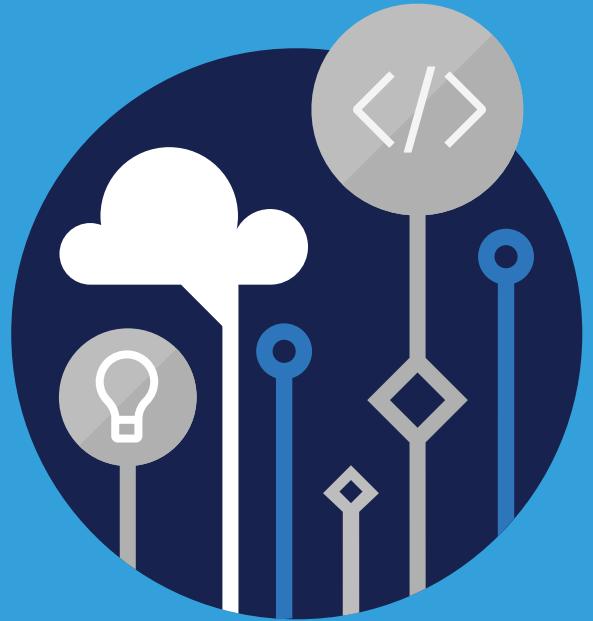


Microsoft
Official
Course



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 IT Academy 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 facility 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, or (iii) a Microsoft full-time employee.
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 and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.
8. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.
9. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
10. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.
11. "MPN Member" means an active Microsoft Partner Network program member in good standing.
12. "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.
13. "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.

14. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.
 15. "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 IT Academy 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, **provided you comply with the following:**
 3. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 4. 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,
 5. 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,
 6. 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,

7. 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,
8. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
9. 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 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 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, **provided you comply with the following:**
 3. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
 4. you will ensure that each End User attending a Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
 5. 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,
 6. 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,
 7. 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,
 8. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
 9. you will only provide access to the Trainer Content to MCTs.

MCT USE ONLY. STUDENT USE PROHIBITED

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, **provided you comply with the following:**

3. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
4. you will ensure that each End User attending a Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
5. 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,
6. you will ensure that each Trainer teaching a Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,
7. 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,
8. 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,
9. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
10. 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. 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. 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 a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member 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 "as is", we may not 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 des 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 contre-façon 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 November 2014



Contents

■	Module 0 Start Here	1
	Start Here	1
■	Module 1 Identity	11
	Azure Active Directory	11
	Users and Groups	20
	Module 01 Lab and Review	28
■	Module 2 Governance and Compliance	35
	Subscriptions and Accounts	35
	Azure Policy	43
	Role-Based Access Control	50
	Module 02 Lab and Review Questions	56
■	Module 3 Azure Administration	63
	Azure Resource Manager	63
	Azure Portal and Cloud Shell	71
	Azure PowerShell and CLI	76
	ARM Templates	82
	Module 03 Lab and Review	91
■	Module 4 Virtual Networking	97
	Virtual Networks	97
	IP Addressing	102
	Network Security Groups	105
	Azure Firewall	111
	Azure DNS	114
	Module 04 Lab and Review	123
■	Module 5 Intersite Connectivity	135
	VNet Peering	135
	VPN Gateway Connections	141
	ExpressRoute Connections	149
	Module 05 Lab and Review	155
■	Module 6 Network Traffic Management	165
	Network Routing and Endpoints	165
	Azure Load Balancer	175

Azure Application Gateway	181
Azure Traffic Manager	185
Module 06 Lab and Review	190
Module 7 Azure Storage	199
Storage Accounts	199
Blob Storage	209
Storage Security	215
Azure Files and File Sync	222
Managing Storage	231
Module 07 Lab and Review	241
Module 8 Azure Virtual Machines	253
Virtual Machine Planning	253
Creating Virtual Machines	262
Virtual Machine Availability	268
Virtual Machine Extensions	276
Module 08 Lab and Review Questions	280
Module 9 Serverless Computing	289
Azure App Service Plans	289
Azure App Services	295
Container Services	307
Azure Kubernetes Service	312
Module 09 Lab and Review	328
Module 10 Data Protection	337
File and Folder Backups	337
Virtual