*
- Service endpoints \*
- Azure Content Delivery Network \*

Features marked with an asterisk (\*) are planned to be unswapped.

### **Settings that aren't swapped:**

- Publishing endpoints
- Custom domain names
- Non-public certificates and TLS/SSL settings
- Scale settings
- WebJobs schedulers
- IP restrictions
- Always On
- Diagnostic settings
- Cross-origin resource sharing (CORS)
- Virtual network integration

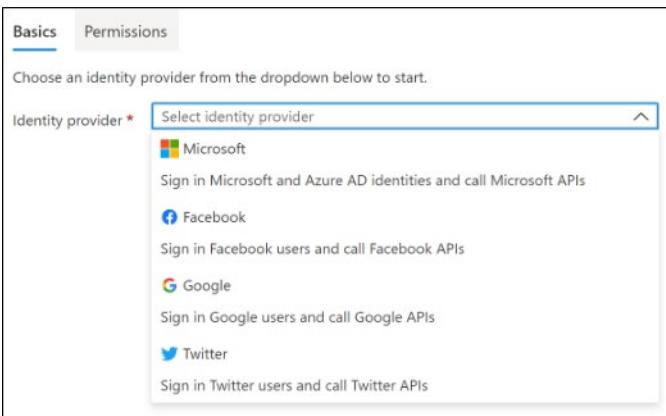
# Secure an App Service

Azure App Service provides built-in authentication and authorization support, so you can sign in users and access data by writing minimal or no code in your web app, API, and mobile back end, and also Azure Functions.

Secure authentication and authorization requires deep understanding of security, including federation, encryption, JSON web tokens (JWT) management, grant types, and so on. App Service provides these utilities so that you can spend more time and energy on providing business value to your customer.

**Note:** You're not required to use App Service for authentication and authorization. Many web frameworks are bundled with security features, and you can use them if you like.

## How it works



The authentication and authorization module runs in the same sandbox as your application code. When it's enabled, every incoming HTTP request passes through it before being handled by your application code. This module handles several things for your app:

- Authenticates users with the specified provider.
- Validates, stores, and refreshes tokens.
- Manages the authenticated session.
- Injects identity information into request headers.

The module runs separately from your application code and is configured using app settings. No SDKs, specific languages, or changes to your application code are required.

## Authorization behavior

In the Azure portal, you can configure App Service authorization with a number of behaviors:

1. **Allow Anonymous requests (no action):** This option defers authorization of unauthenticated traffic to your application code. For authenticated requests, App Service also passes along authentication information in the HTTP headers. This option provides more flexibility in handling anonymous requests. It lets you present multiple sign-in providers to your users.
2. **Allow only authenticated requests:** The option is **Log in with <provider>**. App Service redirects all anonymous requests to `/.auth/login/<provider>` for the provider you choose. If the anonymous request comes from a native mobile app, the returned response is an `HTTP 401 Unauthorized`. With this option, you don't need to write any authentication code in your app.

**Note:** Restricting access in this way applies to all calls to your app, which may not be desirable for apps wanting a publicly available home page, as in many single-page applications.

## Logging and tracing

If you enable application logging, you will see authentication and authorization traces directly in your log files. If you see an authentication error that you didn't expect, you can conveniently find all the details by looking in your existing application logs. If you enable failed request tracing, you can see exactly what role the authentication and authorization module may have played in a failed request. In the trace logs, look for references to a module named `EasyAuthModule_32/64`.

## Create Custom Domain Names

When you create a web app, Azure assigns it to a subdomain of `azurewebsites.net`. For example, if your web app is named `contoso`, the URL is `contoso.azurewebsites.net`. Azure also assigns a virtual IP address. For a production web app, you may want users to see a custom domain name.



## Configuration steps

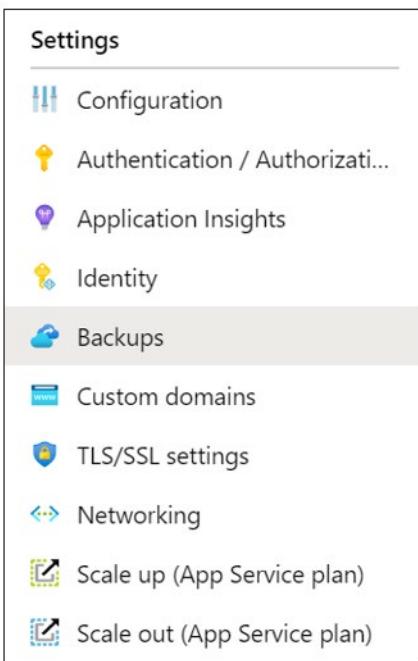
1. **Reserve your domain name.** If you haven't already registered for an external domain name (i.e. not `.azurewebsites.net`) already, the easiest way to set up a custom domain is to buy one directly in the Azure portal. The process enables you to manage your web app's domain name directly in the Portal instead of going to a third-party site to manage it. Likewise, configuring the domain name in your web app is greatly simplified. If you do not use the portal, you can use any domain registrar. When you sign up, the registration site will help you through the process.
2. **Create DNS records that map the domain to your Azure web app.** The Domain Name System (DNS) uses data records to map domain names into IP addresses. There are several types of DNS records. For web apps, you'll create either an A record or a CNAME record. If the IP address changes, a CNAME entry is still valid, whereas an A record must be updated. However, some domain registrars do not allow CNAME records for the root domain or for wildcard domains. In that case, you must use an A record.
  - An A (Address) record maps a domain name to an IP address.
  - A CNAME (Canonical Name) record maps a domain name to another domain name. DNS uses the second name to look up the address. Users still see the first domain name in their browser. For example, you could map `contoso.com` to `yourwebapp.azurewebsites.net`.

3. **Enable the custom domain.** After obtaining your domain and creating your DNS record, you can use the portal to validate the custom domain and add it to your web app. Be sure to test.

**Note:** To map a custom DNS name to a web app, the web app's App Service plan must be a paid tier.

## Backup an App Service

The Backup and Restore feature in Azure App Service lets you easily create app backups manually or on a schedule. You can configure the backups to be retained up to an indefinite amount of time. You can restore the app to a snapshot of a previous state by overwriting the existing app or restoring to another app.



### What gets backed up

App Service can back up the following information to an Azure storage account and container that you have configured your app to use.

- App configuration.
- File content.
- Database connected to your app (SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, MySQL in-app).

### Considerations

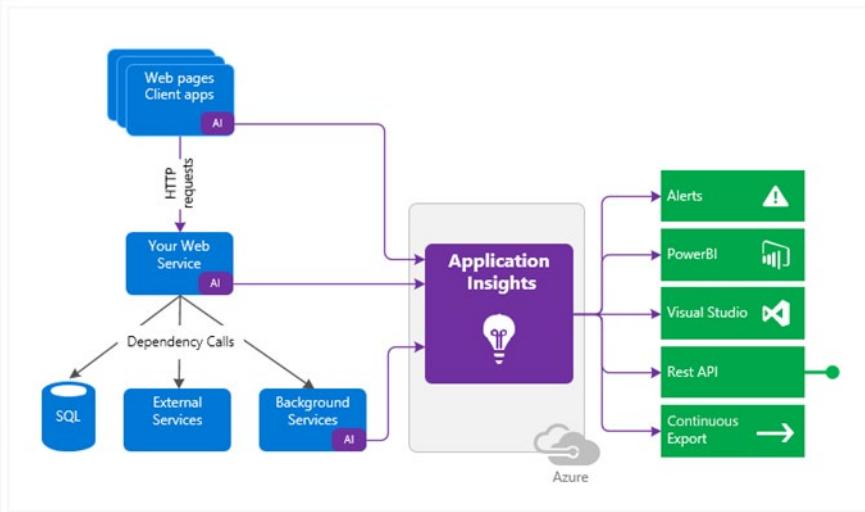
- The Backup and Restore feature requires the App Service plan to be in the Standard tier or Premium tier.
- You can configure backups manually or on a schedule.
- You need an Azure storage account and container in the same subscription as the app that you want to back up. After you have made one or more backups for your app, the backups are visible on the

Containers page of your storage account, and your app. In the storage account, each backup consists of a.zip file that contains the backup data and an .xml file that contains a manifest of the .zip file contents. You can unzip and browse these files if you want to access your backups without actually performing an app restore.

- Full backups are the default. When a full backup is restored, all content on the site is replaced with whatever is in the backup. If a file is on the site, but not in the backup it gets deleted.
- Partial backups are supported. Partial backups allow you choose exactly which files you want to back up. When a partial backup is restored, any content that is located in one of the excluded directories, or any excluded file, is left as is. You restore partial backups of your site the same way you would restore a regular backup.
- You can exclude files and folders you do not want in the backup.
- Backups can be up to 10 GB of app and database content.
- Using a firewall enabled storage account as the destination for your backups is not supported.

## Use Application Insights

Application Insights, a feature of Azure Monitor, monitors your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app. It's designed to help you continuously improve performance and usability. Insights works on various platforms including .NET, Node.js and Java EE, hosted on-premises, hybrid, or any public cloud. It integrates with your DevOps process, and has connection points to a variety of development tools. It can monitor and analyze data from mobile apps by integrating with Visual Studio App Center.



## Application Insights features

Application Insights is aimed at the development team, to help you understand how your app is performing and how it's being used. It monitors:

- **Request rates, response times, and failure rates** - Find out which pages are most popular, at what times of day, and where your users are. See which pages perform best. If your response times and failure rates go high when there are more requests, then perhaps you have a resourcing problem.

- **Dependency rates, response times, and failure rates** - Find out whether external services are slowing you down.
- **Exceptions** - Analyze the aggregated statistics, or pick specific instances and drill into the stack trace and related requests. Both server and browser exceptions are reported.
- **Page views and load performance** - reported by your users' browsers.
- **User and session counts**.
- **Performance counters** from your Windows or Linux server machines, such as CPU, memory, and network usage.
- **Host diagnostics** from Docker or Azure.
- **Diagnostic trace logs** from your app - so that you can correlate trace events with requests.
- **Custom events and metrics** that you write yourself in the client or server code, to track business events such as items sold or games won.

## Demonstration - Create and App Service

In this demonstration, we will create a new web app that runs a Docker container. The container displays a Welcome message.

### Create a Web App

Azure App Service is a collection of four services, all of which are built to help you host and run web applications. The four services (Web Apps, Mobile Apps, API Apps, and Logic Apps) look different, but in the end they all operate in very similar ways. Web Apps are the most used of the four services, and this is the service that we will be using in this lab.

In this task, you will create an Azure App Service Web App.

1. Sign-in to the [Azure portal](#)<sup>7</sup>.
2. From the **All services** blade, search for and select **App Services**, and click **+ Add**
3. On the **Basics** tab of the **Web App** blade, specify the following settings (replace **xxxx** in the name of the web app with letters and digits such that the name is globally unique). Leave the defaults for everything else, including the App Service Plan.

| Setting          | Value                                                          |
|------------------|----------------------------------------------------------------|
| Subscription     | <b>Choose your subscription</b>                                |
| Resource Group   | <b>myRGWebApp1</b> (create new)                                |
| Name             | <b>myLinuxWebAppxxxx</b> (unique)                              |
| Publish          | <b>Docker Container</b>                                        |
| Operating System | <b>Linux</b>                                                   |
| Region           | <b>East US</b> (ignore any service plan availability warnings) |

4. Click **Next > Docker** and configure the container information. The startup command is optional and not needed in this exercise.

| Setting | Value                   |
|---------|-------------------------|
| Options | <b>Single container</b> |

<sup>7</sup> <http://portal.azure.com/>

| Setting      | Value                     |
|--------------|---------------------------|
| Image Source | <b>Quickstart</b>         |
| Sample       | <b>Python Hello World</b> |

5. Click **Review + create**, and then click **Create**.

### Test the Web App

In this task, we will test the Web App.

1. Wait for the Web App to deploy.
2. From **Notifications** click **Go to resource**.
3. On the **Overview** blade, locate the **URL** entry.
4. Click on the **URL** to open the new browser tab and display the "Hello World, App Service!" page.
5. Switch back to the **Overview** blade of your web app and notice that it includes several charts. If you repeat step 4 a few times, you should be able to see corresponding telemetry being displayed in the charts. This includes number of requests and average response time.

### Configure Deployment Slots

In this task, we will configure Deployment Slots for the Web App.

1. From the Web App blade, click **Deployment Slots**.
2. On the **Deployment Slots** blade, click **+ Add Slot**
3. From the **Add a slot** blade, configure the following settings.

| Setting             | Value                    |
|---------------------|--------------------------|
| Name                | <b>DEVELOPMENT</b>       |
| Clone Settings From | <b>myLinuxWebAppXXXX</b> |

4. Click **Add**.
5. If the **Add a slot** blade remains open, click **Close**.
6. From the **Deployment Slots** blade, notice the **Names**, their **Status**, and the **Traffic %** of each Deployment Slot.
7. Click the newly created Deployment Slot **mylinuxwebappXXXX-DEVELOPMENT**. This will take you to the **Overview** blade of the new Deployment Slot.
8. From the **Overview** blade of the DEVELOPMENT Deployment Slot, locate the **URL** entry.
9. Click on the **URL** to open the new browser tab and display the "Hello World, App Service!" page.

**Note:** The process of cloning the Web App settings to the new Deployment Slot, includes cloning the base Docker Image from the initial deployment.

10. Click the **X** in the top right corner of the DEVELOPMENT Deployment Slot blade. This will return you to the **Deployment Slots** blade of the **myLinuxWebAppXXXX** Web App.

### Configure Backup

1. From the Web App blade, click **Backups**.
2. On the **Backups** blade, click **Configure**. This will open up the **Backup Configuration** blade.
3. From the **Backup Configuration** blade, under **Backup Storage**, click **Storage not configured** to configure a Storage Account for backups.

4. On the **Storage accounts** blade, click + **Storage account**.
5. From the **Create storage account** blade, configure the following settings.

| Setting      | Value                                  |
|--------------|----------------------------------------|
| Name         | <b>webappxxxxstorage</b> (unique)      |
| Account kind | <b>Storage (general purpose v1)</b>    |
| Performance  | <b>Standard</b>                        |
| Replication  | <b>Locally-redundant storage (LRS)</b> |
| Location     | <b>(US) East US</b>                    |

6. Click **OK**.
7. On the **Storage accounts** blade, click the Storage Account, **webappxxxxstorage**, that you created in the previous step.
8. From the **Containers** blade, click + **Container**, enter **backups** for the name of the New Container, and set the **Public access level** to **Private (no anonymous access)**.
9. Click **OK**.
10. From the **Containers** blade, click **backups**, and click **Select** to choose the newly created Container. This will take you back to the **Backup Configuration** blade.
11. On the **Backup Configuration** blade, click **On** next to **Scheduled backup**, and configure the following settings.

| Setting                    | Value                              |
|----------------------------|------------------------------------|
| Backup Every               | <b>1 Hours</b>                     |
| Start backup schedule from | <b>Configure custom start time</b> |
| Retention (Days)           | <b>30</b>                          |
| Keep at least one backup   | <b>Yes</b>                         |

12. Click **Save**.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Which of the following settings is not swapped when you swap an app? Select one.*

- Framework version
- Public certificates
- Scale settings

## Multiple choice

*Which of the following is not true about App Service backups? Select one.*

- Incremental backups are the default.
- You can configure backups manually or on a schedule.
- You can exclude files and folders you do not want in the backup.

## Multiple choice

*What method does Microsoft Azure App Service use to obtain credentials for users attempting to access an app? Select one.*

- Credentials that are stored in the browser.
- Pass-through authentication.
- Redirection to a provider endpoint.

## Multiple choice

*Which of the following isn't a valid automated deployment source? Select one.*

- Azure DevOps
- GitHub
- SharePoint

# Summary and Resources

## Summary

Azure App Service is an HTTP-based service for hosting web applications. You can develop in your favorite language. Applications run and scale with ease on both Windows and Linux-based environments.

You should now be able to:

- Identify features and usage cases for the the Azure App Service.
- Create an App Service.
- Configure deployment settings, specifically deployment slots.
- Secure the App Service.
- Configure custom domain names
- Backup the App Service.
- Configure Application Insights.

## Learn more

You can learn more by reviewing the following.

- Azure App Service Overview

- **Application Insights<sup>8</sup>**
- **Learn - Host a web application with Azure App Service<sup>9</sup>**
- **Learn - Stage a web app deployment for testing and rollback by using App Service deployment slots<sup>10</sup>**
- **Learn - Capture and view page load times in your Azure web app with Application Insights<sup>11</sup>**
- **Learn - Dynamically meet changing web app performance requirements with autoscale rules<sup>12</sup>**

---

<sup>8</sup> <https://docs.microsoft.com/Azure/azure-monitor/app/app-insights-overview>

<sup>9</sup> <https://docs.microsoft.com/learn/modules/host-a-web-app-with-azure-app-service/>

<sup>10</sup> <https://docs.microsoft.com/learn/modules/stage-deploy-app-service-deployment-slots/>

<sup>11</sup> <https://docs.microsoft.com/learn/modules/capture-page-load-times-application-insights/>

<sup>12</sup> <https://docs.microsoft.com/learn/modules/app-service-autoscale-rules/>

# Configure Azure Container Instances

## Introduction

### Scenario

Containers offer a standardized and repeatable way to package, deploy and manage cloud applications. Azure Container Instances let you run a container in Azure without managing virtual machines and without a higher-level service.

You work for an online clothing retailer using containers for internal apps. These apps are hosted on-premises, in Azure, and in other cloud providers. The apps can share the hardware resources, but shouldn't access resources used by other apps.

The company relies on you to deploy, manage, size, and scale these containers.

### Skills measured

Azure Container Instances is part of **Exam AZ-104: Microsoft Azure Administrator<sup>13</sup>**.

Deploy and manage Azure compute resources (20–25%)

Create and configure containers

- Configure sizing and scaling for Azure Container Instances.
- Configure container groups for Azure Container Instances.

### Learning objectives

In this module, you will learn how to:

- Identify when to use containers versus virtual machines.
- Identify the features and usage cases of Azure Container Instances.
- Implement Azure Container Groups.

### Prerequisites

None.

## Compare Containers to Virtual Machines

Hardware virtualization has made it possible to run multiple isolated instances of operating systems concurrently on the same physical hardware. Containers represent the next stage in the virtualization of computing resources. Container-based virtualization allows you to virtualize the operating system. This way, you can run multiple applications within the same instance of an operating system, while maintaining isolation between the applications. This means that containers within a VM provide functionality similar to that of VMs within a physical server. To better understand this concept, it is helpful to compare containers and virtual machines.

---

<sup>13</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

| Feature            | Containers                                                                                                                                            | Virtual Machines                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Isolation          | Typically provides lightweight isolation from the host and other containers but doesn't provide as strong a security boundary as a virtual machine.   | Provides complete isolation from the host operating system and other VMs. This is useful when a strong security boundary is critical, such as hosting apps from competing companies on the same server or cluster. |
| Operating system   | Runs the user mode portion of an operating system and can be tailored to contain just the needed services for your app, using fewer system resources. | Runs a complete operating system including the kernel, thus requiring more system resources (CPU, memory, and storage).                                                                                            |
| Deployment         | Deploy individual containers by using Docker via command line; deploy multiple containers by using an orchestrator such as Azure Kubernetes Service.  | Deploy individual VMs by using Windows Admin Center or Hyper-V Manager; deploy multiple VMs by using PowerShell or System Center Virtual Machine Manager.                                                          |
| Persistent storage | Use Azure Disks for local storage for a single node, or Azure Files (SMB shares) for storage shared by multiple nodes or servers.                     | Use a virtual hard disk (VHD) for local storage for a single VM, or an SMB file share for storage shared by multiple servers.                                                                                      |
| Fault tolerance    | If a cluster node fails, any containers running on it are rapidly recreated by the orchestrator on another cluster node.                              | VMs can fail over to another server in a cluster, with the VM's operating system restarting on the new server.                                                                                                     |

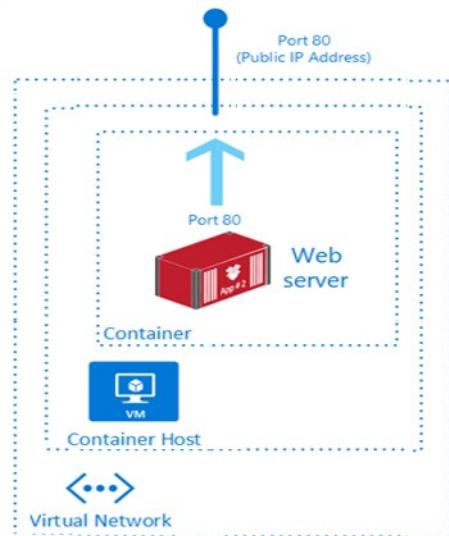
## Container advantages

Containers offer several advantages over physical and virtual machines, including:

- Increased flexibility and speed when developing and sharing the application code.
- Simplified application testing.
- Streamlined and accelerated application deployment.
- Higher workload density, resulting in improved resource utilization.

## Review Azure Container Instances

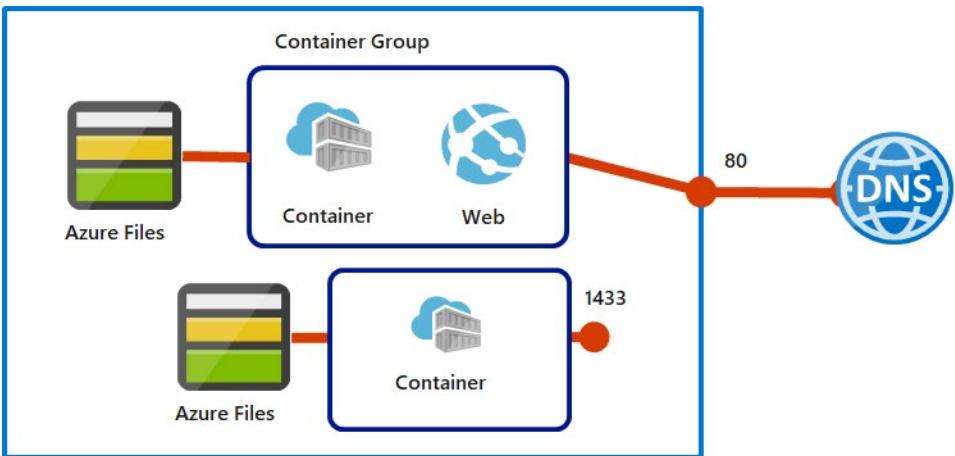
Containers are becoming the preferred way to package, deploy, and manage cloud applications. Azure Container Instances offers the fastest and simplest way to run a container in Azure, without having to manage any virtual machines and without having to adopt a higher-level service. Azure Container Instances is a great solution for any scenario that can operate in isolated containers, including simple applications, task automation, and build jobs.



| Feature                              | Description                                                                                          |
|--------------------------------------|------------------------------------------------------------------------------------------------------|
| Fast Startup Times                   | Containers can start in seconds without the need to provision and manage virtual machines.           |
| Public IP Connectivity and DNS Names | Containers can be directly exposed to the internet with an IP address and FQDN.                      |
| Hypervisor-level Security            | Container applications are as isolated in a container as they would be in a virtual machine.         |
| Custom Sizes                         | Container nodes can be scaled dynamically to match actual resource demands for an application.       |
| Persistent Storage                   | Containers support direct mounting of Azure File Shares.                                             |
| Linux and Windows Containers         | Container instances supports scheduling of multi-container groups that share host machine resources. |
| Coscheduled Groups                   | Container instances supports scheduling of multi-container groups that share host machine resources. |
| Virtual Network Deployment           | Container instances can be deployed into an Azure virtual network.                                   |

## Implement Container Groups

The top-level resource in Azure Container Instances is the container group. A container group is a collection of containers that get scheduled on the same host machine. The containers in a container group share a lifecycle, resources, local network, and storage volumes. It's similar in concept to a pod in Kubernetes.



An example container group:

- Is scheduled on a single host machine.
- Is assigned a DNS name label.
- Exposes a single public IP address, with one exposed port.
- Consists of two containers. One container listens on port 80, while the other listens on port 1433.
- Includes two Azure file shares as volume mounts, and each container mounts one of the shares locally.

## Deployment options

Here are two common ways to deploy a multi-container group: use a Resource Manager template or a YAML file. A Resource Manager template is recommended when you need to deploy additional Azure service resources (for example, an Azure Files share) when you deploy the container instances. Due to the YAML format's more concise nature, a YAML file is recommended when your deployment includes only container instances.

## Resource allocation

Azure Container Instances allocates resources such as CPUs, memory, and optionally GPUs to a multi-container group by adding the resource requests of the instances in the group. Taking CPU resources as an example, if you create a container group with two container instances, each requesting one CPU, then the container group is allocated 2 CPUs.

## Networking

Container groups can share an external-facing IP address, one or more ports on that IP address, and a DNS label with a fully qualified domain name (FQDN). To enable external clients to reach a container within the group, you must expose the port on the IP address and from the container. Because containers within the group share a port namespace, port mapping isn't supported. A container group's IP address and FQDN will be released when the container group is deleted.

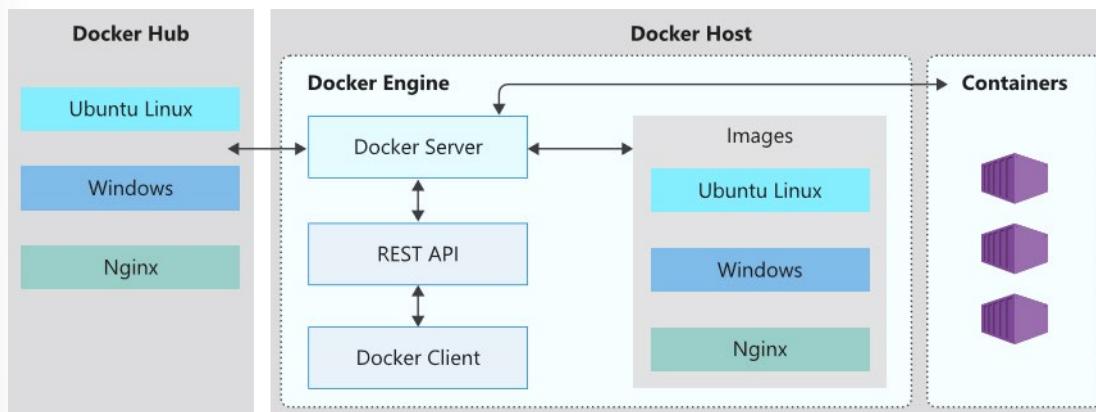
## Common scenarios

Multi-container groups are useful in cases where you want to divide a single functional task into a small number of container images. These images can then be delivered by different teams and have separate resource requirements. Example usage could include:

- A container serving a web application and a container pulling the latest content from source control.
- An application container and a logging container. The logging container collects the logs and metrics output by the main application and writes them to long-term storage.
- An application container and a monitoring container. The monitoring container periodically makes a request to the application to ensure that it's running and responding correctly, and raises an alert if it's not.
- A front-end container and a back-end container. The front end might serve a web application, with the back end running a service to retrieve data.

## Review the Docker Platform

Docker is a platform that enables developers to host applications within a container.



A container is essentially a standalone package that contains everything that is needed to execute a piece of software. The package includes:

- The application executable code.
- The runtime environment (such as .NET Core).
- System tools.
- Settings.

The Docker platform is available on both Linux and Windows and can be hosted on Azure. The key thing that Docker provides is the guarantee that the containerized software will always run the same. It doesn't matter if the code is run locally on Windows, Linux or in the cloud on Azure. The software can be developed locally within a Docker container, shared with Quality Assurance resources for testing, and then deployed to production in the Azure Cloud. Once deployed, the application can easily be scaled up and down using the Azure Container Instances (ACI).

## Docker terminology

You should be familiar with the following key terms before using Docker and Container Instances to create, build, and test containers:

- **Container.** Container is an instance of a Docker image. It represents the execution of a single application, process, or service. It consists of the contents of a Docker image, an execution environment, and a standard set of instructions. When scaling a service, you create multiple instances of a container from the same image. Or a batch job can create multiple containers from the same image, passing different parameters to each instance.
- **Container image.** Container image refers to a package with all the dependencies and information required to create a container. The dependencies include frameworks and the deployment and execution configuration that a container runtime uses. Usually, an image derives from multiple base images that are layers stacked on top of each other to form the container's file system. An image is immutable once it has been created.
- **Build.** Build refers to the action of building a container image based on the information and context provided by the Dockerfile. The build also includes any other files that are needed. You build images by using the Docker docker build command.
- **Pull.** Pull refers to the process of downloading a container image from a container registry.
- **Push.** Push refers to the process of uploading a container image to a container registry.
- **Dockerfile.** Dockerfile refers to a text file that contains instructions on how to build a Docker image. The Dockerfile is like a batch script. The first line identifies the base image. The rest of the file includes the build actions.

## Demonstration - Deploy Azure Container Instances

In this demonstration we create, configure, and deploy a container by using Azure Container Instances (ACI) in the Azure Portal. The container is a Welcome to ACI web application that displays a static HTML page.

### Create a container instance

In this task, we will create a new container instance for the web application.

1. Sign in to the Azure portal.
2. From the **All services** blade, search for and select **Container instances** and then click **+ Add, + Create, + New**.
3. Provide the following Basic details for the new container instance (leave the defaults for everything else):

| Setting        | Value                               |
|----------------|-------------------------------------|
| Subscription   | <b>Use default supplied</b>         |
| Resource group | <b>Create new resource group</b>    |
| Container name | <b>mycontainer</b>                  |
| Region         | <b>(US) East US</b>                 |
| Image source   | <b>Docker Hub or other registry</b> |
| Image type     | <b>Public</b>                       |
| Image          | <b>microsoft/aci-helloworld</b>     |

| Setting | Value                       |
|---------|-----------------------------|
| OS type | <b>Linux</b>                |
| Size    | <b>Leave at the default</b> |

4. Configure the Networking tab (replace **xxxxx** with letters and digits such that the name is globally unique). Leave all other settings at their default values.

| Setting        | Value                      |
|----------------|----------------------------|
| DNS name label | <b>mycontainerdnsxxxxx</b> |

**Note:** Your container will be publicly reachable at dns-name-label.region.azurecontainer.io. If you receive a **DNS name label not available** error message following the deployment, specify a different DNS name label (replacing the xxxx) and re-deploy.

5. Click **Review and Create** to start the automatic validation process.
6. Click **Create** to create the container instance.
7. Monitor the deployment page and the **Notifications** page.

#### Verify deployment of the container instance

In this task, we verify that the container instance is running by ensuring that the welcome page displays.

1. After the deployment is complete, click the **Go to resource** link the deployment blade or the link to the resource in the Notification area.
2. On the **Overview** blade of **mycontainer**, ensure your container **Status** is **Running**.
3. Locate the Fully Qualified Domain Name (FQDN).
4. Copy the container's FQDN into a new web browser tab and press **Enter**. The Welcome page should display.

**Note:** To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click **Delete resource group**. Verify the name of the resource group and then click **Delete**. Monitor the **Notifications** to see how the delete is proceeding.

## Knowledge Check

Choose the best response for each question.

### Multiple choice

*Which of the following is not true about container groups?*

- Are scheduled on multiple host machines.
- Consists of two containers.
- Exposes a single public IP address, with one exposed port.

## Multiple choice

*Which of the following is a reason to select virtual machines over containers?*

- Virtual machines provide complete isolation from the host operating system and other VMs.
- Virtual machines run the user mode portion of an operating system and can be tailored to contain just the needed services for your app.
- Virtual machines use Azure Disks for local storage for a single node.

## Multiple choice

*All the following are true about Azure Container Instances, except?*

- You are billed only when the container is in use.
- Containers launch in seconds.
- Container storage uses Azure blobs.

## Summary and Resources

### Summary

Azure Container Instances is a great solution for any scenario that can operate in isolated containers. This includes simple applications, task automation, and build jobs.

You should now be able to:

- Identify when to use Azure Containers versus Azure virtual machines.
- Identify the features and usage cases of Azure Container Instances.
- Implement Azure Container Groups.

### Learn more

You can learn more by reviewing the following.

- **Containers vs Virtual Machines<sup>14</sup>**
- **Azure Container Instances documentation<sup>15</sup>**
- **Learn - Introduction to Docker containers<sup>16</sup>**
- **Learn - Run Docker containers with Azure Container Instances<sup>17</sup>**
- **Learn - Build a containerized web application with Docker<sup>18</sup>**

<sup>14</sup> <https://docs.microsoft.com/virtualization/windowscontainers/about/containers-vs-vm>

<sup>15</sup> <https://docs.microsoft.com/azure/container-instances/>

<sup>16</sup> <https://docs.microsoft.com/learn/modules/intro-to-docker-containers/>

<sup>17</sup> <https://docs.microsoft.com/learn/modules/run-docker-with-azure-container-instances/>

<sup>18</sup> <https://docs.microsoft.com/learn/modules/intro-to-containers/>

# Configure Azure Kubernetes Service

## Introduction

### Scenario

The standard container management runtime focuses on managing individual containers. If you want to scale a complex system with multiple containers working together, this scenario becomes challenging. To make the management process easier, it's common to use a container management platform, such as Kubernetes.

Suppose you work at a fleet management company. Your company provides an asset tracking solution to customers worldwide. Your tracking solution is built and deployed as microservices. You're using containerized instances to quickly deploy into new customer regions and scale resources as needed to meet customer demands. The company plans to use AKS to deploy, and manage containerized applications.

You need to manage storage, scaling, network connections, and upgrades for the AKS solution.

### Skills measured

The Azure Kubernetes Service is part of **Exam AZ-104: Microsoft Azure Administrator<sup>19</sup>**.

Deploy and manage Azure compute resources (20–25%)

Create and configure containers

- Configure storage for Azure Kubernetes Service (AKS).
- Configure scaling for AKS.
- Configure network connections for AKS.
- Upgrade an AKS cluster.

### Learning objectives

In this module, you will learn how to:

- Identify AKS components including pods, clusters, and nodes.
- Configure network connections for AKS.
- Configure storage options for AKS.
- Implement security options for AKS.
- Scale AKS including adding Azure Container Instances.

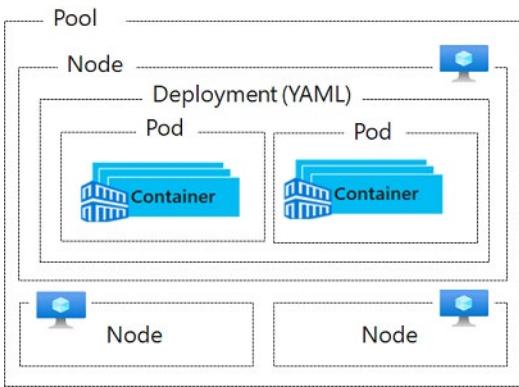
### Prerequisites

None.

---

<sup>19</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

## Explore AKS Terminology



**Pools** are groups of nodes with identical configurations.

**Nodes** are individual virtual machines running containerized applications.

**Pods** are a single instance of an application. A pod can contain multiple containers.

**Container** is a lightweight and portable executable image that contains software and all of its dependencies.

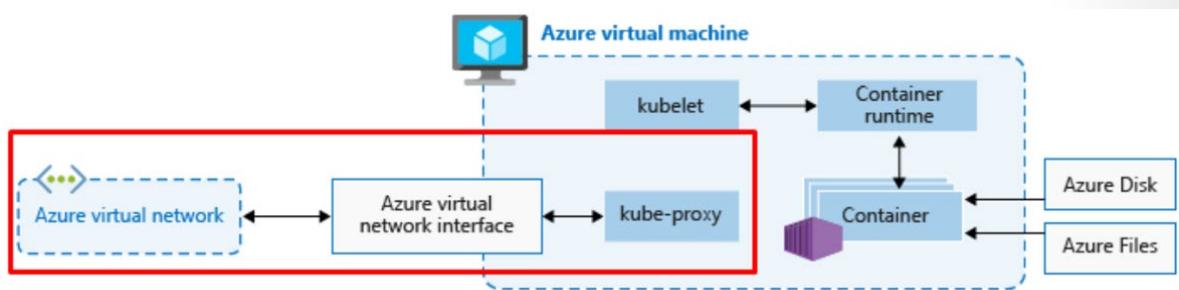
**Deployment** has one or more identical pods managed by Kubernetes.

**Manifest** is the YAML file describing a deployment.

## Explore AKS Clusters and Nodes

A Kubernetes cluster is divided into two components:

- **Azure-managed nodes**, which provide the core Kubernetes services and orchestration of application workloads.
- **Customer-managed nodes** that run your application workloads.



### Azure-managed node

When you create an AKS cluster, a cluster node is automatically created and configured. This node is provided as a managed Azure resource abstracted from the user. You pay only for running agent nodes

## Nodes and node pools

To run your applications and supporting services, you need a Kubernetes node. An AKS cluster contains one or more nodes (Azure Virtual Machines) that run the Kubernetes node components and the container runtime.

- The *kubelet* is the Kubernetes agent that processes the orchestration requests from the Azure-managed node, and scheduling of running the requested containers.
- Virtual networking is handled by the *kube-proxy* on each node. The proxy routes network traffic and manages IP addressing for services and pods.
- The *container runtime* is the component that allows containerized applications to run and interact with additional resources such as the virtual network and storage. AKS clusters using Kubernetes version 1.19 node pools and greater use containerd as its container runtime. AKS clusters using Kubernetes prior to v1.19 for node pools use Moby (upstream docker) as its container runtime.

Nodes of the same configuration are grouped together into *node pools*. A Kubernetes cluster contains one or more node pools. The initial number of nodes and size are defined when you create an AKS cluster, which creates a default node pool. This default node pool in AKS contains the underlying VMs that run your agent nodes.

## Configure AKS Networking

To allow access to your applications, or for application components to communicate with each other, Kubernetes provides an abstraction layer to virtual networking. Kubernetes nodes are connected to a virtual network, and can provide inbound and outbound connectivity for pods. The *kube-proxy* component runs on each node to provide these network features.

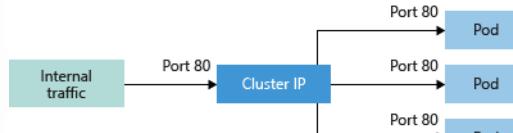
In Kubernetes, Services logically group pods to allow for direct access via an IP address or DNS name and on a specific port. You can also distribute traffic using a load balancer. More complex routing of application traffic can also be achieved with Ingress Controllers. Security and filtering of the network traffic for pods is possible with Kubernetes network policies.

The Azure platform also helps to simplify virtual networking for AKS clusters. When you create a Kubernetes load balancer, the underlying Azure load balancer resource is created and configured. As you open network ports to pods, the corresponding Azure network security group rules are configured. For HTTP application routing, Azure can also configure external DNS as new ingress routes are configured.

## Services

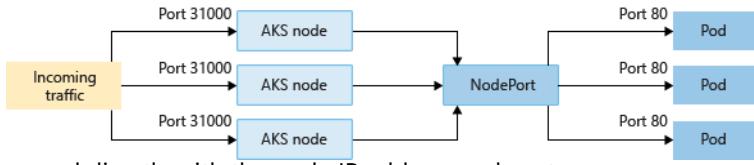
To simplify the network configuration for application workloads, Kubernetes uses Services to logically group a set of pods together and provide network connectivity. The following Service types are available:

- **Cluster IP** - Creates an internal IP address for use within the AKS cluster. Good for internal-only



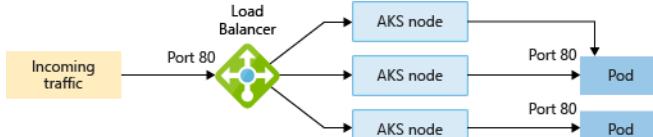
applications that support other workloads within the cluster.

- **NodePort** - Creates a port mapping on the underlying node that allows the application to be accessed directly with the node IP address and port.



Accessed directly with the node IP address and port.

- **LoadBalancer** - Creates an Azure load balancer resource, configures an external IP address, and connects the requested pods to the load balancer backend pool. To allow customers traffic to reach



the application, load-balancing rules are created on the desired ports. For additional control and routing of the inbound traffic, you may instead use an Ingress controller.

- **ExternalName** - Creates a specific DNS entry for easier application access.

The IP address for load balancers and services can be dynamically assigned, or you can specify an existing static IP address to use. Both internal and external static IP addresses can be assigned. This existing static IP address is often tied to a DNS entry.

Both *internal* and *external* load balancers can be created. Internal load balancers are only assigned a private IP address, so can't be accessed from the Internet.

## Pods

Kubernetes uses pods to run an instance of your application. A pod represents a single instance of your application. Pods typically have a 1:1 mapping with a container, although there are advanced scenarios where a pod might contain multiple containers. These multi-container pods are scheduled together on the same node, and allow containers to share related resources.

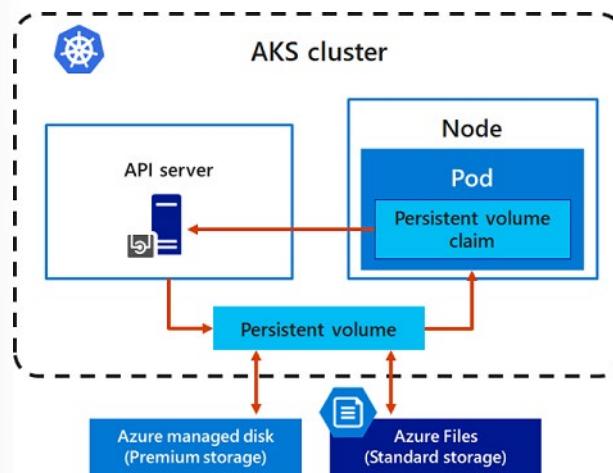
When you create a pod, you can define resource limits to request a certain amount of CPU or memory resources. The Kubernetes Scheduler attempts to schedule the pods to run on a node with available resources to meet the request. You can also specify maximum resource limits that prevent a given pod from consuming too much compute resource from the underlying node.

**Note:** A best practice is to include resource limits for all pods to help the Kubernetes Scheduler understand what resources are needed and permitted.

A pod is a logical resource, but the container (or containers) is where the application workloads run. Pods are typically ephemeral, disposable resources. Therefore, individually scheduled pods miss some of the high availability and redundancy features Kubernetes provides. Instead, pods are usually deployed and managed by Kubernetes controllers, such as the Deployment controller.

## Configure AKS Storage

Applications that run in Azure Kubernetes Service (AKS) may need to store and retrieve data. For some application workloads, this data storage can use local, fast storage on the node that is no longer needed when the pods are deleted. Other application workloads may require storage that persists on more regular data volumes within the Azure platform. Multiple pods may need to share the same data volumes, or reattach data volumes if the pod is rescheduled on a different node. Finally, you may need to inject sensitive data or application configuration information into pods.



This section introduces the core concepts that provide storage to your applications in AKS:

- Volumes
- Persistent volumes
- Storage classes
- Persistent volume claims

## Volumes

Applications often need to be able to store and retrieve data. As Kubernetes typically treats individual pods as ephemeral, disposable resources, different approaches are available for applications use and persist data as necessary. A *volume* represents a way to store, retrieve, and persist data across pods and through the application lifecycle.

Traditional volumes to store and retrieve data are created as Kubernetes resources backed by Azure Storage. You can manually create these data volumes to be assigned to pods directly, or have Kubernetes automatically create them. These data volumes can use Azure Disks or Azure Files:

- *Azure Disks* can be used to create a Kubernetes *DataDisk* resource. Disks can use Azure Premium storage, backed by high-performance SSDs, or Azure Standard storage, backed by regular HDDs. For most production and development workloads, use Premium storage. Azure Disks are mounted as *ReadWriteOnce*, so are only available to a single node. For storage volumes that can be accessed by multiple nodes simultaneously, use Azure Files.
- *Azure Files* can be used to mount an SMB 3.0 share backed by an Azure Storage account to pods. Files let you share data across multiple nodes and pods. Files can use Azure Standard storage backed by regular HDDs, or Azure Premium storage, backed by high-performance SSDs.

## Persistent volumes

Volumes are defined and created as part of the pod lifecycle only exist until the pod is deleted. Pods often expect their storage to remain if a pod is rescheduled on a different host during a maintenance event, especially in StatefulSets. A *persistent volume* (PV) is a storage resource created and managed by the Kubernetes API that can exist beyond the lifetime of an individual pod.

Azure Disks or Files are used to provide the PersistentVolume. As noted in the previous section on Volumes, the choice of Disks or Files is often determined by the need for concurrent access to the data or the performance tier.

A PersistentVolume can be *statically* created by a cluster administrator, or dynamically created by the Kubernetes API server. If a pod is scheduled and requests storage that is not currently available, Kubernetes can create the underlying Azure Disk or Files storage and attach it to the pod. Dynamic provisioning uses a *StorageClass* to identify what type of Azure storage needs to be created.

## Storage classes

To define different tiers of storage, such as Premium and Standard, you can create a *StorageClass*. The StorageClass also defines the *reclaimPolicy*. This reclaimPolicy controls the behavior of the underlying Azure storage resource when the pod is deleted and the persistent volume may no longer be required. The underlying storage resource can be deleted, or retained for use with a future pod.

In AKS, four initial StorageClasses are created for cluster using the in-tree storage plugins:

- default - Uses Azure StandardSSD storage to create a Managed Disk. The reclaim policy ensures that the underlying Azure Disk is deleted when the persistent volume that used it is deleted.
- managed-premium - Uses Azure Premium storage to create a Managed Disk. The reclaim policy again ensures that the underlying Azure Disk is deleted when the persistent volume that used it is deleted.
- azurefile - Uses Azure Standard storage to create an Azure File Share. The reclaim policy ensures that the underlying Azure File Share is deleted when the persistent volume that used it is deleted.
- azurefile-premium - Uses Azure Premium storage to create an Azure File Share. The reclaim policy ensures that the underlying Azure File Share is deleted when the persistent volume that used it is deleted.

If no StorageClass is specified for a persistent volume, the default StorageClass is used. Take care when requesting persistent volumes so that they use the appropriate storage you need. You can create a StorageClass for additional needs using `kubectl`.

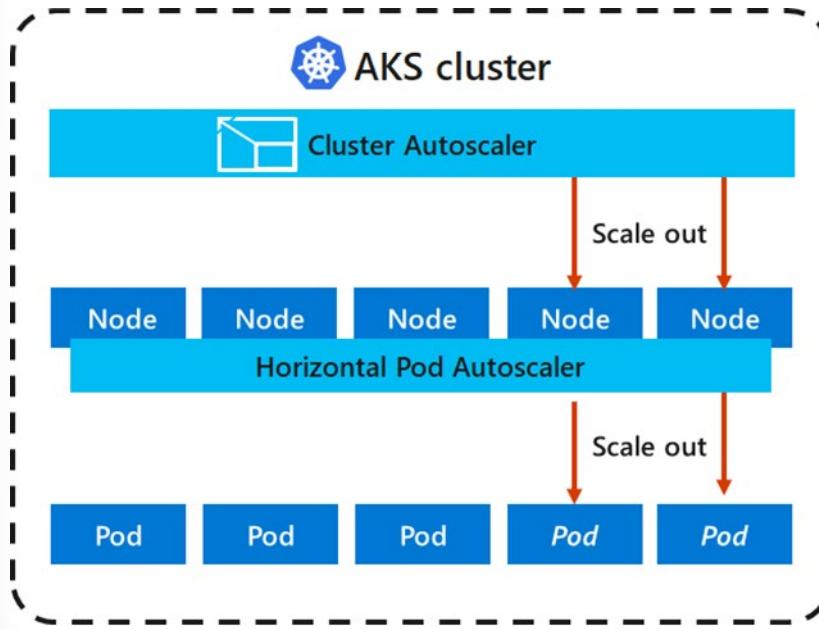
## Persistent volume claims

A PersistentVolumeClaim requests either Disk or File storage of a particular StorageClass, access mode, and size. The Kubernetes API server can dynamically provision the underlying storage resource in Azure if there is no existing resource to fulfill the claim based on the defined StorageClass. The pod definition includes the volume mount once the volume has been connected to the pod.

A PersistentVolume is *bound* to a PersistentVolumeClaim once an available storage resource has been assigned to the pod requesting it. There is a 1:1 mapping of persistent volumes to claims.

## Configure AKS Scaling

As you run applications in Azure Kubernetes Service (AKS), you may need to increase or decrease the amount of compute resources. As the number of application instances you need change, the number of underlying Kubernetes nodes may also need to change. You may also need to quickly provision a large number of additional application instances.



## Manually scale pods or nodes

You can manually scale replicas (pods) and nodes to test how your application responds to a change in available resources and state. Manually scaling resources also lets you define a set amount of resources to use to maintain a fixed cost, such as the number of nodes. To manually scale, you define the replica or node count, and the Kubernetes API schedules creating new pods or draining nodes.

## Horizontal pod autoscaler

Kubernetes uses the horizontal pod autoscaler (HPA) to monitor the resource demand and automatically scale the number of replicas. By default, the horizontal pod autoscaler checks the Metrics API every 30 seconds for any required changes in replica count. When changes are required, the number of replicas is increased or decreased accordingly. Horizontal pod autoscaler works with AKS clusters that have deployed the Metrics Server for Kubernetes 1.8+.

When you configure the horizontal pod autoscaler for a given deployment, you define the minimum and maximum number of replicas that can run. You also define the metric to monitor and base any scaling decisions on, such as CPU usage.

## Coldown of scaling events

As the horizontal pod autoscaler checks the Metrics API every 30 seconds, previous scale events may not have successfully completed before another check is made. This behavior could cause the horizontal pod autoscaler to change the number of replicas before the previous scale event has been able to receive application workload and the resource demands to adjust accordingly.

To minimize these race events, cooldown or delay values can be set. These values define how long the horizontal pod autoscaler must wait after a scale event before another scale event can be triggered. This behavior allows the new replica count to take effect and the Metrics API reflect the distributed workload. By default, the delay on scale up events is 3 minutes, and the delay on scale down events is 5 minutes.

You may need to tune these cooldown values. The default cooldown values may give the impression that the horizontal pod autoscaler isn't scaling the replica count quickly enough. For example, to more quickly increase the number of replicas in use, reduce the `--horizontal-pod-autoscaler-upscale-delay` when you create your horizontal pod autoscaler definitions using `kubectl`.

## Cluster autoscaler

To respond to changing pod demands, Kubernetes has a cluster autoscaler that adjusts the number of nodes based on the requested compute resources in the node pool. By default, the cluster autoscaler checks the API server every 10 seconds for any required changes in node count. If the cluster autoscaler determines that a change is required, the number of nodes in your AKS cluster is increased or decreased accordingly. The cluster autoscaler works with RBAC-enabled AKS clusters that run Kubernetes 1.10.x or higher.

Cluster autoscaler is typically used alongside the horizontal pod autoscaler. When combined, the horizontal pod autoscaler increases or decreases the number of pods based on application demand, and the cluster autoscaler adjusts the number of nodes as needed to run those additional pods accordingly.

## Scale up events

If a node does not have sufficient compute resources to run a requested pod, that pod cannot progress through the scheduling process. The pod cannot start unless other compute resources are available within the node pool.

When the cluster autoscaler notices pods that cannot be scheduled due to node pool resource constraints, the number of nodes within the node pool is increased to provide the extra compute resources. When those additional nodes are successfully deployed and available for use within the node pool, the pods are then scheduled to run on them.

If your application needs to scale rapidly, some pods may remain in a state waiting to be scheduled until the new nodes deployed by the cluster autoscaler can accept the scheduled pods. For applications that have high burst demands, you can scale with virtual nodes and Azure Container Instances.

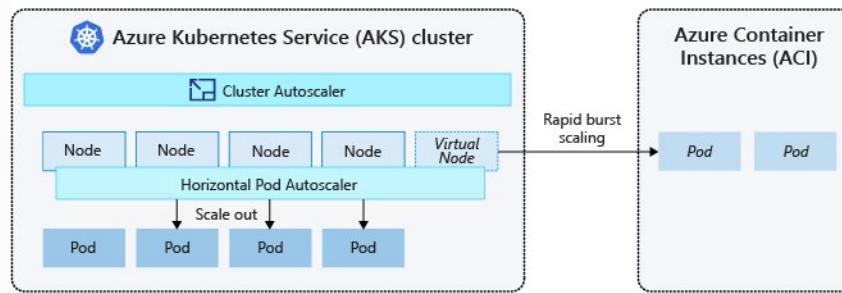
## Scale down events

The cluster autoscaler also monitors the pod scheduling status for nodes that have not recently received new scheduling requests. This scenario indicates that the node pool has more compute resources than are required, and that the number of nodes can be decreased.

A node that passes a threshold for no longer being needed for 10 minutes by default is scheduled for deletion. When this situation occurs, pods are scheduled to run on other nodes within the node pool, and the cluster autoscaler decreases the number of nodes.

Your applications may experience some disruption as pods are scheduled on different nodes when the cluster autoscaler decreases the number of nodes. To minimize disruption, avoid applications that use a single pod instance.

## Configure AKS Scaling to ACI



To rapidly scale your AKS cluster, you can integrate with Azure Container Instances (ACI). Kubernetes has built-in components to scale the replica and node count. However, if your application needs to rapidly scale, the horizontal pod autoscaler may schedule more pods than can be provided by the existing compute resources in the node pool. If configured, this scenario would then trigger the cluster autoscaler to deploy additional nodes in the node pool. It may take a few minutes for those nodes to successfully provision.

ACI lets you quickly deploy container instances without more infrastructure overhead. When you connect with AKS, ACI becomes a secured, logical extension of your AKS cluster. The Virtual Kubelet component is installed in your AKS cluster that presents ACI as a virtual Kubernetes node. Kubernetes can then schedule pods that run as ACI instances through virtual nodes, not as pods on VM nodes directly in your AKS cluster.

Your application requires no modification to use virtual nodes. Deployments can scale across AKS and ACI. There is no delay when the cluster autoscaler deploys new nodes in your AKS cluster.

Virtual nodes are deployed to another subnet in the same virtual network as your AKS cluster. This virtual network configuration allows the traffic between ACI and AKS to be secured. Like an AKS cluster, an ACI instance is a secure, logical compute resource that is isolated from other users.

## Demonstration - Deploy AKS

In this demonstration, we will deploy an Azure Kubernetes Service.

### Create a Kubernetes service

1. Sign-in to the [Azure portal](#)<sup>20</sup>.
2. Search for and select **Kubernetes services**, and then click **+ Add**.
3. On the Basics page, configure the following options and then select **Next: Scale**.
  - **Project details:** Select an Azure Subscription, then select or create an Azure Resource group, such as **myResourceGroup**.
  - **Cluster details:** Enter a Kubernetes cluster name, such as **myAKSCluster**. Select a Region, Kubernetes version, and DNS name prefix for the AKS cluster.
  - **Primary node pool:** Select a VM Node size for the AKS nodes. The VM size can't be changed once an AKS cluster has been deployed. - Select the number of nodes to deploy into the cluster. For this demonstration, set Node count to 1. Node count can be adjusted after the cluster has been deployed.
4. On the **Scale** page, review and keep the default options. At the bottom of the screen, click **Next: Authentication**.

<sup>20</sup> <http://portal.azure.com/>

5. On the **Authentication** page, configure the following options:
  - Create a new service principal by leaving the Service Principal field with (new) default service principal. Or you can choose Configure service principal to use an existing one. If you use an existing one, you will need to provide the SPN client ID and secret.
  - Enable the option for Kubernetes role-based access controls (RBAC). This will provide more fine-grained control over access to the Kubernetes resources deployed in your AKS cluster.
6. By default, **Basic networking** is used, and Azure Monitor for containers is enabled. Click **Review + create** and then **Create** when validation completes.
7. It takes a few minutes to create the AKS cluster.

### Connect to the cluster

1. To manage a Kubernetes cluster, you use **kubectl**, the Kubernetes command-line client. The kubectl client is pre-installed in the Azure Cloud Shell.

2. Open the **Cloud Shell**, select the **Bash** shell.

3. Connect to the cluster, download your credentials, and configure the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

4. Verify the connection to your cluster and return a list of the cluster nodes. Make sure that the status of the nodes is Ready.

```
kubectl get nodes
```

### Run the application

**Note:** You will need a Kubernetes manifest file for the next steps. Navigate to the **Quickstart - Deploy an AKS cluster in the portal**<sup>21</sup>.

1. In the cloud shell, use either the **nano azure-vote.yaml** or **vi azure-vote.yaml** command to create a file named azure-vote.yaml.
2. Copy the YAML definition from the Quickstart page. Be sure to save your changes.
3. Deploy the application.

```
kubectl apply -f azure-vote.yaml
```

4. Ensure there are no errors and the output shows the Deployments and Services created successfully.

### Test the application

1. When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete.
2. Continue in the cloud shell to monitor the progress of the deployment.

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

3. Wait until the EXTERNAL-IP address changes from pending to an actual public IP address. Use Ctrl + C to break out of the command.
4. To see the Azure Vote app in action, open a web browser to the external IP address of your service.

<sup>21</sup> <https://docs.microsoft.com/azure/aks/kubernetes-walkthrough-portal#run-the-application>

5. Return to the Azure portal and your myAKSCluster resource.
6. Under **Monitoring** choose **Insights**. Review the available information.
7. As you have time review other areas of the cluster.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*You decide to move all your services to Azure Kubernetes service. Which of the following components will contribute to your monthly Azure charge? Select one.*

- Azure managed node
- Pods
- Customer node virtual machines

### Multiple choice

*Which of the following is the Kubernetes agent that processes the orchestration requests and schedules running the requested containers? Select one.*

- controller
- kube-proxy
- kubelet

### Multiple choice

*You are configuring networking for the Azure Kubernetes service. Which of the following maps incoming direct traffic to the pods? Select one.*

- AKS node
- ClusterIP
- NodePort

## Summary and Resources

### Summary

Azure Kubernetes Services (AKS) is recommended when you need full container organization. AKS includes discovery across multiple containers, automatic scaling, and coordinated application upgrades.

You should now be able to:

- Identify AKS components including pods, clusters, and nodes.
- Configure network connections for AKS.

- 
- Configure storage options for AKS.
  - Implement security options for AKS.
  - Scale AKS including adding Azure Container Instances.

## Learn more

You can learn more by reviewing the following.

- **Azure Kubernetes Service documentation<sup>22</sup>**
- **Learn - Introduction to Kubernetes<sup>23</sup>**

---

<sup>22</sup> <https://docs.microsoft.com/azure/aks/intro-kubernetes>

<sup>23</sup> <https://docs.microsoft.com/learn/modules/intro-to-kubernetes/>

# Module 09 Lab

## Lab 09a - Implement Web Apps

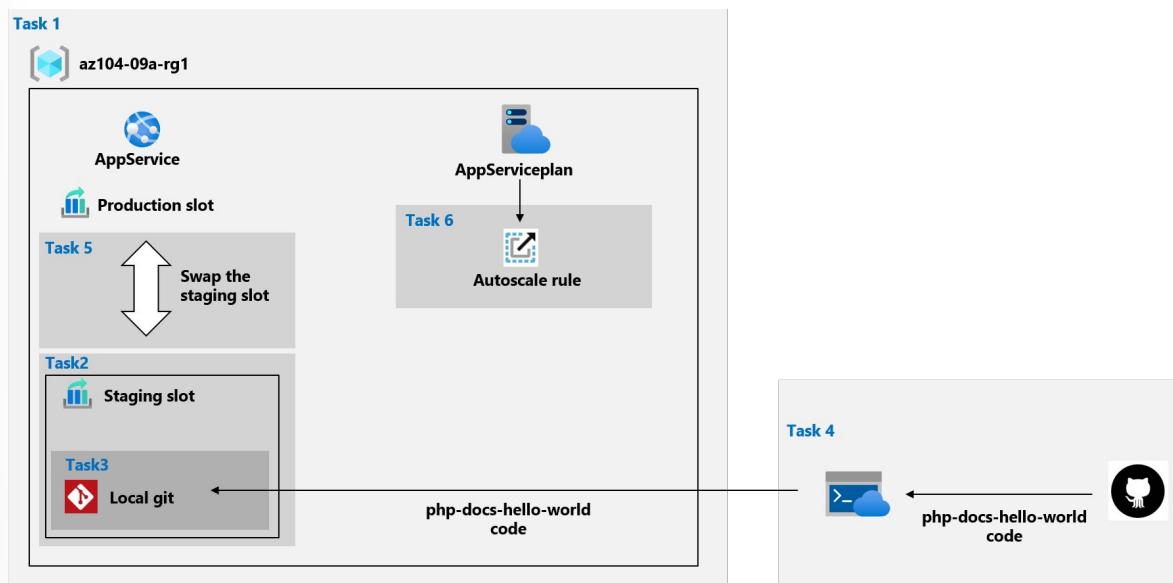
### Lab scenario

You need to evaluate the use of Azure Web apps for hosting Contoso's web sites, hosted currently in the company's on-premises data centers. The web sites are running on Windows servers using PHP runtime stack. You also need to determine how you can implement DevOps practices by leveraging Azure web apps deployment slots.

### Objectives

In this lab, you will:

- Task 1: Create an Azure web app.
- Task 2: Create a staging deployment slot.
- Task 3: Configure web app deployment settings.
- Task 4: Deploy code to the staging deployment slot.
- Task 5: Swap the staging slots.
- Task 6: Configure and test autoscaling of the Azure web app.



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Lab 09b - Implement Azure Container Instances

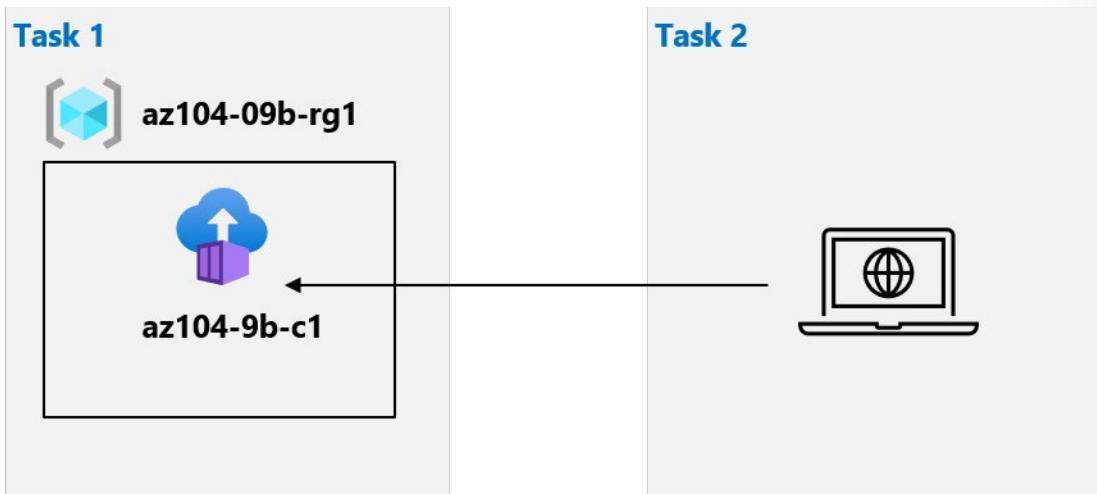
## Lab scenario

Contoso wants to find a new platform for its virtualized workloads. You identified a number of container images that can be leveraged to accomplish this objective. Since you want to minimize container management, you plan to evaluate the use of Azure Container Instances for deployment of Docker images.

## Objectives

In this lab, you will:

- Task 1: Deploy a Docker image by using the Azure Container Instance
- Task 2: Review the functionality of the Azure Container Instance



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Lab 09c - Implement Azure Kubernetes Service

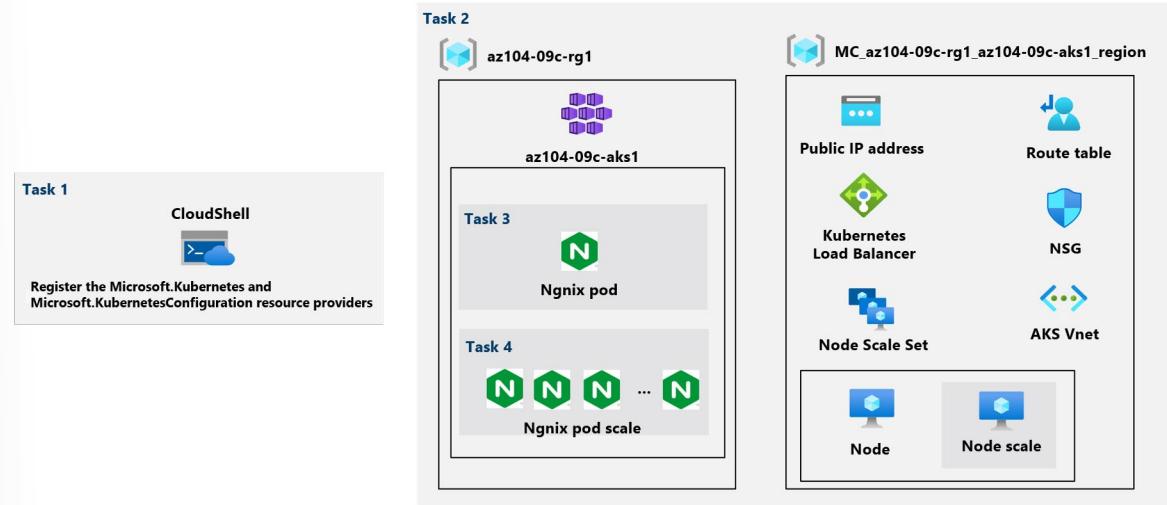
## Lab scenario

Contoso has a number of multi-tier applications that are not suitable to run by using Azure Container Instances. In order to determine whether they can be run as containerized workloads, you want to evaluate using Kubernetes as the container orchestrator. To further minimize management overhead, you want to test Azure Kubernetes Service, including its simplified deployment experience and scaling capabilities.

## Objectives

In this lab, you will:

- Task 1: Deploy an Azure Kubernetes Service cluster
- Task 2: Deploy pods into the Azure Kubernetes Service cluster
- Task 3: Scale containerized workloads in the Azure Kubernetes service cluster



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Answers

## Multiple choice

You are administering a production web app. The app requires scaling to five instances, 40GB of storage, and a custom domain name. Which App Service Plan should you select? Select one.

- Basic
- Standard
- Premium

*Explanation*

*Standard. The Standard App Service Plan meets the requirements at the least cost.*

## Multiple choice

Which of the following is not true of the App Service plan? Select one.

- The App Service plan is a set of virtual server resources that run App Service apps.
- The App Service plan determines the performance characteristics of the virtual servers.
- The App Service plan hosts a single App Service web app.

*Explanation*

*The App Service plan hosts a single App Service web app. A single App Service plan can host multiple App Service web apps. In most cases, the number of apps you can run on a single plan will be limited by the performance characteristics of the apps and the resource limitations of the plan.*

## Multiple choice

To get more CPU, memory, or disk space you should? Select one.

- Scale up
- Scale out

*Explanation*

*Scale up. Scale up gives you more CPU, memory, disk space, and more. You scale up by changing the pricing tier of the App Service plan that your app belongs to.*

## Multiple choice

To configure an autoscale trigger based on average response time, you should select ... Select one.

- Metric-based
- Time-based
- User-based

*Explanation*

*Metric-based. Metric-based rules measure application load and add or remove VMs based on that load. For example, do this action when CPU usage is above 50%. Examples of metrics are CPU time, Average response time, and Requests.*

**Multiple choice**

Which of the following settings is not swapped when you swap an app? Select one.

- Framework version
- Public certificates
- Scale settings

*Explanation*

*Scale settings. Scale settings are not swapped.*

**Multiple choice**

Which of the following is not true about App Service backups? Select one.

- Incremental backups are the default.
- You can configure backups manually or on a schedule.
- You can exclude files and folders you do not want in the backup.

*Explanation*

*Incremental backups are the default. Full backups are the default.*

**Multiple choice**

What method does Microsoft Azure App Service use to obtain credentials for users attempting to access an app? Select one.

- Credentials that are stored in the browser.
- Pass-through authentication.
- Redirection to a provider endpoint.

*Explanation*

*Redirection to a provider endpoint. Microsoft Azure App Service apps redirect requests to an endpoint that signs in users for that provider. The App Service can automatically direct all unauthenticated users to the endpoint that signs in users. Course: Module 4*

**Multiple choice**

Which of the following isn't a valid automated deployment source? Select one.

- Azure DevOps
- GitHub
- SharePoint

*Explanation*

*SharePoint. Azure currently supports Azure DevOps, GitHub, Bitbucket, OneDrive, Dropbox, and external Git repositories.*

**Multiple choice**

Which of the following is not true about container groups?

- Are scheduled on multiple host machines.
- Consists of two containers.
- Exposes a single public IP address, with one exposed port.

*Explanation*

*Are scheduled on a multiple host machines is not correct. A container group is scheduled on a single host machine.*

**Multiple choice**

Which of the following is a reason to select virtual machines over containers?

- Virtual machines provide complete isolation from the host operating system and other VMs.
- Virtual machines run the user mode portion of an operating system and can be tailored to contain just the needed services for your app.
- Virtual machines use Azure Disks for local storage for a single node.

*Explanation*

*That's correct. Containers only provide lightweight isolation from the host and other containers but doesn't provide as strong a security boundary as a virtual machine.*

**Multiple choice**

All the following are true about Azure Container Instances, except?

- You are billed only when the container is in use.
- Containers launch in seconds.
- Container storage uses Azure blobs.

*Explanation*

*ACI uses persistent storage. You can mount Azure Files shares directly to a container to retrieve and persist state.*

**Multiple choice**

You decide to move all your services to Azure Kubernetes service. Which of the following components will contribute to your monthly Azure charge? Select one.

- Azure managed node
- Pods
- Customer node virtual machines

*Explanation*

*Customer node virtual machines. You only pay for the virtual machines instances, storage, and networking resources consumed by your Kubernetes cluster.*

**Multiple choice**

Which of the following is the Kubernetes agent that processes the orchestration requests and schedules running the requested containers? Select one.

- controller
- kube-proxy
- kubelet

*Explanation*

*kubelet. The kubelet process the orchestration requests and schedules running the requested containers.*

**Multiple choice**

You are configuring networking for the Azure Kubernetes service. Which of the following maps incoming direct traffic to the pods? Select one.

- AKS node
- ClusterIP
- NodePort

*Explanation*

*NodePort. NodePort maps incoming direct traffic to the pods.*

# Module 10 Administer Data Protection

## Configure File and Folder Backups

### Introduction

#### Scenario

Your company stores critical compliance information on Azure file shares. You must ensure this content can be recovered if there's data loss or corruption.

You must configure backup and restore policies that meet your company's regulatory needs.

#### Skills measured

Backup and recovery are part of **Exam AZ-104: Microsoft Azure Administrator<sup>1</sup>**.

Monitor and back up Azure resources (10–15%)

Implement backup and recovery

- Create a Recovery Services vault.
- Create and configure backup policy.
- Perform backup and restore operations by using Azure Backup.
- Configure and review backup reports.

#### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for Azure Backup.
- Configure Recovery Services Vault backup options.

<sup>1</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

- Implement on-premises file and folder backup.
- Configure the Microsoft Azure Recovery Services Agent.

## Prerequisites

None.

# Describe Azure Backup Benefits

**Azure Backup** is the Azure-based service you can use to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive.

Azure Backup offers multiple components that you download and deploy on the appropriate computer, server, or in the cloud. The component, or agent, that you deploy depends on what you want to protect. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Recovery Services vault in Azure.

## Key benefits

- **Offload on-premises backup.** Azure Backup offers a simple solution for backing up your on-premises resources to the cloud. Get short and long-term backup without the need to deploy complex on-premises backup solutions.
- **Back up Azure IaaS VMs.** Azure Backup provides independent and isolated backups to guard against accidental destruction of original data. Backups are stored in a Recovery Services vault with built-in management of recovery points. Configuration and scalability is simple, backups are optimized, and you can easily restore as needed.
- **Get unlimited data transfer.** Azure Backup does not limit the amount of inbound or outbound data you transfer, or charge for the data that is transferred. Outbound data refers to data transferred from a Recovery Services vault during a restore operation. If you perform an offline initial backup using the Azure Import/Export service to import large amounts of data, there is a cost associated with inbound data.
- **Keep data secure.** Data encryption allows for secure transmission and storage of your data in the public cloud. You store the encryption passphrase locally, and it is never transmitted or stored in Azure. If it is necessary to restore any of the data, only you have encryption passphrase, or key.
- **Get app-consistent backups.** An application-consistent backup means a recovery point has all required data to restore the backup copy. Azure Backup provides application-consistent backups, which ensure additional fixes are not required to restore the data. Restoring application-consistent data reduces the restoration time, allowing you to quickly return to a running state.
- **Retain short and long-term data.** You can use Recovery Services vaults for short-term and long-term data retention. Azure doesn't limit the length of time data can remain in a Recovery Services vault. You can keep it for as long as you like. Azure Backup has a limit of 9999 recovery points per protected instance.
- **Automatic storage management.** Hybrid environments often require heterogeneous storage - some on-premises and some in the cloud. With Azure Backup, there is no cost for using on-premises storage devices. Azure Backup automatically allocates and manages backup storage, and it uses a pay-as-you-use model, so that you only pay for the storage you consume.

- **Multiple storage options.** Azure Backup offers two types of replication to keep your storage/data highly available.
  - Locally redundant storage (LRS) replicates your data three times (it creates three copies of your data) in a storage scale unit in a datacenter. All copies of the data exist within the same region. LRS is a low-cost option for protecting your data from local hardware failures.
  - Geo-redundant storage (GRS) is the default and recommended replication option. GRS replicates your data to a secondary region (hundreds of miles away from the primary location of the source data). GRS costs more than LRS, but GRS provides a higher level of durability for your data, even if there is a regional outage.

**Note:** What are some of the reasons your organization might choose Azure Backup? Is your organization using Azure Backup?

## Implement Azure Backup Center

Backup Center provides a single unified management experience in Azure for enterprises to govern, monitor, operate, and analyze backups at scale. As such, it's consistent with Azure's native management experiences.

The screenshot shows the Azure Backup Center interface. The left sidebar includes links for Overview, Getting started, Community, Manage (Backup instances, Backup policies, Vaults), Monitoring + reporting, Backup jobs, Backup reports, Policy and compliance (Backup compliance, Azure policies for backup, Protectable datasources), Support + troubleshooting, and New support request. The main content area is titled 'Datasource type: Azure Virtual machines' and shows 'Overview of Jobs and Backup instances'. It displays 'Jobs (last 24 Hours)' with a table showing Scheduled backup (0 Failed, 0 In progress, 2 Completed), On-demand backup (0 Failed, 0 In progress, 0 Completed), and Restore (0 Failed, 0 In progress, 0 Completed). Below this is a 'Backup instances' section for 'Azure Virtual machines' showing 2 Protection configured, 0 Protection stopped, and 0 Soft deleted. It also shows 0 out of 2 Backup instances with the underlying datasource not found.

Some of the key benefits of Backup Center include:

- **Single pane of glass to manage backups.** Backup Center is designed to function well across a large and distributed Azure environment. You can use Backup Center to efficiently manage backups spanning multiple workload types, vaults, subscriptions, regions, and tenants.
- **Datasource-centric management.** Backup Center provides views and filters that are centered on the datasources that you're backing up. Datasources like VMs and databases. This feature lets a resource owner or a backup admin to administer backup items across different vaults. The admin can also filter views by datasource-specific properties. These properties include datasource subscription, datasource resource group, and datasource tags.
- **Connected experiences.** Backup Center provides native integrations to existing Azure services that enable management at scale. For example, Backup Center uses the Azure Policy experience to help

you govern your backups. It uses Azure workbooks and Azure Monitor Logs to help you view detailed reports on backups. So you don't need to learn any new principles to use the varied features that Backup Center offers. You can also discover community resources from the Backup Center.

## Supported scenarios

Backup Center is currently supported for Azure VM backup, SQL in Azure VM backup, SAP HANA in Azure VM backup, Azure Files backup, Azure Blobs backup, Azure-managed disks backup, and Azure Database for PostgreSQL Server backup.

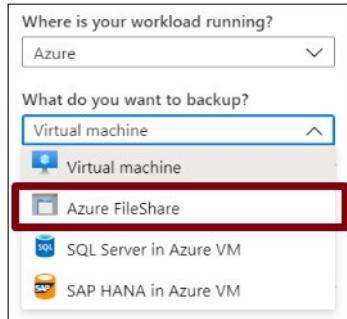
## Get started

To get started with using Backup Center, search for Backup Center in the Azure portal and navigate to the Backup Center dashboard.

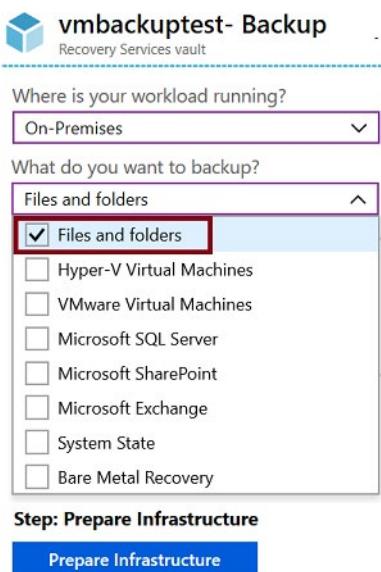
## Setup Recovery Service Vault Backup Options

The **Recovery Services vault** is a storage entity in Azure that stores data.

Recovery Services vaults store backup data for various Azure services such as IaaS VMs (Linux or Windows) and Azure SQL databases. Recovery Services vaults support System Center DPM, Windows Server, Azure Backup Server, and other services. Recovery Services vaults make it easy to organize your backup data, while minimizing management overhead.



- The Recovery Services vault can be used to back up Azure file shares.



- The Recovery Services vault can also be used to back up on-premises files and folders.

**Note:** Within an Azure subscription, you can create up to 25 Recovery Services vaults per region.

## Demonstration - Backup Azure File Shares

In this demonstration, we will explore backing up a file share in the Azure portal.

### Configure a storage account with file share

**Note:** If you already have a storage account and file share, you can skip this step.

1. In the Azure portal, search for **Storage Accounts**.
2. **Add** a new storage account.
3. Provide the storage account information (your choice).
4. Click **Review + create** and then **Create**.
5. Access your storage account, and click **Files**.
6. Click **+ File share** and give your new file share a **Name** and a **Quota**.
7. After your file share is created **Upload a file**.

### Create a Recovery Services vault

1. In the Azure portal, type Recovery Services and click **Recovery Services vaults**.
2. Click **Add**.
3. Provide a **Name**, **Subscription**, **Resource group**, and **Location**.
4. Your new vault should be in the same location as the file share.
5. Click **Create**. It can take several minutes for the Recovery Services vault to be created. Monitor the status notifications in the upper right-hand area of the portal. Once your vault is created, it appears in the list of Recovery Services vaults.
6. If after several minutes the vault is not added, click **Refresh**.

### Configure file share backup

1. Open your recovery services vault.
2. Click **Backup** and create a new backup instance.
3. From the **Where is your workload running?** drop-down menu, select **Azure**.
4. From the **What do you want to backup?** menu, select **Azure FileShare**.
5. Click **Backup**.
6. From the list of Storage accounts, **select a storage account**, and click **OK**. Azure searches the storage account for files shares that can be backed up. If you recently added your file shares, allow a little time for the file shares to appear.
7. From the File Shares list, **select one or more of the file shares** you want to backup, and click **OK**.
8. On the Backup Policy page, choose **Create New backup policy** and provide Name, Schedule, and Retention information. Click **OK**.
9. When you are finished configuring the backup click **Enable backup**.

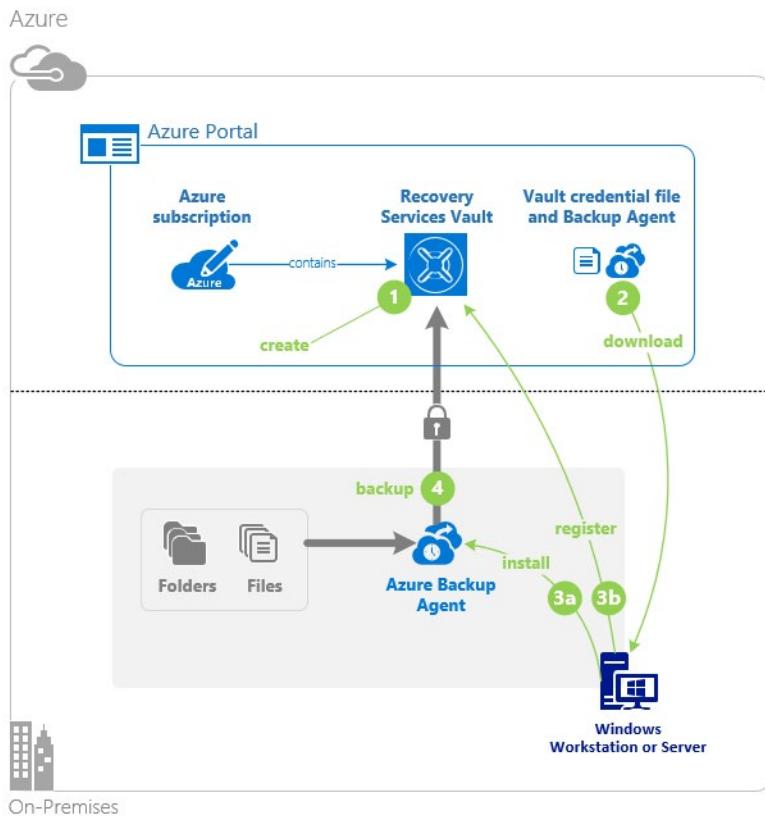
### Verify the file share backup

1. Explore the **Backup items** blade. There is information on backed up items and replicated items.
2. Explore the **Backup policies** blade. You can add or delete backup policies.
3. Explore the **Backup jobs** blade. Here you can review the status of your backup jobs.

## Configure On-Premises File and Folder Backups

There are several steps to configuring Azure backup of on-premises files and folders.

**Note:** The Backup agent can be deployed on any Windows Server VM or physical machine.



## Manage the Azure Recovery Services Agent

Azure Backup for files and folders relies on the Microsoft Azure Recovery Services (MARS) agent to be installed on the Window client or server.

The screenshot shows the Microsoft Azure Backup interface. At the top, it says "Microsoft Azure Backup". Below that, there's a message: "Microsoft Azure Backup supports scheduled backups of files and folders to an cloud storage account." A warning icon indicates that backups have not been configured for this server. It suggests clicking "Schedule Backup" in the Actions pane to configure them. It also mentions that you can configure notifications from the Alerts blade to receive email alerts for backup failures. There's a link to "Learn More".

The main area shows a table titled "Jobs (Activity in the past 7 days, double click on the message to see details)". It has two tabs: "Jobs" (selected) and "Alerts". The "Jobs" tab displays three rows of data:

| Status | Time              | Message  | Description    |
|--------|-------------------|----------|----------------|
| ✓      | 2/28/2019 6:48 AM | Recovery | Job completed. |
| ✓      | 2/28/2019 6:45 AM | Recovery | Job completed. |
| ✓      | 2/28/2019 6:41 AM | Backup   | Job completed. |

To the right of the interface is a vertical "Actions" menu:

- Backup
  - Register Server
  - Schedule Backup
  - Recover Data
- Change Properties
- Open Portal
- Privacy & Cookies
- View
- Help

The MARS agent is a full featured agent that has many features.

- Back up files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure).
- No separate backup server required.
- Not application aware; file, folder, and volume-level restore only.
- Back up and restore content.

## Demonstration - Backup Files and Folders

In this demonstration, we will step through the process to backup and restore files and folders from Windows to Azure.

**Note:** This demonstration assumes you have not used the Azure Backup Agent before and need a complete installation.

### Create a Recovery Services vault

1. In the Azure portal, type Recovery Services and click **Recovery Services vaults**.
2. Click **Add**.
3. Provide a **Name**, **Subscription**, **Resource group**, and **Location**.
4. Click **Create**. It can take several minutes for the Recovery Services vault to be created. Monitor the status notifications in the upper right-hand area of the portal. Once your vault is created, it appears in the list of Recovery Services vaults.
5. If after several minutes you don't observe your vault, click **Refresh**.

### Configure the vault

1. For your recovery services vault, click **Backup**.
2. From the **Where is your workload running?** drop-down menu, select **On-premises**.
3. From the **What do you want to backup?** menu, select **Files and folders**. Notice your other choices.
4. Click **Prepare infrastructure**.
5. Click **Download Agent for Windows Server or Windows Client**. A pop-up menu prompts you to run or **save** MARSagentinstaller.exe.
6. By default, the MARSagentinstaller.exe file is saved to your **Downloads** folder. When the installer completes, a pop-up asking if you want to run the installer, or open the folder. You **don't need** to install the agent yet. You can install the agent after you have downloaded the vault credentials.

7. Return to your recovery services vault, check the box **Already downloaded or using the latest recovery services agent.**
8. Click **Download**. After the vault credentials finish downloading, a pop-up asking if you want to open or **save** the credentials. Click **Save**. If you accidentally click **Open**, let the dialog that attempts to open the vault credentials, fail. You cannot open the vault credentials. Proceed to the next step. The vault credentials are in the **Downloads** folder.

**Note:** You must have the latest version of the MARS agent. Versions of the agent below 2.0.9083.0 must be upgraded by uninstalling and reinstalling the agent.

### Install and register the agent

1. Locate and double-click the **MARSagentinstaller.exe** from the **Downloads** folder (or other saved location). The installer provides a series of messages as it extracts, installs, and registers the Recovery Services agent.
2. To complete the wizard, you need to:
  - Choose a location for the installation and cache folder.
  - Provide your proxy server info if you use a proxy server to connect to the internet.
  - Provide your user name and password details if you use an authenticated proxy.
  - If prompted, install any missing software.
  - Provide the downloaded vault credentials
  - Enter and save the encryption passphrase in a secure location.
3. Wait for the server registration to complete. This could take a couple of minutes.
4. The agent is now installed and your machine is registered to the vault. You're ready to configure and schedule your backup.

### Create the backup policy

1. Open the **Microsoft Azure Recovery Services** agent. You can find it by searching your machine for Microsoft Azure Recovery Services.
2. If this is the first time you are using the agent there will be a **Warning** to create a backup policy. The backup policy is the schedule when recovery points are taken, and the length of time the recovery points are retained.
3. Click **Schedule Backup** to launch the Schedule Backup Wizard.
  - Read the **Getting Started** page.
  - **Add items** to include files and folders that you want to protect. Select just a few sample files. Notice you can exclude files from the backup.
  - Specify the **backup schedule**. You can schedule daily (at a maximum rate of three times per day) or weekly backups.
  - Select your **retention policy** settings. The retention policy specifies the duration for which the backup is stored. Rather than just specifying a "flat policy" for all backup points, you can specify different retention policies based on when the backup occurs. You can modify the daily, weekly, monthly, and yearly retention policies to meet your needs.
  - Choose your **initial backup type page** as **Automatically**. Notice there is a choice for offline backup.
  - **Confirm** your choices and **Finish** the wizard.

### Backup files and folders

1. Click **Back Up Now** to complete the initial sending over the network.
2. In the wizard, confirm your settings, and then click **Back Up**.
3. You may **Close** the wizard. It will continue to run in the background.
4. The **Status** of your backup will show on the first page of the agent.
5. You can **View Details** for more information.

### Explore the recover settings

1. Click **Recover data**.
2. Walkthrough the wizard making selections based on your backup settings.
3. Notice your choices to restore from the current server or another server.
4. Notice you can backup individual files and folders or an entire volume.
5. Select a volume and **Mount** the drive. This can take a couple of minutes.
6. Verify the mounted volume can be accessed in **File Explorer** and that your backup files are available.
7. **Unmount** the drive.

### Explore the backup properties

1. Click **Change Properties**.
2. Explore the different tabs.
3. On the **Encryption** tab you can change the passphrase.
4. On the **Proxy Configuration** tab you can add proxy information.
5. On the **Throttling** tab you can enable internet bandwidth usage throttling. Throttling controls how network bandwidth is used during data transfer. This control can be helpful if you need to back up data during work hours but do not want the backup process to interfere with other Internet traffic. Throttling applies to back up and restore activities.

### Delete your backup schedule

1. Click **Schedule Backup**.
2. In the wizard, select **Stop using this backup schedule and delete all the stored backups**.
3. Verify your choices and click **Finish**.
4. You will be prompted for a recovery services vault security pin.
5. In the Azure portal locate your recovery services vault.
6. Select **Properties** and then Security PIN **Generate**.
7. Copy the PIN into the Backup agent to finish deleting the schedule.

## Knowledge check

Choose the best response for each question.

## Multiple choice

You need to backup files and folders to Azure. Which of these steps would you do first?

- Download, install and register the backup agent.
- Back up files and folders.
- Create a recovery services vault.

## Multiple choice

You are responsible for implementing server workload backups. You need to implement on-premises backups to an Azure Recovery Vault service. What should you do? Select one.

- Download and install the MARS agent, and then register the server by installing the vault credentials.
- Just download and install the MARS agent.
- Don't do anything. Windows Servers contain the required agent for inclusion in the Recovery Vault service.

## Multiple choice

You have created the Recovery Vault service. Now you decide to change the storage replication type to locally redundant. In which situations can Larissa change the storage replication type?

- You can change this setting at any time.
- You can change this setting, but only before a Recovery Vault service starts providing protection for items.
- You cannot change this setting at any time.

## Summary and Resources

### Summary

Azure file share backup is a native, cloud based backup solution that protects your data in the cloud. Azure Backup eliminates additional maintenance overhead involved in on-premises backup solutions. The Azure Backup service smoothly integrates with Azure File Sync. You can centralize your file share data as well as your backups.

You should now be able to:

- Identify features and usage cases for Azure Backup.
- Configure Recovery Services Vault backup options.
- Implement on-premises file and folder backup.
- Configure the Microsoft Azure Recovery Services Agent.

## Learn more

You can learn more by reviewing the following.

- **What is the Azure Backup service?**<sup>2</sup> <https://docs.microsoft.com/azure/backup/backup-overview>
- **About Azure file share backup**<sup>3</sup> <https://docs.microsoft.com/azure/backup/azure-file-share-backup-overview>
- **Learn - Implement hybrid backup and recovery with Windows Server IaaS**<sup>4</sup> <https://docs.microsoft.com/learn/modules/implement-hybrid-backup-recovery-windows-server-iaas/>

---

<sup>2</sup> <https://docs.microsoft.com/azure/backup/backup-overview>

<sup>3</sup> <https://docs.microsoft.com/azure/backup/azure-file-share-backup-overview>

<sup>4</sup> <https://docs.microsoft.com/learn/modules/implement-hybrid-backup-recovery-windows-server-iaas/>

# Configure Virtual Machine Backups

## Introduction

### Scenario

Your company has several critical virtual machine workloads running on Azure. You must ensure the company can recover these virtual machines if there's data loss or corruption.

You use the built-in capabilities of Azure Backup to help protect these virtual machines. Azure Backup is used for both Azure and on-premises workloads.

### Skills measured

Backup and recovery are part of **Exam AZ-104: Microsoft Azure Administrator<sup>5</sup>**.

Monitor and back up Azure resources (10–15%)

Implement backup and recovery

- Create a Recovery Services vault.
- Create and configure backup policy.
- Perform backup and restore operations by using Azure Backup.
- Perform site-to-site recovery by using Azure Site Recovery.
- Configure and review backup reports.

### Learning objectives

In this module, you will learn how to:

- Identify features and usage cases for different Azure backup methods.
- Configure virtual machine snapshots and backup options.
- Implement virtual machine backup and restore, including soft delete.
- Compare the Azure Backup (MARS) agent to the Azure Backup Server (MABS).
- Perform site-to-site recovery by using Azure Site Recovery.

### Prerequisites

None.

## Protect Virtual Machine Data

You can protect your data by taking backups at regular intervals. There are several backup options available for VMs, depending on your use-case.

<sup>5</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

[Solutions](#)[Azure Backup](#)[Azure Site Recovery](#)

## Azure Backup

For backing up Azure VMs running production workloads, use Azure Backup. Azure Backup supports application-consistent backups for both Windows and Linux VMs. Azure Backup creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the whole VM or just specific files.

## Azure Site Recovery

Azure Site Recovery protects your VMs from a major disaster scenario when a whole region experiences an outage due to major natural disaster or widespread service interruption. You can configure Azure Site Recovery for your VMs so that you can recover your application with a single click in matter of minutes. You can replicate to an Azure region of your choice.

## Managed disk snapshots

In development and test environments, snapshots provide a quick and simple option for backing up VMs that use Managed Disks. A managed disk snapshot is a read-only full copy of a managed disk that is stored as a standard managed disk by default. With snapshots, you can back up your managed disks at any point in time. These snapshots exist independent of the source disk and can be used to create new managed disks. They are billed based on the used size. For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GiB and actual used data size of 10 GiB, that snapshot is billed only for the used data size of 10 GiB.

## Images

Managed disks also support creating a managed custom image. You can create an image from your custom VHD in a storage account or directly from a generalized (sysprepped) VM. This process captures a single image. This image contains all managed disks associated with a VM, including both the OS and data disks. This managed custom image enables creating hundreds of VMs using your custom image without the need to copy or manage any storage accounts.

## Images versus snapshots

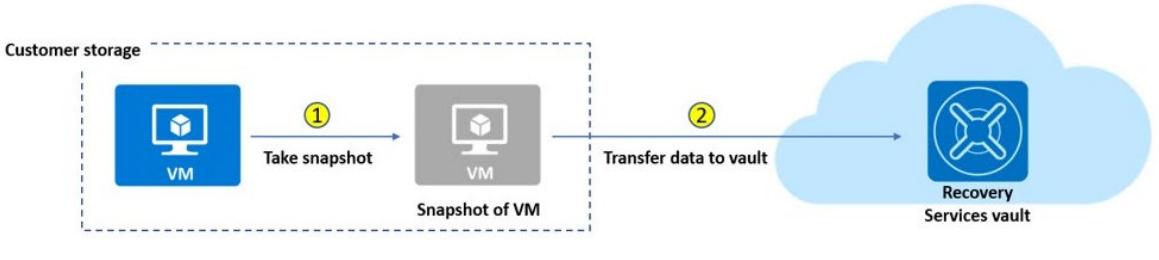
It's important to understand the difference between images and snapshots. With managed disks, you can take an image of a generalized VM that has been deallocated. This image includes all of the disks attached to the VM. You can use this image to create a VM, and it includes all of the disks.

- A snapshot is a copy of a disk at the point in time the snapshot is taken. It applies only to one disk. If you have a VM that has one disk (the OS disk), you can take a snapshot or an image of it and create a VM from either the snapshot or the image.
- A snapshot doesn't have awareness of any disk except the one it contains. This makes it problematic to use in scenarios that require the coordination of multiple disks, such as striping. Snapshots would need to be able to coordinate with each other and this is currently not supported.

**Note:** Have you tried any of these backup methods? Do you have a backup plan?

## Create Virtual Machine Snapshots

An Azure backup job consists of two phases. First, a virtual machine snapshot is taken. Second, the virtual machine snapshot is transferred to the Azure Recovery Services vault.



A recovery point is considered created only after both steps are completed. As a part of the upgrade, a recovery point is created as soon as the snapshot is finished. This recovery point is used to perform a restore. You can identify the recovery point in the Azure portal by using “snapshot” as the recovery point type. After the snapshot is transferred to the vault, the recovery point type changes to “snapshot and vault”.

## Capabilities and considerations

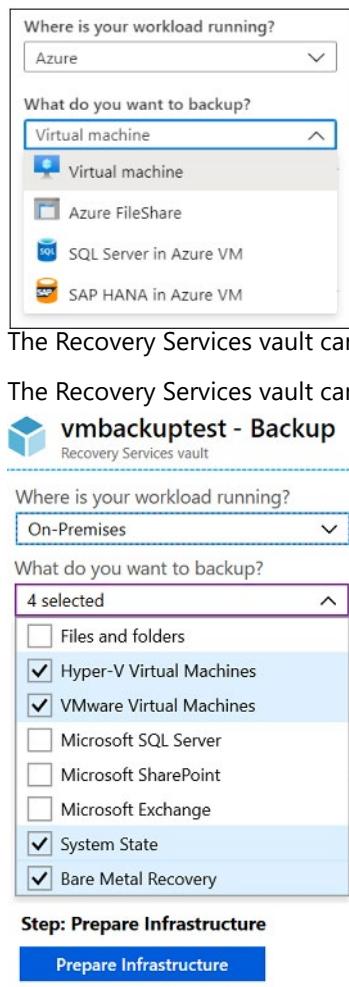
- Ability to use snapshots taken as part of a backup job that is available for recovery without waiting for data transfer to the vault to finish.
- Reduces backup and restore times by retaining snapshots locally, for two days by default. This default snapshot retention value is configurable to any value between 1 to 5 days.
- Supports disk sizes up to 32 TB. Resizing of disks is not recommended by Azure Backup.
- Supports Standard SSD disks along with Standard HDD disks and Premium SSD disks.
- Incremental snapshots are stored as page blobs. All the users using unmanaged disks are charged for the snapshots stored in their local storage account. Since the restore point collections used by Managed VM backups use blob snapshots at the underlying storage level, for managed disks you will see costs corresponding to blob snapshot pricing and they are incremental.
- For premium storage accounts, the snapshots taken for instant recovery points count towards the 10-TB limit of allocated space.
- You get an ability to configure the snapshot retention based on the restore needs. Depending on the requirement, you can set the snapshot retention to a minimum of one day in the backup policy blade as explained below. This will help you save cost for snapshot retention if you don't perform restores frequently.
- It is a one directional upgrade, once upgraded to Instant restore, you cannot go back.

**Note:** By default, snapshots are retained for two days. This feature allows restore operation from these snapshots thereby cutting down the restore times. It reduces the time that is required to transform and copy data back from the vault.

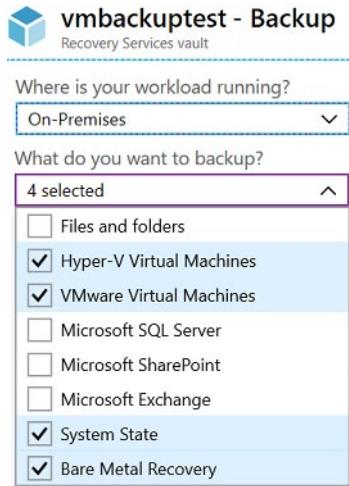
## Setup Recovery Services Vault Backup Options

**Recovery Services vault** is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services such as IaaS VMs (Linux or

Windows) and Azure SQL databases. Recovery Services vaults support System Center DPM, Windows Server, Azure Backup Server, and more. Recovery Services vaults make it easy to organize your backup data, while minimizing management overhead.



- The Recovery Services vault can be used to backup Azure virtual machines.
- The Recovery Services vault can be used to backup on-premises virtual machines including: Hyper-V,



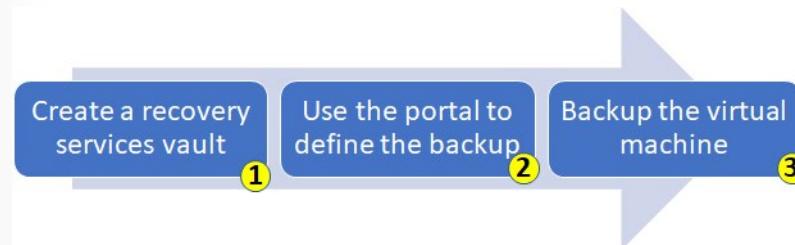
#### Step: Prepare Infrastructure

[Prepare Infrastructure](#)

VMware, System State, and Bare Metal Recovery.

## Backup Virtual Machines

Backing up Azure virtual machines using Azure Backup is easy and follows a simple process.



1. **Create a recovery services vault.** To back up your files and folders, you need to create a Recovery Services vault in the region where you want to store the data. You also need to determine how you want your storage replicated, either geo-redundant (default) or locally redundant. By default, your vault has geo-redundant storage. If you are using Azure as a primary backup storage endpoint, use

the default geo-redundant storage. If you are using Azure as a non-primary backup storage endpoint, then choose locally redundant storage, which will reduce the cost of storing data in Azure.

2. **Use the Portal to define the backup.** Protect your data by taking snapshots of your data at defined intervals. These snapshots are known as recovery points, and they are stored in recovery services vaults. If or when it is necessary to repair or rebuild a VM, you can restore the VM from any of the saved recovery points. A backup policy defines a matrix of when the data snapshots are taken, and how long those snapshots are retained. When defining a policy for backing up a VM, you can trigger a backup job once a day.
3. **Backup the virtual machine.** The Azure VM Agent must be installed on the Azure virtual machine for the Backup extension to work. However, if your VM was created from the Azure gallery, then the VM Agent is already present on the virtual machine. VMs that are migrated from on-premises data centers would not have the VM Agent installed. In such a case, the VM Agent needs to be installed.

## Restore Virtual Machines

Once your virtual machine snapshots are safely in the recovery services vault it is easy to recover them.

**ContosoWebFE1**  
Backup Item

Backup now | Restore VM | File Recovery | Stop backup | Resume backup

| Alerts and Jobs                                 | Backup status                                     |
|-------------------------------------------------|---------------------------------------------------|
| <a href="#">View all Alerts</a> (last 24 hours) | Backup Pre-Check Passed                           |
| <a href="#">View all Jobs</a> (last 24 hours)   | Last backup status Success 3/12/2020, 12:20:38 AM |

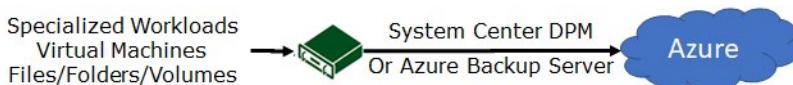
**Restore points (30)**

| CRASH CONSISTENT       | APPLICATION CONSISTENT | FILE-SYSTEM CONSISTENT |
|------------------------|------------------------|------------------------|
| 30                     | 0                      | 0                      |
| Time                   | Consistency            |                        |
| 3/12/2020, 12:20:42 AM | Crash Consistent       |                        |
| 3/11/2020, 12:20:59 AM | Crash Consistent       |                        |

Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation. The Backup service also creates and temporarily displays notifications, so you monitor how the backup is proceeding.

## Implement Azure Backup Server

Another method of backing up virtual machines is using a Data Protection Manager (DPM) or Microsoft Azure Backup Server (MABS) server. This method can be used for specialized workloads, virtual machines, or files, folders, and volumes. Specialized workloads can include SharePoint, Exchange, and SQL Server.



## Advantages

The advantages of backing up machines and apps to MABS/DPM storage, and then backing up DPM/MABS storage to a vault are as follows:

- Backing up to MABS/DPM provides app-aware backups optimized for common apps. These apps include SQL Server, Exchange, and SharePoint. Also, file/folder/volume backups, and machine state backups. Machine state backups can be bare-metal, or system state.
- For on-premises machines, you don't need to install the MARS agent on each machine you want to back up. Each machine runs the DPM/MABS protection agent, and the MARS agent runs on the MABS/DPM only.
- You have more flexibility and granular scheduling options for running backups.
- You can manage backups for multiple machines that you gather into protection groups in a single console. Grouping machines is useful when apps are tiered over multiple machines and you want to back them up at the same time.

## Backup steps

- Install the DPM or MABS protection agent on machines you want to protect. You then add the machines to a DPM protection group.
- To protect on-premises machines, the DPM or MABS server must be located on-premises.
- To protect Azure VMs, the MABS server must be located in Azure, running as an Azure VM.
- With DPM/MABS, you can protect backup volumes, shares, files, and folders. You can also protect a machine's system state (bare metal), and you can protect specific apps with app-aware backup settings.
- When you set up protection for a machine or app in DPM/MABS, you select to back up to the MABS/DPM local disk for short-term storage and to Azure for online protection. You also specify when the backup to local DPM/MABS storage should run and when the online backup to Azure should run.
- The disk of the protected workload is backed up to the local MABS/DPM disks, according to the schedule you specified.
- The DPM/MABS disks are backed up to the vault by the MARS agent that's running on the DPM/MABS server.

## Compare Backup Options

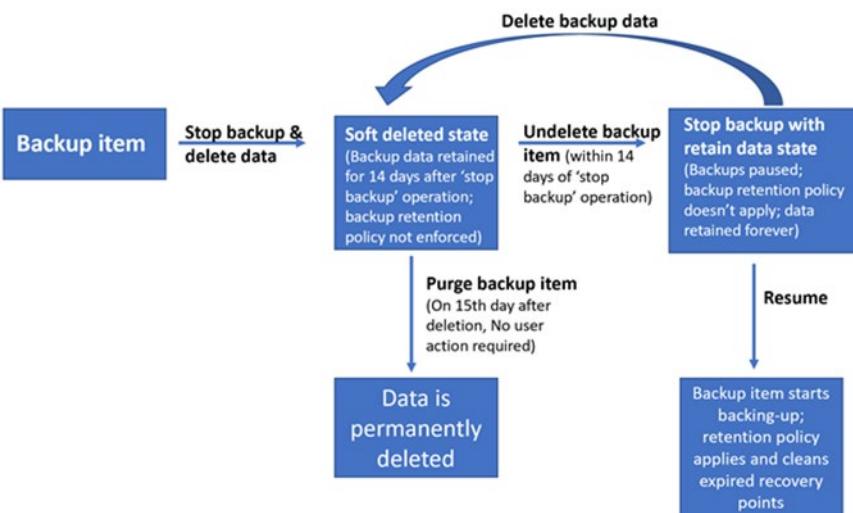
This table summarizes the Azure Backup (MARS) agent and the Azure Backup Server usage cases.

| Component                 | Benefits                                                                                       | Limits                                                                                                      | What is protected? | Where are backups stored? |
|---------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------|---------------------------|
| Azure Backup (MARS) agent | Backup files and folders on physical or virtual Windows OS; no separate backup server required | Backup 3x per day; not application aware; file, folder, and volume-level restore only; no support for Linux | Files and folders  | Recovery services vault   |

| Component                  | Benefits                                                                                                                                                                                  | Limits                                                                                              | What is protected?                                        | Where are backups stored?                      |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------|------------------------------------------------|
| Azure Backup Server (MABS) | App aware snapshots; full flex for when to backups; recovery granularity; linux support on Hyper-V and VMware VMs; backup and restore VMware VMs, doesn't require a System Center license | Cannot backup Oracle workloads; always requires live Azure subscription; no support for tape backup | Files, folders, volumes, VMs, applications, and workloads | Recovery services vault, locally attached disk |

## Manage Soft Delete

Azure Storage now offers soft delete for blob objects so that you can more easily recover your data when it is erroneously modified or deleted by an application or other storage account user. Soft delete for VMs protects the backups of your VMs from unintended deletion. Even after the backups are deleted, they're preserved in soft-delete state for 14 additional days.



## How soft delete works for virtual machines

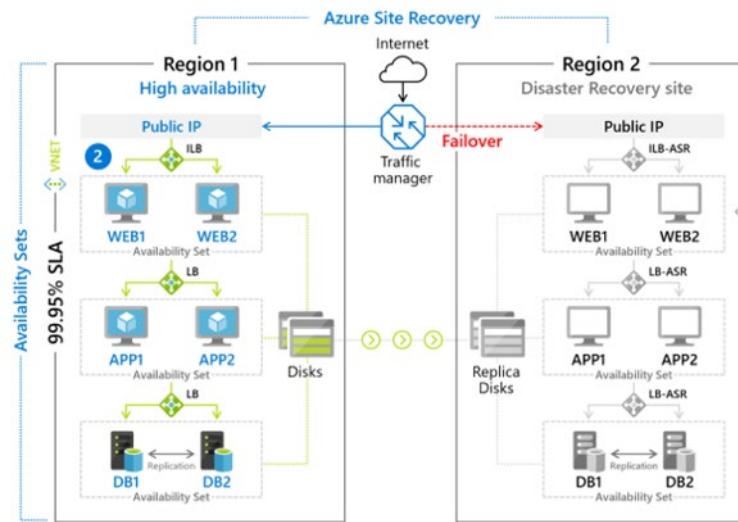
1. To delete the backup data of a VM, the backup must be stopped.
2. You can then choose to delete or retain the backup data. If you choose **Delete backup data** and then **Stop backup**, the VM backup won't be permanently deleted. Rather, the backup data will be retained for 14 days in the soft deleted state.
3. During those 14 days, in the Recovery Services vault, the soft deleted VM will appear with a red **soft-delete** icon next to it. If any soft-deleted backup items are present in the vault, the vault can't be deleted at that time. Try deleting the vault after the backup items are permanently deleted, and there are no items in soft deleted state left in the vault.

4. To restore the soft-deleted VM, it must first be undeleted. To undelete, choose the soft-deleted VM, and then select the option **Undelete**. At this point, you can also restore the VM by selecting **Restore VM** from the chosen restore point.
5. After the undelete process is completed, the status will return to **Stop backup with retain data** and then you can choose **Resume backup**. The Resume backup operation brings back the backup item in the active state, associated with a backup policy selected by the user defining the backup and retention schedules.

**Note:** Soft delete only protects deleted backup data. If a VM is deleted without a backup, the soft-delete feature won't preserve the data. All resources should be protected with Azure Backup to ensure full resilience.

## Implement Azure Site Recovery

Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.



## Replications Scenarios

- Replicate Azure VMs from one Azure region to another.
- Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure.
- Replicate AWS Windows instances to Azure.
- Replicate on-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site.

## Features

- Using Site Recovery, you can set up and manage replication, failover, and failback from a single location in the Azure portal.

- Replication to Azure eliminates the cost and complexity of maintaining a secondary datacenter.
- Site Recovery orchestrates replication without intercepting application data. When you replicate to Azure, data is stored in Azure storage, with the resilience that provides. When failover occurs, Azure VMs are created, based on the replicated data.
- Site Recovery provides continuous replication for Azure VMs and VMware VMs, and replication frequency as low as 30 seconds for Hyper-V.
- You can replicate using recovery points with application-consistent snapshots. These snapshots capture disk data, all data in memory, and all transactions in process.
- You can run planned failovers for expected outages with zero-data loss, or unplanned failovers with minimal data loss (depending on replication frequency) for unexpected disasters. You can easily fail back to your primary site when it's available again.
- Site Recovery integrates with Azure for simple application network management, including reserving IP addresses, configuring load-balancers, and integrating Azure Traffic Manager for efficient network switchovers.

**Note:** Are you considering using Azure Site Recovery and are you interested in any of these specific features? Which one is most important to you?

## Demonstration - Virtual Machine Backups

In this demonstration, we will schedule a daily backup of a virtual machine to a Recovery Services vault.

**Note:** This demonstration requires a virtual machine and a recovery service vault.

### Enable a backup on a virtual machine

1. In the Azure portal select the virtual machine you would like to backup.
2. In the **Operations** section, choose **Backup**. The Enable backup window opens.
3. Select **Create new** and provide a name for the new vault, such as **myRecoveryServicesVault**.
4. If not already selected, choose **Use existing**, then select the resource group of your VM from the drop-down menu.
5. Discuss how, by default, the vault is set for Geo-Redundant storage. This storage redundancy level ensures that your backup data is replicated to a secondary Azure region that's hundreds of miles away from the primary region.
6. Discuss how you can create and use policies to define when a backup job runs and how long the recovery points are stored. The default protection policy runs a backup job each day and retains recovery points for 30 days.
7. To accept the default backup policy values, select **Enable Backup**.
8. It takes a few moments to create the Recovery Services vault.

### Start a backup job and monitor the progress

1. Discuss how you can start a backup at any time, rather than wait for the default policy to run the job at the scheduled time. This first backup job creates a full recovery point. Each backup job after this initial backup creates incremental recovery points. Incremental recovery points are storage and time-efficient, as they only transfer changes made since the last backup.
2. In the Backup window for your VM, select **Backup now**.
3. Accept the backup retention policy of 30 days.

4. To start the job, select **Backup**.
5. In the Backup window for your VM, review the status of the backup and number of completed restore points.
6. Once the VM backup job is complete, information on the **Last backup time**, **Latest restore point**, and **Oldest restore point** is shown.
7. Point out the **Stop Backup** selection.

## Knowledge Check

Choose the best response for each question.

### Multiple choice

*You are responsible for creating a disaster recovery plan for your data center. You must be able to recreate virtual machines from scratch. This includes the Operating System, its configuration/ settings, and patches. Which of the following will provide a bare metal backup of your machines? Select one.*

- Azure Backup (MARS) agent
- Enable disk snapshots
- Azure Backup Server

### Multiple choice

*You have several Azure VMs that are currently running production workloads. You have a mix of Windows Server and Linux servers and you need to implement a backup strategy for your production workloads. Which feature should you use in this case? Select one.*

- Managed snapshots.
- Azure Backup.
- Azure Site Recovery.

### Multiple choice

*You plan to use Azure Backup to protect your virtual machines and data and are ready to create a backup. What is the first thing you need to do? Select one.*

- Create a Recovery Services vault.
- Create a Backup policy.
- Install the Azure VM Agent.

## Multiple choice

You deploy several virtual machines to Azure. You are responsible for backing up all data processed by the VMs. In the event of a failure, you need to restore the data as quickly as possible. Which of these options would you recommend to restore a database used for development on a data disk? Select one.

- Virtual machine backup
- Azure Site Recovery
- Disk snapshot

## Multiple choice

You deploy several virtual machines (VMs) to Azure. You are responsible for backing up all data processed by the VMs. In the event of a failure, you need to restore the data as quickly as possible. Which of these options would you recommend to restore the entire virtual machine or files on the virtual machine? Select one.

- Virtual machine backup
- Disk image backup
- Disk snapshot

## Multiple choice

Your organization needs a way to create application aware snapshots, and backup Linux virtual machines and VMware virtual machines. You have files, folders, volumes, and workloads to protect. You recommend which of the following solutions? Select one.

- Azure Backup Server
- Enable disk snapshots
- Enable backup for individual Azure VMs

## Summary and Resources

Azure Backup provides independent and isolated backups to guard against unintended destruction of the data on your VMs.

You should now be able to:

- Identify features and usage cases for different Azure backup methods.
- Configure virtual machine snapshots and backup options.
- Implement virtual machine backup and restore, including soft delete.
- Compare the Azure Backup (MARS) agent to the Azure Backup Server (MABS).
- Perform site-to-site recovery by using Azure Site Recovery.

## Learn more

You can learn more by reviewing the following.

- **An overview of Azure VM backup<sup>6</sup>**
- **Azure Backup Center<sup>7</sup>**
- **Azure Site Recovery documentation<sup>8</sup>**.
- **Learn - Protect your virtual machines by using Azure Backup<sup>9</sup>**
- **Learn - Implement hybrid backup and recovery with Windows Server IaaS<sup>10</sup>**
- **Learn - Protect your Azure infrastructure with Azure Site Recovery<sup>11</sup>**
- **Learn - Protect your on-premises infrastructure from disasters with Azure Site Recovery<sup>12</sup>**

---

<sup>6</sup> <https://docs.microsoft.com/azure/backup/backup-azure-vms-introduction>

<sup>7</sup> <https://docs.microsoft.com/azure/backup/backup-center-overview>

<sup>8</sup> <https://docs.microsoft.com/azure/site-recovery/site-recovery-overview>

<sup>9</sup> <https://docs.microsoft.com/learn/modules/protect-virtual-machines-with-azure-backup/>

<sup>10</sup> <https://docs.microsoft.com/learn/modules/implement-hybrid-backup-recovery-windows-server-iaas/>

<sup>11</sup> <https://docs.microsoft.com/learn/modules/protect-infrastructure-with-site-recovery/>

<sup>12</sup> <https://docs.microsoft.com/learn/modules/protect-on-premises-infrastructure-with-azure-site-recovery/>

# Module 10 Lab

## Lab 10 - Backup virtual machines

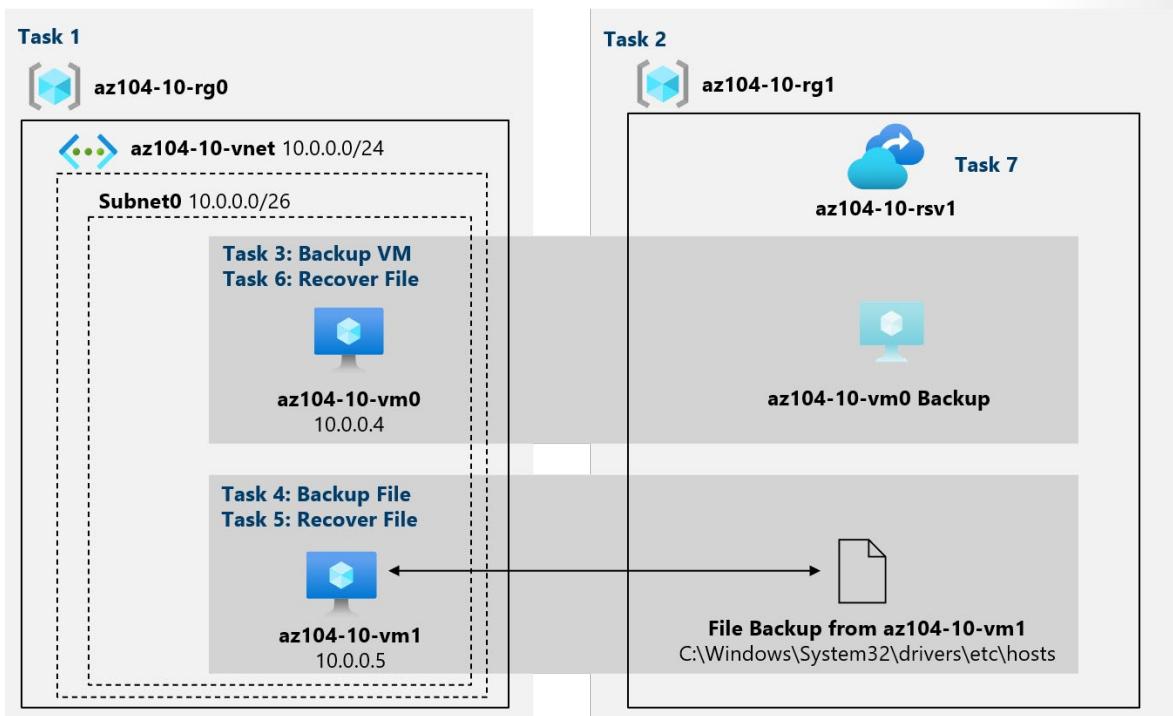
### Lab scenario

You have been tasked with evaluating the use of Azure Recovery Services for backup and restore of files hosted on Azure virtual machines and on-premises computers. In addition, you want to identify methods of protecting data stored in the Recovery Services vault from accidental or malicious data loss.

### Objectives

In this lab, you will:

- Task 1: Provision the lab environment.
- Task 2: Create a Recovery Services vault.
- Task 3: Implement Azure virtual machine-level backup.
- Task 4: Implement File and Folder backup.
- Task 5: Perform file recovery by using Azure Recovery Services agent.
- Task 6: Perform file recovery by using Azure virtual machine snapshots.
- Task 7: Review the Azure Recovery Services soft delete functionality.



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).



# Answers

## Multiple choice

You need to backup files and folders to Azure. Which of these steps would you do first?

- Download, install and register the backup agent.
- Back up files and folders.
- Create a recovery services vault.

### Explanation

*First, create a recovery services vault. Second, download, install and register the backup agent. Lastly, backup your files and folders.*

## Multiple choice

You are responsible for implementing server workload backups. You need to implement on-premises backups to an Azure Recovery Vault service. What should you do? Select one.

- Download and install the MARS agent, and then register the server by installing the vault credentials.
- Just download and install the MARS agent.
- Don't do anything. Windows Servers contain the required agent for inclusion in the Recovery Vault service.

### Explanation

*Download and install the MARS agent, and then register the server by installing the vault credentials. You can download all the required components direct from the Azure portal.*

## Multiple choice

You have created the Recovery Vault service. Now you decide to change the storage replication type to locally redundant. In which situations can Larissa change the storage replication type?

- You can change this setting at any time.
- You can change this setting, but only before a Recovery Vault service starts providing protection for items.
- You cannot change this setting at any time.

### Explanation

*You can change this setting, but only before a Recovery Vault service starts providing protection for items.*

## Multiple choice

You are responsible for creating a disaster recovery plan for your data center. You must be able to recreate virtual machines from scratch. This includes the Operating System, its configuration/ settings, and patches. Which of the following will provide a bare metal backup of your machines? Select one.

- Azure Backup (MARS) agent
- Enable disk snapshots
- Azure Backup Server

### Explanation

*Azure Backup Server provides a bare metal backup capability.*

**Multiple choice**

You have several Azure VMs that are currently running production workloads. You have a mix of Windows Server and Linux servers and you need to implement a backup strategy for your production workloads. Which feature should you use in this case? Select one.

- Managed snapshots.
- Azure Backup.
- Azure Site Recovery.

*Explanation*

*Azure Backup is the best option for your production workloads.*

**Multiple choice**

You plan to use Azure Backup to protect your virtual machines and data and are ready to create a backup. What is the first thing you need to do? Select one.

- Create a Recovery Services vault.
- Create a Backup policy.
- Install the Azure VM Agent.

*Explanation*

*Create Recovery Services vault. When performing a virtual machine backup, you must first create a Recovery Services vault in the region where you want to store the data. Recovery points are stored in the Recovery Services vault. While creating a backup policy is a good practice, it is not a dependency to creating a backup. The Azure VM agent is required on an Azure virtual machine for the Backup extension to work. However, if the VM was created from the Azure gallery, then the VM Agent is already present on the virtual machine.*

**Multiple choice**

You deploy several virtual machines to Azure. You are responsible for backing up all data processed by the VMs. In the event of a failure, you need to restore the data as quickly as possible. Which of these options would you recommend to restore a database used for development on a data disk? Select one.

- Virtual machine backup
- Azure Site Recovery
- Disk snapshot

*Explanation*

*Disk snapshot. You can use snapshots to quickly restore the database data disks.*

**Multiple choice**

You deploy several virtual machines (VMs) to Azure. You are responsible for backing up all data processed by the VMs. In the event of a failure, you need to restore the data as quickly as possible. Which of these options would you recommend to restore the entire virtual machine or files on the virtual machine? Select one.

- Virtual machine backup
- Disk image backup
- Disk snapshot

*Explanation*

*Use Azure Backup to restore a VM to a specific point in time, and to restore individual files. Azure Backup supports application-consistent backups for both Windows and Linux VMs.*

**Multiple choice**

Your organization needs a way to create application aware snapshots, and backup Linux virtual machines and VMware virtual machines. You have files, folders, volumes, and workloads to protect. You recommend which of the following solutions? Select one.

- Azure Backup Server
- Enable disk snapshots
- Enable backup for individual Azure VMs

*Explanation*

*Azure backup server provides app aware snapshots, support for Linux virtual machines and VMware virtual machines. Backup server can protect files, folders, volumes, and workloads.*



## Module 11 Administer Monitoring

### Configure Azure Monitor

#### Introduction

#### Scenario

Logging and monitoring the health of your services is a vital component of production applications. Azure Administrators determine the causes of failures and try to identify any problems before they occur.

Azure Monitor is an important tool to help you in this process. It enables you to gather monitoring and diagnostic information about the health of your services. You can use this information to visualize and analyze the causes of problems that might occur in your app.

Suppose that you work for the operations team of a large organization. The organization is running large-scale production apps in the cloud. The operations team wants to consolidate its log data in a single service to improve visibility across services and simplify its logging strategy.

#### Skills measured

Azure Monitor is part of **Exam AZ-104: Microsoft Azure Administrator<sup>1</sup>**.

Monitor and back up Azure resources (10–15%)

Monitor resources by using Azure Monitor

- Configure and interpret metrics
- Configure Azure Monitor logs

<sup>1</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

## Learning objectives

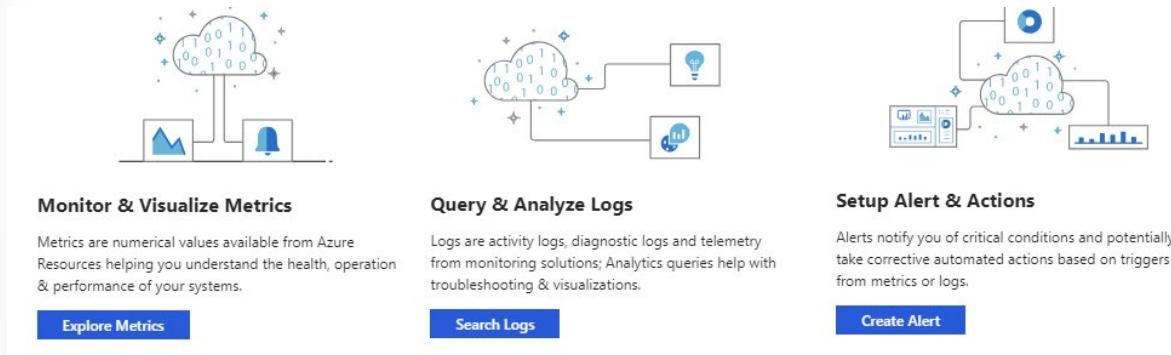
In this module, you will learn how to:

- Identify the features and usage cases for Azure Monitor.
- Configure and interpret metrics and logs.
- Identify the Azure Monitor components and data types.
- Configure the Activity Log.

## Prerequisites

None.

## Describe Azure Monitor Key Capabilities



- **Monitor and visualize metrics.** Metrics are numerical values available from Azure resources helping you understand the health, operation and performance of your system.
- **Query and analyze logs.** Logs are activity logs, diagnostic logs, and telemetry from monitoring solutions; analytics queries help with troubleshooting and visualizations.
- **Setup alerts and actions.** Alerts notify you of critical conditions and potentially take automated corrective actions based on triggers from metrics or logs.

## Describe Azure Monitor Components

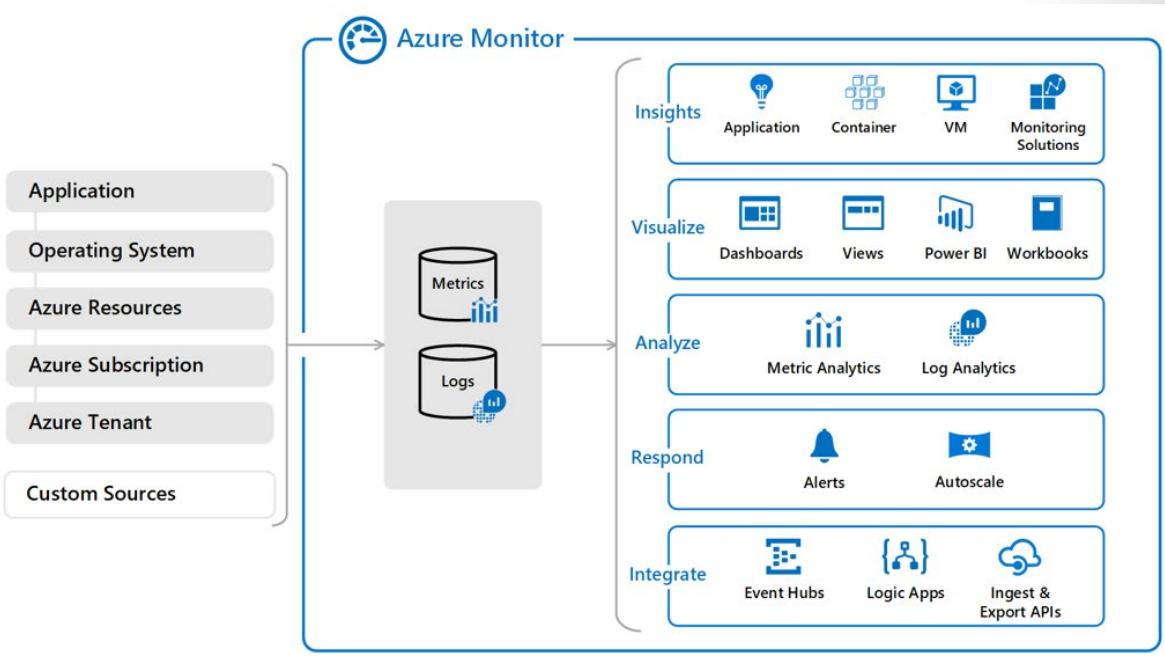
Monitoring is the act of collecting and analyzing data. The data can be used to determine the performance, health, and availability of your business application and the resources that it depends on.

An effective monitoring strategy helps you understand the detailed operation of the components of your application. Monitoring also helps you increase your uptime by proactively notifying you of critical issues. You can then resolve the issues before they become severe.

Azure includes multiple services that individually perform a specific role or task in the monitoring space. Together, these services deliver a comprehensive solution for collecting, analyzing, and acting on data from your application and the Azure resources that support them. The services also work to monitor critical on-premises resources to provide a hybrid monitoring environment. Understanding the tools and data that are available is the first step in developing a complete monitoring strategy for your application.

The next diagram gives a high-level view of Azure Monitor. At the center of the diagram, are the data stores for metrics and logs. Metrics and logs are the two fundamental types of data use by Azure Monitor. On the left side of the diagram, are the sources of monitoring data that populate these data stores.

On the right side of the diagram, are the different functions that Azure Monitor performs with this collected data such as analysis, alerting, and streaming to external systems.



## Define Metrics and Logs

All data collected by Azure Monitor fits into one of two fundamental types, **metrics and logs<sup>2</sup>**.

- **Metrics** are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios.
- **Logs** contain different kinds of data organized into records with different sets of properties for each type. Data such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis.

## Metrics

For many Azure resources, the data collected by Azure Monitor is displayed on the Overview page in the Azure portal. For example, virtual machines have several charts displaying performance metrics. Click on any of the graphs to open the data in Metric explorer in the Azure portal, which allows you to chart the values of multiple metrics over time. You can view the charts interactively or pin them to a dashboard to view them with other visualizations.

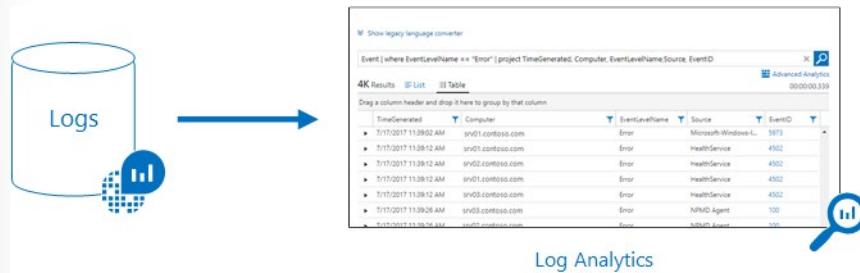
<sup>2</sup> <https://docs.microsoft.com/azure/azure-monitor/platform/data-collection>



## Logs

Log data collected by Azure Monitor is stored in Log Analytics which includes a **rich query language<sup>3</sup>** to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using the Log Analytics page in the Azure portal. You can use the query results to directly analyze the data, save queries, visualize the data, or create alert rules.

Azure Monitor uses a version of the **Data Explorer<sup>4</sup>** query language that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics. You can quickly learn the query language using multiple lessons. Particular guidance is provided to users who are already familiar with SQL and Splunk.



## Identify Data Types

Azure Monitor can collect data from various sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

- **Application monitoring data:** Data about the performance and functionality of the code you have written, regardless of its platform.
- **Guest OS monitoring data:** Data about the operating system on which your application is running. The application could be running in Azure, another cloud, or on-premises.
- **Azure resource monitoring data:** Data about the operation of an Azure resource.
- **Azure subscription monitoring data:** Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- **Azure tenant monitoring data:** Data about the operation of tenant-level Azure services, such as Azure Active Directory.

<sup>3</sup> <https://docs.microsoft.com/azure/azure-monitor/log-query/log-query-overview>

<sup>4</sup> <https://docs.microsoft.com/azure/kusto/query/>

Azure Monitor starts collecting data as soon as you create an Azure subscription and add resources. Activity Logs record when resources are created or modified. Metrics tell you how the resource is performing and the resources it is consuming.

Extend the data you're collecting into the actual operation of the resources by enabling diagnostics and adding an agent to compute resources. Extending your data sources will collect data for the internal operation of the resource. It will also let you configure different data sources to collect logs and metrics from Windows and Linux guest operating systems.

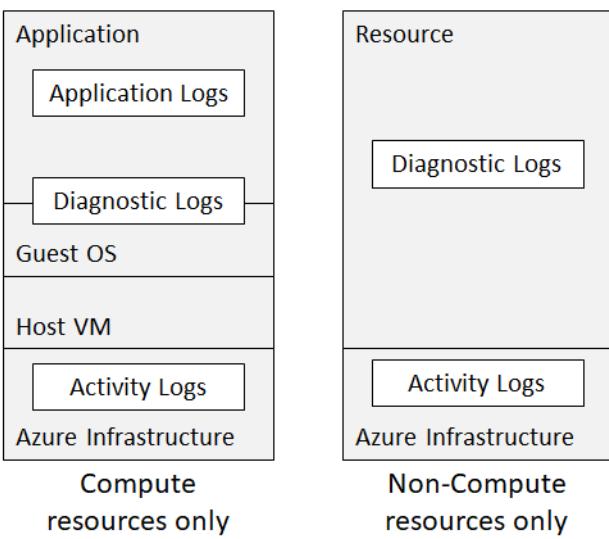
**Note:** Azure Monitor can collect log data from any REST client using the Data Collector API. The Data Collector API lets you create custom monitoring scenarios and extend monitoring to resources that don't expose data through other sources.

## Describe Activity Log Events

The Azure Activity Log is a subscription log that provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events.

With the Activity Log, you can determine the 'what, who, and when' for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. You can also understand the status of the operation and other relevant properties. Through activity logs, you can determine:

- What operations were taken on the resources in your subscription?
- Who started the operation?
- When the operation occurred?
- The status of the operation.
- The values of other properties that might help you research the operation.

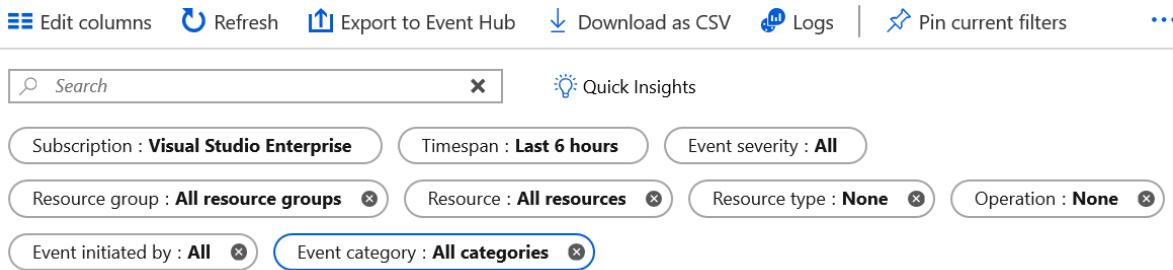


**Note:** Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past. You can retrieve events from your Activity Log using the Azure portal, CLI, PowerShell cmdlets, and Azure Monitor REST API.

# Query the Activity Log

In the Azure portal, you can filter your Activity Log.

## Activity log



The screenshot shows the Azure Activity Log search interface. At the top, there are several buttons: 'Edit columns', 'Refresh', 'Export to Event Hub', 'Download as CSV', 'Logs' (with a bell icon), 'Pin current filters', and a three-dot menu. Below these are search and filter controls. A 'Search' input field contains 'x'. To its right is a 'Quick Insights' button with a lightbulb icon. Below these are several filter boxes: 'Subscription : Visual Studio Enterprise', 'Timespan : Last 6 hours', 'Event severity : All', 'Resource group : All resource groups (x)', 'Resource : All resources (x)', 'Resource type : None (x)', 'Operation : None (x)', 'Event initiated by : All (x)', and 'Event category : All categories (x)'. The 'Event category : All categories' box is highlighted with a blue border.

- **Subscription.** One or more Azure subscription names.
- **Timespan.** The start and end time for events.
- **Event Severity.** The severity level of the event (Informational, Warning, Error, Critical).
- **Resource group.** One or more resource groups within those subscriptions.
- **Resource (name).** The name of a specific resource.
- **Resource type.** The type of resource, for example, Microsoft.Compute/virtualmachines.
- **Operation name.** The name of an Azure Resource Manager operation, for example, Microsoft.SQL/servers/Write.
- **Event initiated by.** The 'caller,' or user who performed the operation.
- **Search.** This is an open text search box that searches for that string across all fields in all events.

## Event categories

- **Administrative.** This category contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of the types of events you would observe in this category include "create virtual machine" and "delete network security group". The Administrative category also includes any changes to role-based access control in a subscription.
- **Service Health.** This category contains the record of any service health incidents that have occurred in Azure. An example of the type of event you would observe in this category is "SQL Azure in East US is experiencing downtime." Service health events come in five varieties: Action Required, Assisted Recovery, Incident, Maintenance, Information, or Security.
- **Resource Health.** This category contains the record of any resource health events that have occurred to your Azure resources. An example of the type of event you would see in this category is "Virtual Machine health status changed to unavailable." Resource health events can represent one of four health statuses: Available, Unavailable, Degraded, and Unknown.
- **Alert.** This category contains the record of all activations of Azure alerts. An example of the type of event you would observe in this category is "CPU % on myVM has been over 80 for the past 5 minutes."
- **Autoscale.** This category contains the record of any events related to the operation of the autoscale engine based on any autoscale settings you have defined in your subscription. An example of the type of event you would observe in this category is "Autoscale scale up action failed."

- **Recommendation.** This category contains recommendation events from certain resource types, such as web sites and SQL servers. These events offer recommendations for how to better utilize your resources.
- **Security.** This category contains the record of any alerts generated by Azure Defender for Servers. An example of the type of event you would observe in this category is "Suspicious double extension file executed."
- **Policy.** This category contains records of all effect action operations performed by Azure Policy. Examples of the types of events you would see in this category include Audit and Deny.

**Note:** Once you have defined a set of filters, you can pin the filtered state to the dashboard or download the search results as a CSV file.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*You need to determine who deleted a network security group through Resource Manager. You are viewing the Activity Log when another Azure Administrator says you should use this event category to narrow your search. Select one.*

- Administrative
- Service Health
- Policy

### Multiple choice

*What is the shared underlying logging data platform for Azure Sentinel and Azure Security Center?*

- Activity Logs
- Azure Monitor Logs
- Diagnostic Settings

### Multiple choice

*What data does Azure Monitor collect?*

- Data from a variety of sources, such as the application event log, the operating system (Windows and Linux), Azure resources, and custom data sources
- Azure billing details
- Backups of database transaction logs

## Multiple choice

What two fundamental types of data does Azure Monitor collect?

- Metrics and logs
- Username and password
- Email notifications and errors

## Summary and Resources

### Summary

Azure Monitor helps you maximize the availability and performance of your applications and services.

You should now be able to:

- Identify the features and usage cases for Azure Monitor.
- Configure and interpret metrics and logs.
- Identify the Azure Monitor components and data types.
- Configure Activity Log monitoring.

### Learn more

You can learn more by reviewing the following.

- **Azure Monitor documentation<sup>5</sup>**
- **Learn - Monitor and report on security events in Azure AD<sup>6</sup>**
- **Learn - Monitor performance of virtual machines by using Azure Monitor for VMs<sup>7</sup>**
- **Learn - Monitor, diagnose, and troubleshoot your Azure storage<sup>8</sup>**
- **Learn - Design a holistic monitoring strategy on Azure<sup>9</sup>**

---

<sup>5</sup> <https://docs.microsoft.com/azure/azure-monitor/>

<sup>6</sup> <https://docs.microsoft.com/learn/modules/monitor-report-aad-security-events/>

<sup>7</sup> <https://docs.microsoft.com/learn/modules/monitor-performance-using-azure-monitor-for-vms/>

<sup>8</sup> <https://docs.microsoft.com/learn/modules/monitor-diagnose-and-troubleshoot-azure-storage/>

<sup>9</sup> <https://docs.microsoft.com/learn/modules/design-monitoring-strategy-on-azure/>

# Configure Azure Alerts

## Introduction

### Scenario

You use Azure Monitor to configure notifications and alerts for your key systems and applications. These alerts will ensure that the correct team knows when a problem arises.

You work for a large retail company that recently deployed several shopping applications to the Azure platform. During peak sales times, the system begins to slow and response times increase.

As an Azure Administrator, you need to detect these problems in real time. You need to resolve any problems before your customers notice.

### Skills measured

Configuring alerts and actions is part of the **Exam AZ-104: Microsoft Azure Administrator<sup>10</sup>**.

Monitor and back up Azure resources (10–15%)

Monitor resources by using Azure Monitor

- Set up alerts and actions.

### Learning objectives

In this module, you will learn how to:

- Configure Azure Monitor alerts.
- Create alert rules and action groups.

### Prerequisites

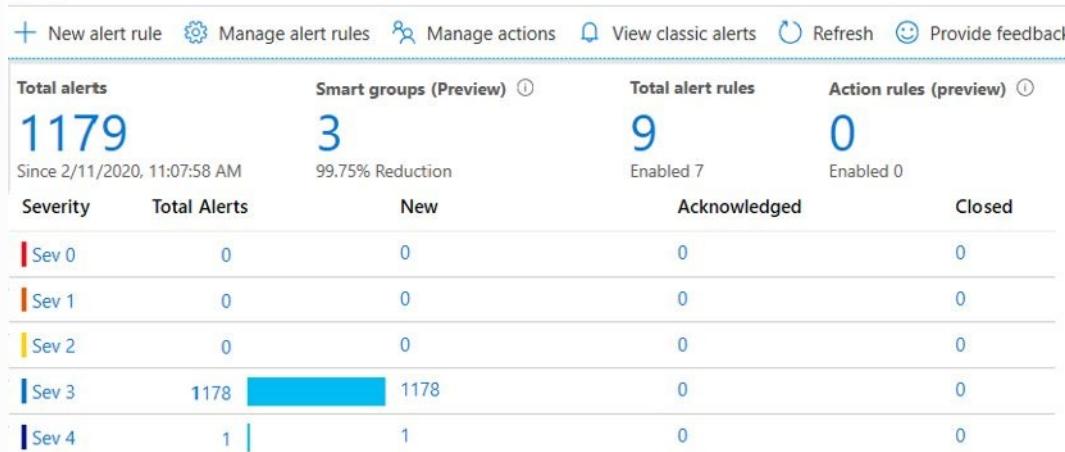
None.

---

<sup>10</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

# Manage Azure Monitor Alerts

## Alerts



The Monitor Alerts experience has many benefits.

- **Better notification system.** All newer alerts use action groups, which are named groups of notifications and actions that can be reused in multiple alerts.
- **A unified authoring experience.** All alert creation for metrics, logs and activity log across Azure Monitor, Log Analytics, and Application Insights is in one place.
- **View Log Analytics alerts in Azure portal.** You can now also observe Log Analytics alerts in your subscription. Previously these were in a separate portal.
- **Separation of Fired Alerts and Alert Rules.** Alert Rules (the definition of the condition that triggers an alert), and Fired Alerts (an instance of the alert rule firing) are differentiated, so the operational and configuration views are separated.
- **Better workflow.** The new alerts authoring experience guides the user along the process of configuring an alert rule, which makes it simpler to discover the right things to get alerted on.

## Managing Alerts

You can alert on metrics and logs as described in monitoring data sources. These include but are not limited to:

- Metric values
- Log search queries
- Activity Log events
- Health of the underlying Azure platform
- Tests for web site availability

## Alert states

You can set the state of an alert to specify where it is in the resolution process. When the criteria specified in the alert rule is met, an alert is created or fired, it has a status of **New**. You can change the status when you acknowledge an alert and when you close it. All state changes are stored in the history of the alert. The following alert states are supported.

| State               | Description                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>New</b>          | The issue has been detected and has not yet been reviewed.                                                      |
| <b>Acknowledged</b> | An administrator has reviewed the alert and started working on it.                                              |
| <b>Closed</b>       | The issue has been resolved. After an alert has been closed, you can reopen it by changing it to another state. |

**Note:** Alert state is different and independent of the monitor condition. Alert state is set by the user. Monitor condition is set by the system. When an alert fires, the alert's monitor condition is set to fired. When the underlying condition that caused the alert to fire clears, the monitor condition is set to re-solved. The alert state isn't changed until the user changes it.

## Create Alert Rules

Alerts proactively notify you when important conditions are found in your monitoring data. They allow you to identify and address issues before the users of your system notice them. Alerts consist of alert rules, action groups, and monitor conditions.

[Home](#) > [Alerts](#) >

### Create alert rule

Rules management

Create an alert rule to identify and address issues when important conditions are found in your monitoring data. When defining the alert rule, check that your inputs do not contain any sensitive content.

#### Scope

Select the target resource you wish to monitor.

Resource

No resource selected yet

[Select resource](#)

#### Condition

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name

No condition selected yet

#### Action group

Send notifications or invoke actions when the alert rule triggers, by selecting or creating a new action group

Action group name

No action group selected yet

Alert rules are separated from alerts and the actions that are taken when an alert fires. The alert rule captures the target and criteria for alerting. The alert rule can be in an enabled or a disabled state. Alerts only fire when enabled. The key attributes of an alert rule are:

- **Target Resource** – Defines the scope and signals available for alerting. A target can be any Azure resource. Example targets: a virtual machine, a storage account, a virtual machine scale set, a Log Analytics workspace, or an Application Insights resource. For certain resources (like Virtual Machines), you can specify multiple resources as the target of the alert rule.
- **Signal** – Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

- **Criteria** – Criteria is a combination of Signal and Logic applied on a Target resource. Examples: \* Percentage CPU > 70%; Server Response Time > 4 ms; and Result count of a log query > 100.
- **Alert Name** – A specific name for the alert rule configured by the user.
- **Alert Description** – A description for the alert rule configured by the user.
- **Severity** – The severity of the alert once the criteria specified in the alert rule is met. Severity can range from 0 to 4.
- **Action** – A specific action taken when the alert is fired.

## Create Action Groups

An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered. Various alerts may use the same action group or different action groups depending on the user's requirements.

**Notifications** configure the method in which users will be notified when the action group triggers.

### Notifications

Configure the method in which users will be notified when the action group triggers. Select notification types, provide receiver details and add a unique description. This step is optional.

| Notification type ⓘ               | Name ⓘ | Selected ⓘ |
|-----------------------------------|--------|------------|
| <input type="checkbox"/>          |        |            |
| Email Azure Resource Manager Role |        |            |
| Email/SMS message/Push/Voice      |        |            |

- **Email Azure Resource Manager role** – Send email to the members of the subscription's role. Email will only be sent to Azure AD user members of the role. Email will not be sent to Azure AD groups or service principals.
- **Email/SMS message/Push/Voice** - Specify any email, SMS, push, or voice actions.

**Actions** configure the method in which actions are performed when the action group triggers.

### Actions

Configure the method in which actions are performed when the action group triggers. Select action types, fill out associated details, and add a unique description. This step is optional.

| Action type ⓘ            | Name ⓘ | Selected ⓘ |
|--------------------------|--------|------------|
| <input type="checkbox"/> |        |            |
| Automation Runbook       |        |            |
| Azure Function           |        |            |
| ITSM                     |        |            |
| Logic App                |        |            |
| Secure Webhook           |        |            |
| Webhook                  |        |            |

- **Automation runbook** - An automation runbook is the ability to define, build, orchestrate, manage, and report on workflows that support system and network operational processes. A runbook workflow can potentially interact with all types of infrastructure elements, such as applications, databases, and hardware.

- **Azure Function** – Azure functions is a serverless compute service that lets you run event-triggered code without having to explicitly provision or manage infrastructure.
- **ITSM** – Connect Azure and a supported IT Service Management (ITSM) product/service. This requires an ITSM Connection.
- **Logic App** – Logic apps connect your business-critical apps and services by automating your workflows.
- **Webhook** – A webhook is a HTTPS or HTTP endpoint that allows external applications to communicate with your system.

## Demonstration - Alerts

In this demonstration, we will create an alert rule.

### Create an alert rule

1. In Azure portal, click on **Monitor**. The Monitor blade consolidates all your monitoring settings and data in one view.
2. Click **Alerts** then click **+ New alert rule**. As most resource blades also have Alerts in their resource menu under Monitoring, you could create alerts from there as well.

### Explore alert targets

1. Click **Select** under Target, to select a target resource that you want to alert on. Use **Subscription** and **Resource type** drop-downs to find the resource you want to monitor. You can also use the search bar to find your resource.
2. If the selected resource has metrics you can create alerts on, Available signals on the bottom right will include metrics. You can view the full list of resource types supported for metric alerts in this article.
3. Click **Done** when you have made your selection.

### Explore alert conditions

1. Once you have selected a target resource, click on **Add condition**.
2. You will observe a list of signals supported for the resource, select the metric you want to create an alert on.
3. Optionally, refine the metric by adjusting Period and Aggregation. If the metric has dimensions, the Dimensions table will be presented.
4. Observe a chart for the metric for the last 6 hours. Adjust the **Show history** drop-down.
5. Define the **Alert logic**. This will determine the logic which the metric alert rule will evaluate.
6. If you are using a static threshold, the metric chart can help determine what might be a reasonable threshold. If you are using a Dynamic Thresholds, the metric chart will display the calculated thresholds based on recent data.
7. Click **Done**.
8. Optionally, add another criteria if you want to monitor a complex alert rule.

### Explore alert details

1. Fill in Alert details like **Alert Rule Name**, **Description** and **Severity**.
2. Add an action group to the alert either by selecting an existing action group or creating a new action group.

3. Click **Done** to save the metric alert rule.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*Your organization has an app that is used across the business. The performance of this app is critical to day-to-day operations. Because the app is so important, four IT administrators have been identified to address any issues. You have configured an alert and need to ensure the administrators are notified if there is a problem. In which area of the portal will you provide the administrator email addresses? Select one.*

- Activity log
- Performance group
- Action Group

### Multiple choice

*You are reviewing the Alerts page and notice an alert has been Acknowledged. What does this mean? Select one.*

- An administrator has reviewed the alert and started working on it.
- The issue has been resolved.
- The issue has been closed.

### Multiple choice

*What's the composition of an alert rule? Select one.*

- Resource, condition, log, alert type
- Metrics, logs, application, operating system
- Resource, condition, actions, alert details

### Multiple choice

*Which of the following is an example of a log data type?*

- HTTP response records
- Percentage of CPU over time
- Website requests per hour

# Summary and Resources

## Summary

Alerts proactively notify you when issues are found with your infrastructure or application using your monitoring data in Azure Monitor. They allow you to identify and address issues before the users of your system notice them.

You should now be able to:

- Configure Azure Monitor alerts.
- Create alert rules and action groups.

## Learn more

You can learn more by reviewing the following.

- **The new alerts experience in Azure Monitor<sup>11</sup>**
- **Learn - Improve incident response with alerting on Azure<sup>12</sup>**
- **Learn - Manage alerts and incidents in Microsoft Defender for Endpoint<sup>13</sup>**
- **Learn - Configure alerts and detections in Microsoft Defender for Endpoint<sup>14</sup>**
- **Learn - Monitor the health of your Azure virtual machine by using Azure Metrics Explorer and metric alerts<sup>15</sup>**

<sup>11</sup> <https://docs.microsoft.com/azure/monitoring-and-diagnostics/monitoring-overview-unified-alerts>

<sup>12</sup> <https://docs.microsoft.com/learn/modules/incident-response-with-alerting-on-azure/>

<sup>13</sup> <https://docs.microsoft.com/learn/modules/manage-alerts-incidents-microsoft-defender-for-endpoints/>

<sup>14</sup> <https://docs.microsoft.com/learn/modules/incident-response-with-alerting-on-azure/>

<sup>15</sup> <https://docs.microsoft.com/learn/modules/monitor-azure-vm-using-diagnostic-data/>

# Configure Log Analytics

## Introduction

### Scenario

Azure Monitor collects log data and stores it in tables. As an Administrator, you configure the input data sources and then conduct queries. Queries provide insights into your infrastructure. For example, assessing system updates and troubleshooting operational incidents. To quickly retrieve and consolidate data in the repository you will create Kusto Query Language (KQL) queries.

As part of a larger team, you must know what the capabilities are to query and evaluate the log data that's fed into the service.

### Skills measured

Log Analytics querying is part of **Exam AZ-104: Microsoft Azure Administrator<sup>16</sup>**.

Monitor and back up Azure resources (10–15%)

Monitor resources by using Azure Monitor

- Query and analyze logs.

### Learning objectives

In this module, you will learn how to:

- Identify the features and usage cases for Log Analytics.
- Create a Log Analytics workspace and configure connected and data sources.
- Structure a Log Analytics query and review results.

### Prerequisites

None.

## Determine Log Analytics Uses

Log Analytics is a service in that helps you collect and analyze data generated by resources in your cloud and on-premises environments.

Log queries help you to use the data collected in Azure Monitor Logs. A powerful query language allows you to join data from multiple tables, aggregate large sets of data, and perform complex operations with minimal code. Virtually any question can be answered and analysis performed as long as the supporting data has been collected, and you understand how to construct the right query.

Some features in Azure Monitor such as insights and solutions process log data without exposing you to the underlying queries. To use other features of Azure Monitor, you should understand how queries are constructed and how you can use them to interactively analyze data in Azure Monitor Logs.

---

<sup>16</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

The screenshot shows the Microsoft Monitor - Logs interface. On the left, there's a sidebar with various navigation options: Overview, Activity log, Alerts, Metrics, Logs (which is selected and highlighted with a red box), and Service Health. Below that is an Insights section with Applications, Virtual Machines (preview), Containers, Network, and More. The main pane shows a 'New Query 1' search bar at the top, followed by a tree view of log sources. The 'Active' workspace is selected, and it lists several resources under the 'contosoretail-IT' node, including ADAssessment, ADReplication, AlertManagement, AntiMalware, ApplicationInsights, AzureAutomation, ChangeTracking, CompatibilityAssessment, ContainerInsights, Containers, DeviceHealthProd, DnsAnalytics, InfrastructureInsights, and LogManagement.

## Example 1 - Assessing updates

An important part of the daily routine for any IT administrator is assessing systems update requirements and planning patches. Accurate scheduling is critical, as it directly relates to SLAs to the business and can seriously impact business functions. In the past, you had to schedule an update with only limited knowledge of how long the patching would take. Operations Management Suite collects data from all customers performing patches and uses that data to provide an average patching time for specific missing updates. This use of "crowd-sourced" data is unique to cloud systems, and is a great example of how Log Analytics can help meet strict SLAs.

## Example 2 - Change tracking

Troubleshooting an operational incident is a complex process, requiring access to multiple data streams. With Operations Management Suite, you can easily perform analysis from multiple angles, using data from a wide variety of sources through a single interface for correlation of information. By tracking changes throughout the environment, Log Analytics helps to easily identify things like abnormal behavior from a specific account, users installing unapproved software, unexpected system reboots or shutdowns, evidence of security breaches, or specific problems in loosely coupled applications.

## Create a Workspace

To get started with Log Analytics you need to add a workspace.

**Log Analytics workspace**

Create new or link existing workspace

Create New  Link Existing

**Log Analytics Workspace \*** ⓘ  
enter workspace name

**Subscription \***  
Azure Pass - Sponsorship

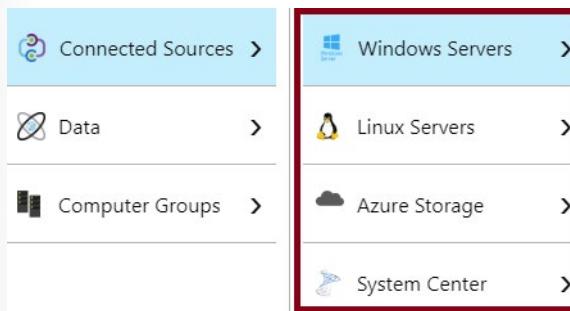
**Resource group \***  
Select existing... ⏺  
[Create new](#)

**Location \***  
West US ⏺

- Provide a name for the new Log Analytics workspace.
- Select a Subscription from the drop-down list.
- For Resource Group, select an existing resource group that contains one or more Azure virtual machines.
- Select the Location your VMs are deployed to.
- The workspace will automatically use the Per GB pricing plan.

## Define Connected Sources

Connected Sources are the computers and other resources that generate data collected by Log Analytics. This can include agents installed on **Windows<sup>17</sup>** and **Linux<sup>18</sup>** computers that connect directly or agents in a connected **System Center Operations Manager management group<sup>19</sup>**. Log Analytics can also collect data from **Azure storage<sup>20</sup>**.



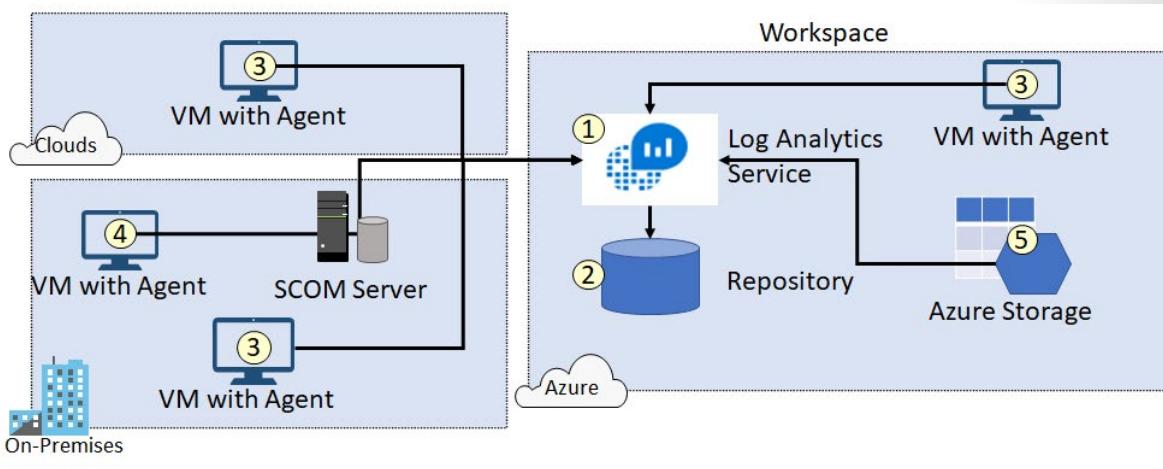
This following diagram shows how Connected Sources flow data to the Log Analytics service.

<sup>17</sup> <https://docs.microsoft.com/azure/log-analytics/log-analytics-windows-agents>

<sup>18</sup> <https://docs.microsoft.com/azure/log-analytics/log-analytics-linux-agents>

<sup>19</sup> <https://docs.microsoft.com/azure/log-analytics/log-analytics-om-agents>

<sup>20</sup> <https://docs.microsoft.com/azure/log-analytics/log-analytics-azure-storage>

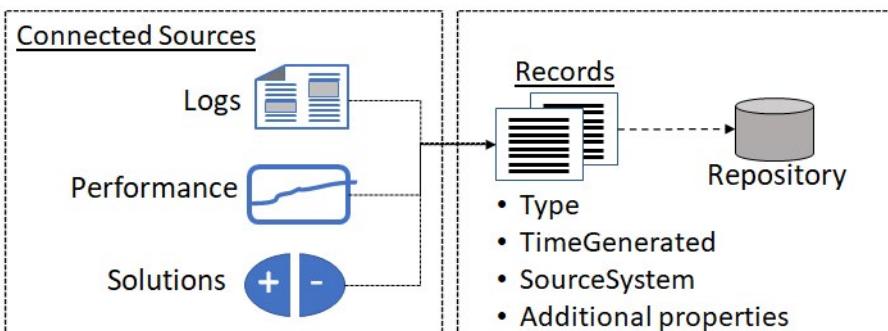


Ensure you can locate each of the following.

- The Log Analytics service (1) collects data and stores it in the repository (2). The repository is hosted in Azure. Connected Sources provide information to the Log Analytics service.
- Computer agents (3) generate data to the Log Analytics service. These agents can run on Windows or Linux computers, virtual or physical computers, on-premises or cloud computers, and Azure or other cloud providers.
- A System Center Operations Manager (SCOM) management group can be connected to Log Analytics. SCOM agents (4) communicate with management servers that forward events and performance data to Log Analytics.
- An Azure storage account (5) can also collect Azure Diagnostics data from a worker role, web role, or virtual machine in Azure. This information can be sent to the Log Analytics service.

## Define Data Sources

Data sources are the different data collected from each connected source. Data sources can include events and performance data from Windows and Linux agents. Data sources can also include data like IIS logs and custom text logs. You must configure each data source that you want to collect from.



When you configure the Log Analytics settings, the available data sources are shown. Data sources include: Windows Event Logs, Windows Performance Counters, Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs, and Syslog. Each data source has additional configuration options. For example, the Windows Event Log can be configured to forward Error, Warning, or Informational messages.

The screenshot shows the 'Data Sources' section of the Log Analytics portal. The 'Data' category is selected and highlighted with a red box. Under 'Data Sources', 'Windows Event Logs' is also highlighted with a red box. On the right, there's a table for collecting event logs from Application, Operators Manager, and System logs.

## Visualize Log Analytics Data

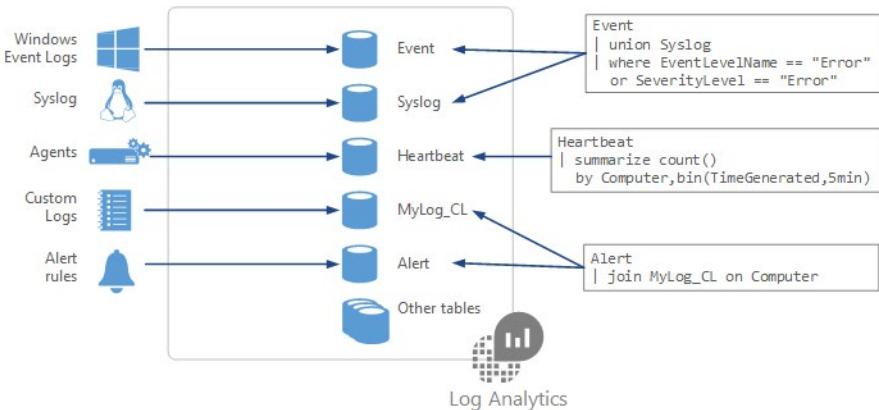
Log Analytics provides a query syntax to quickly retrieve and consolidate data in the repository. You can create and save Log Searches to directly analyze data in the portal or have log searches run automatically to create an alert if the results of the query indicate an important condition.



To give a quick graphical view of the health of your overall environment, you can add visualizations for saved log searches to your dashboard. To analyze data outside of Log Analytics, you can export the data from the repository into tools such as Power BI or Excel. You can also use the Log Search API to build custom solutions.

## Structure Log Analytics Queries

When you build a query, you start by determining which tables have the data that you're looking for. Each data source and solution stores its data in dedicated tables in the Log Analytics workspace. Documentation for each data source and solution includes the name of the data type that it creates and a description of each of its properties. Many queries will only require data from a single table, but others may use a variety of options to include data from multiple tables.



Some common query tables are: Event, Syslog, Heartbeat, and Alert.

The basic structure of a query is a source table followed by a series of operators separated by a pipe character |. You can chain together multiple operators to refine the data and perform advanced functions. For example, this query returns a count of the top 10 errors in the Event log during the last day. The results are in descending order.

```
Event
| where (EventLevelName == "Error")
| where (TimeGenerated > ago(1days))
| summarize ErrorCode = count() by Computer
| top 10 by ErrorCode desc
```

Some common operators are:

- **count** - Returns the number of records in the input record set.

```
StormEvents | count
```

- **limit** - Return up to the specified number of rows.

```
T | limit 5
```

- **summarize** - Produces a table that aggregates the content of the input table.

```
T | summarize count(), avg(price) by fruit, supplier
```

- **top** - Returns the first N records sorted by the specified columns.

```
T | top 5 by Name desc nulls last
```

- **where** - Filters a table to the subset of rows that satisfy a predicate.

```
T | where fruit=="apple"
```

For more information, [Azure Monitor log queries<sup>21</sup>](https://docs.microsoft.com/azure/azure-monitor/log-query/query-language)

<sup>21</sup> <https://docs.microsoft.com/azure/azure-monitor/log-query/query-language>

# Demonstration - Log Analytics

In this demonstration, you will work with the Log Analytics query language.

## Access the demonstration environment

1. Access the **Log Analytics Querying Demonstration**<sup>22</sup> page.
2. This page provides a live demonstration workspace where you can run and test queries.

## Use the Query Explorer

1. Select **Query Explorer** (top right).
2. Expand **Favorites** and then select **All Syslog records with errors**.
3. Notice the query is added to the editing pane. Notice the structure of the query.
4. **Run** the query. Explore the records returned.
5. As you have time experiment with other **Favorites** and also **Saved Queries**.

**Note:** Is there a particular query you are interested in?

## Knowledge check

Choose the best response for each question.

### Multiple choice

*How does Azure Monitor organize log data for queries?*

- Azure Monitor organizes log data into tables.
- Azure Monitor organizes log data into tabular operators.
- Azure Monitor organizes log data into the Kusto Query Language.

### Multiple choice

*Your organization has a very large web farm with more than 100 virtual machines. You would like to use Log Analytics to ensure these machines are responding to requests. You plan to automate the process, so you create a search query. You begin the query by identifying the source table. Which source table do you use? Select one.*

- Event
- SysLog
- Heartbeat

---

<sup>22</sup> <https://portal.loganalytics.io/demo>

## Multiple choice

Your organization has several Linux virtual machines. You would like to use Log Analytics to retrieve error messages for these machines. You plan to automate the process, so you create a search query. You begin the query by identifying the source table. Which source table do you use? Select one.

- SysLog
- Heartbeat
- Alert

## Summary and Resources

### Summary

Azure Administrators use the Log Analytics tool to run log queries on data in Azure Monitor Logs.

You should now be able to: In this module, you learned about Log Analytics including:

- Identify the features and usage cases for Log Analytics.
- Create a Log Analytics workspace and configure connected and data sources.
- Structure a Log Analytics query and review results.

### Learn more

You can learn more by reviewing the following.

- **Overview of Log Analytics in Azure Monitor<sup>23</sup>**
- **Log Analytics tutorial<sup>24</sup>**
- **Learn - Analyze your Azure infrastructure by using Azure Monitor logs<sup>25</sup>**
- **Learn - Monitor performance of virtual machines by using Azure Monitor for VMs<sup>26</sup>**

<sup>23</sup> <https://docs.microsoft.com/azure/azure-monitor/logs/log-analytics-overview>

<sup>24</sup> <https://docs.microsoft.com/azure/azure-monitor/logs/log-analytics-tutorial>

<sup>25</sup> <https://docs.microsoft.com/learn/modules/analyze-infrastructure-with-azure-monitor-logs/>

<sup>26</sup> <https://docs.microsoft.com/en-us/learn/modules/monitor-performance-using-azure-monitor-for-vms/>

# Configure Network Watcher

## Introduction

### Scenario

You can create complex and flexible setups in Azure that connect many virtual machines (VMs) to meet your needs. Just like in an on-premises network, configuration errors can result in problems that are challenging to troubleshoot. When you have to diagnose network problems in Azure, use Azure Network Watcher.

Suppose you have deployed a VM in Azure, and the VM has network connectivity issues. You want to learn how to troubleshoot and fix the problem so that you can help your colleagues to do the same, if they face similar issues in the future.

Administrators use Network Watcher to monitor, diagnose, and gain insight into their network health and performance with metrics. The elements can be broken down into four areas: monitoring, network diagnostic tools, metrics, and logs. Additionally, Network Watcher provides tools for troubleshooting connection problems.

### Skills measured

Network watcher is part of **Exam AZ-104: Microsoft Azure Administrator<sup>27</sup>**.

Configure and manage virtual networking (25–30%)

Monitor and troubleshoot virtual networking

- Configure and use Network Performance Monitor.
- Configure Azure Network Watcher.

### Learning objectives

In this module, you will learn how to:

- Identify the features and usage cases for Azure Network Watcher.
- Configure diagnostic capabilities like IP Flow Verify, Next Hop, and Network Topology.

### Prerequisites

None.

## Describe Network Watcher Features

**Network Watcher** provides tools to **monitor**, **diagnose**, view **metrics**, and enable or disable **logs** for resources in an Azure virtual network. Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level.

- **Automate remote network monitoring with packet capture.** Monitor and diagnose networking issues without logging in to your virtual machines (VMs) using Network Watcher. Trigger packet

---

<sup>27</sup> <https://docs.microsoft.com/learn/certifications/exams/az-104>

capture by setting alerts, and gain access to real-time performance information at the packet level. When you observe an issue, you can investigate in detail for better diagnoses.

- **Gain insight into your network traffic using flow logs.** Build a deeper understanding of your network traffic pattern using Network Security Group flow logs. Information provided by flow logs helps you gather data for compliance, auditing and monitoring your network security profile.
- **Diagnose VPN connectivity issues.** Network Watcher provides you the ability to diagnose your most common VPN Gateway and Connections issues. Allowing you, not only, to identify the issue but also to use the detailed logs created to help further investigate.



**Verify IP Flow:** Quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment. For example, confirming if a security rule is blocking ingress or egress traffic to or from a virtual machine. IP flow verify is ideal for making sure security rules are being correctly applied. When used for troubleshooting, if IP flow verify doesn't show a problem, you will need to explore other areas such as firewall restrictions.

**Next Hop:** To determine if traffic is being directed to the intended destination by showing the next hop. This will help determine if networking routing is correctly configured. Next hop also returns the route table associated with the next hop. If the route is defined as a user-defined route, that route is returned. Otherwise, next hop returns System Route. Depending on your situation the next hop could be Internet, Virtual Appliance, Virtual Network Gateway, VNet Local, VNet Peering, or None. None lets you know that while there may be a valid system route to the destination, there is no next hop to route the traffic to the destination. When you create a virtual network, Azure creates several default outbound routes for network traffic. The outbound traffic from all resources, such as VMs, deployed in a virtual network, are routed based on Azure's default routes. You might override Azure's default routes or create additional routes.

**VPN Diagnostics:** Troubleshoot gateways and connections. VPN Diagnostics returns a wealth of information. Summary information is available in the portal and more detailed information is provided in log files. The log files are stored in a storage account and include things like connection statistics, CPU and memory information, IKE security errors, packet drops, and buffers and events.

**NSG Flow Logs:** NSG Flow Logs maps IP traffic through a network security group. These capabilities can be used in security compliance and auditing. You can define a prescriptive set of security rules as a model for security governance in your organization. A periodic compliance audit can be implemented in a programmatic way by comparing the prescriptive rules with the effective rules for each of the VMs in your network.

**Connection Troubleshoot.** Azure Network Watcher Connection Troubleshoot is a more recent addition to the Network Watcher suite of networking tools and capabilities. Connection Troubleshoot enables you to troubleshoot network performance and connectivity issues in Azure.

**Note:** To use Network Watcher, you must be an Owner, Contributor, or Network Contributor. If you create a custom role, the role must be able to read, write, and delete the Network Watcher.

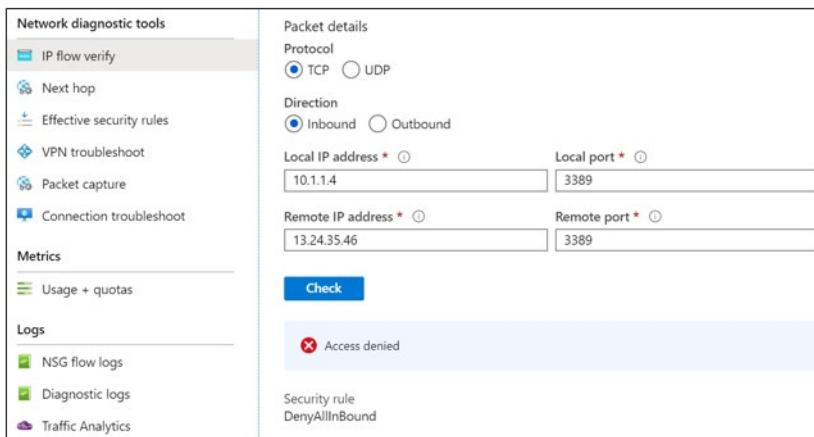
## Review IP Flow Verify Diagnostics

**IP Flow Verify Purpose:** Checks if a packet is allowed or denied to or from a virtual machine. For example, confirming if a security rule is blocking ingress or egress traffic to or from a virtual machine.

### Example

When you deploy a VM, Azure applies several default security rules to the VM. These rules allow or deny traffic to or from the VM. You might override Azure's default rules or create additional rules. At some point, a VM may become unable to communicate with other resources, because of a security rule.

The IP Flow Verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP Flow Verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP Flow Verify identifies which security rule allowed or denied the communication. With this information, you can then resolve the problem.



**Note:** IP Flow Verify is ideal for making sure security rules are being correctly applied. When used for troubleshooting, if IP Flow Verify doesn't show a problem, you will need to explore other areas such as firewall restrictions.

## Review Next Hop Diagnostics

**Next Hop Purpose:** To determine if traffic is being directed to the intended destination. Next hop information will help determine if network routing is correctly configured.

When you create a virtual network, Azure creates several default outbound routes for network traffic. The outbound traffic from all resources, such as VMs, deployed in a virtual network, are routed based on Azure's default routes. You might override Azure's default routes or create additional routes.

### Example

You may find that a VM can no longer communicate with other resources because of a specific route. The next hop capability enables you to specify a source and destination IPv4 address. Next hop then tests the communication and informs you what type of next hop is used to route the traffic. You can then remove, change, or add a route, to resolve a routing problem.

Subscription \* ⓘ  
MSDN Platforms Subscription

Resource group \* ⓘ  
Demo

Virtual machine \* ⓘ  
vm01

Network interface \* ⓘ  
vm01165

Source IP address \* ⓘ  
10.1.1.4

Destination IP address \* ⓘ  
13.24.35.46

**Next hop**

Result  
Next hop type  
**None**

IP address  
**10.1.1.100**

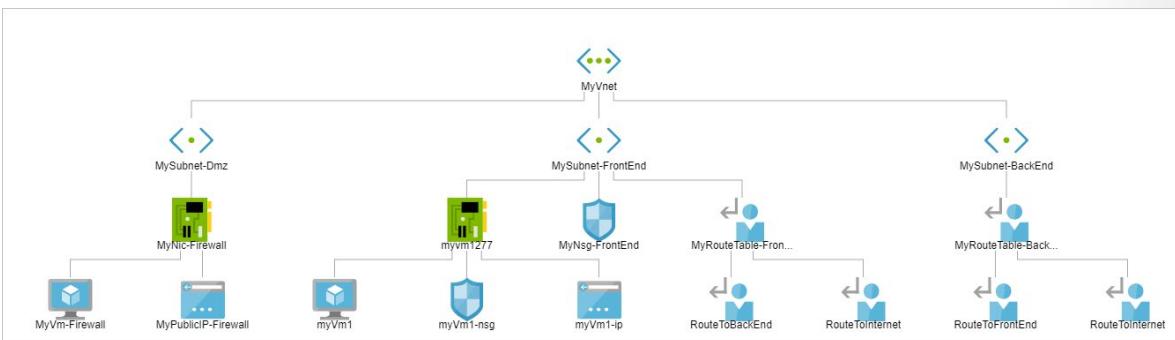
Route table ID  
</subscriptions/2301e3a0-8420-...>

Next Hop also returns the route table associated with the next hop. If the route is defined as a user-defined route, that route is returned. Otherwise, Next Hop returns the system route. Depending on your situation, the next hop could be the Internet, Virtual Appliance, Virtual Network Gateway, VNet Local, VNet Peering, or None. A returned value of None lets you know that there may be a valid system route to the destination, there is no next hop to route the traffic to the destination.

## Visualize the Network Topology

Suppose you have to troubleshoot a virtual network created by your colleagues. Unless you were involved in the creation process of the network, you might not know about all the aspects of the infrastructure. You can use the topology tool to visualize and understand the infrastructure you're dealing with before you start troubleshooting.

Network Watcher's Topology capability enables you to generate a visual diagram of the resources in a virtual network, and the relationships between the resources. The following picture shows an example topology diagram for a virtual network that has three subnets, two VMs, network interfaces, public IP addresses, network security groups, route tables, and the relationships between the resources:



The topology tool generates a graphical display of your Azure virtual network, its resources, its interconnections, and their relationships with each other.

**Note:** To generate the topology, you need a Network Watcher instance in the same region as the virtual network.

## Knowledge check

Choose the best response for each question.

### Multiple choice

*You are analyzing the company virtual network and think it would be helpful to get a visual representation of the networking elements. Which feature can you use? Select one.*

- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology

### Multiple choice

*Your company has a website and users are reporting connectivity errors and timeouts. You suspect that a security rule may be blocking traffic to or from one of the virtual machines. You need to quickly troubleshoot the problem, so you do which of the following? Select one.*

- Use Network Watcher's VPN Diagnostics feature.
- Use Network Watcher's IP Flow Verify feature.
- Configure Windows performance counters and use Performance Monitor.

### Multiple choice

*To capture traffic on a VM, Azure Network Watcher requires:*

- An Azure storage account
- Azure Traffic Manager
- Network Watcher Agent VM Extension

## Summary and Resources

### Summary

Azure Network Watcher provides the tools you need to monitor, troubleshoot, and optimize your network infrastructure.

You should now be able to:

- Identify the features and usage cases for Azure Network Watcher.
- Configure diagnostic capabilities like IP Flow Verify, Next Hop, and Effective Security Rules.

## Learn more

You can learn more by reviewing the following.

- **Azure Network Watcher documentation<sup>28</sup>**
- **Network Performance Monitor solution in Azure<sup>29</sup>**
- **Learn - Monitor and troubleshoot your end-to-end Azure network infrastructure by using network monitoring tools<sup>30</sup>**

---

<sup>28</sup> <https://docs.microsoft.com/azure/network-watcher/>

<sup>29</sup> <https://docs.microsoft.com/azure/azure-monitor/insights/network-performance-monitor>

<sup>30</sup> <https://docs.microsoft.com/learn/modules/troubleshoot-azure-network-infrastructure/>

# Module 11 Lab

## Lab 11 - Implement Monitoring

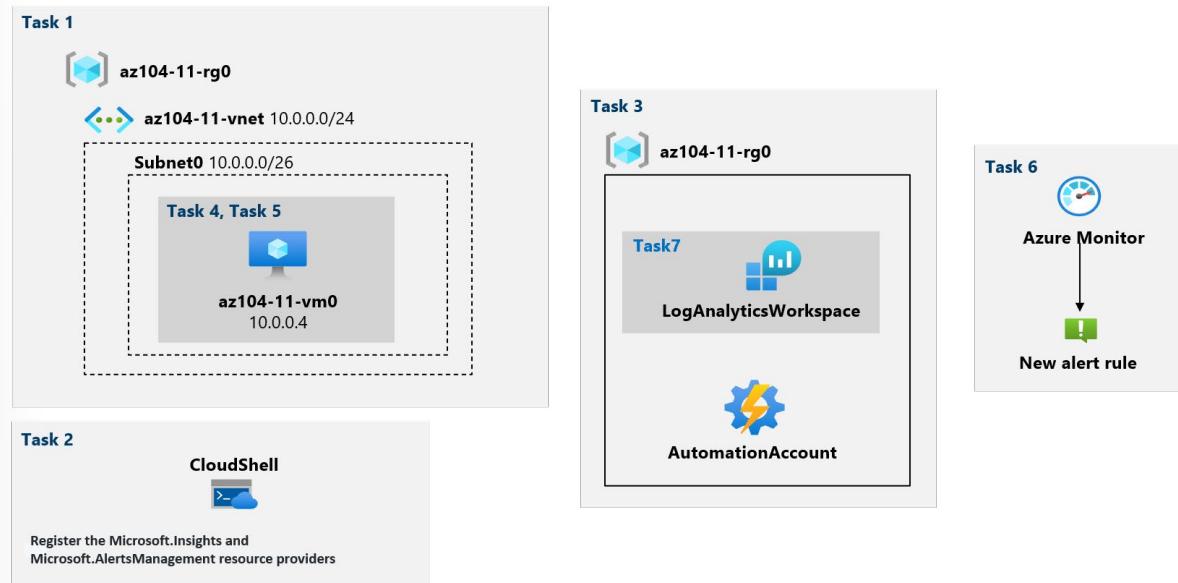
### Lab scenario

You need to evaluate Azure functionality that would provide insight into performance and configuration of Azure resources, focusing in particular on Azure virtual machines. To accomplish this, you intend to examine the capabilities of Azure Monitor, including Log Analytics.

### Objectives

In this lab, you will:

- Task 1: Provision the lab environment.
- Task 2: Create and configure an Azure Log Analytics workspace and Azure Automation-based solutions.
- Task 3: Review default monitoring settings of Azure virtual machines.
- Task 4: Configure Azure virtual machine diagnostic settings.
- Task 5: Review Azure Monitor functionality.
- Task 6: Review Azure Log Analytics functionality.



**Note:** Consult with your instructor for how to access the lab instructions and lab environment (if provided).

# Answers

## Multiple choice

You need to determine who deleted a network security group through Resource Manager. You are viewing the Activity Log when another Azure Administrator says you should use this event category to narrow your search. Select one.

- Administrative
- Service Health
- Policy

### Explanation

*Administrative. This category contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of the types of events you would observe in this category include "create virtual machine" and "delete network security group". The Administrative category also includes any changes to role-based access control in a subscription.*

## Multiple choice

What is the shared underlying logging data platform for Azure Sentinel and Azure Security Center?

- Activity Logs
- Azure Monitor Logs
- Diagnostic Settings

### Explanation

*Azure Monitor Logs. Several services in Azure including Sentinel and Security Center use Azure Monitor Logs as their underlying logging data platform.*

## Multiple choice

What data does Azure Monitor collect?

- Data from a variety of sources, such as the application event log, the operating system (Windows and Linux), Azure resources, and custom data sources
- Azure billing details
- Backups of database transaction logs

### Explanation

*Data from a variety of sources, such as the application event log, the operating system (Windows and Linux), Azure resources, and custom data sources.*

## Multiple choice

What two fundamental types of data does Azure Monitor collect?

- Metrics and logs
- Username and password
- Email notifications and errors

### Explanation

*Metrics and logs. Azure Monitor collects two types of data: metrics and logs. Metrics are numerical values that describe some aspect of a system at a particular time. Logs contain different kinds of data, such as event information, organized into records.*

**Multiple choice**

Your organization has an app that is used across the business. The performance of this app is critical to day-to-day operations. Because the app is so important, four IT administrators have been identified to address any issues. You have configured an alert and need to ensure the administrators are notified if there is a problem. In which area of the portal will you provide the administrator email addresses? Select one.

- Activity log
- Performance group
- Action Group

*Explanation*

*Action Group. When creating the alert, you will select Email as the Action Type. You will then be able to provide the administrator email addresses as part of the Action Group.*

**Multiple choice**

You are reviewing the Alerts page and notice an alert has been Acknowledged. What does this mean? Select one.

- An administrator has reviewed the alert and started working on it.
- The issue has been resolved.
- The issue has been closed.

*Explanation*

*An administrator has reviewed the alert and started working on it. An alert status of Acknowledged means an administrator has reviewed the alert and started working on it. Alert state is different and independent of the monitor condition. Alert state is set by the user. Monitor condition is set by the system.*

**Multiple choice**

What's the composition of an alert rule? Select one.

- Resource, condition, log, alert type
- Metrics, logs, application, operating system
- Resource, condition, actions, alert details

*Explanation*

*Resource, condition, actions, alert details. These elements make up an alert rule.*

**Multiple choice**

Which of the following is an example of a log data type?

- HTTP response records
- Percentage of CPU over time
- Website requests per hour

*Explanation*

*HTTP response records. HTTP response records are examples of log data types.*

**Multiple choice**

How does Azure Monitor organize log data for queries?

- Azure Monitor organizes log data into tables.
- Azure Monitor organizes log data into tabular operators.
- Azure Monitor organizes log data into the Kusto Query Language.

*Explanation*

Azure Monitor organizes log data into tables. Azure Monitor organizes log data in tables, each composed of multiple columns. Every query contains data that's organized into a hierarchy similar to SQL (databases, tables, and columns).

**Multiple choice**

Your organization has a very large web farm with more than 100 virtual machines. You would like to use Log Analytics to ensure these machines are responding to requests. You plan to automate the process, so you create a search query. You begin the query by identifying the source table. Which source table do you use? Select one.

- Event
- SysLog
- Heartbeat

*Explanation*

The Heartbeat table will help you identify computers that haven't had a heartbeat in a specific time frame, for example, the last six hours.

**Multiple choice**

Your organization has several Linux virtual machines. You would like to use Log Analytics to retrieve error messages for these machines. You plan to automate the process, so you create a search query. You begin the query by identifying the source table. Which source table do you use? Select one.

- SysLog
- Heartbeat
- Alert

*Explanation*

Syslog is an event logging protocol that is common to Linux. Syslog includes information such as error messages.

**Multiple choice**

You are analyzing the company virtual network and think it would be helpful to get a visual representation of the networking elements. Which feature can you use? Select one.

- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology

*Explanation*

Network Watcher's Topology feature provides a visual representation of your networking elements.

**Multiple choice**

Your company has a website and users are reporting connectivity errors and timeouts. You suspect that a security rule may be blocking traffic to or from one of the virtual machines. You need to quickly troubleshoot the problem, so you do which of the following? Select one.

- Use Network Watcher's VPN Diagnostics feature.
- Use Network Watcher's IP Flow Verify feature.
- Configure Windows performance counters and use Performance Monitor.

*Explanation*

*IP Flow Verify. Diagnosing connectivity issues is ideal for Network Watcher's IP Flow Verify feature. The IP Flow Verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP Flow Verify then tests the communication and informs you if the connection succeeds or fails.*

**Multiple choice**

To capture traffic on a VM, Azure Network Watcher requires:

- An Azure storage account
- Azure Traffic Manager
- Network Watcher Agent VM Extension

*Explanation*

*Network Watcher Agent VM Extension. The Network Watcher Agent VM Extension is required when you capture traffic on a VM. It's automatically installed when you start a packet capture session in the Azure portal.*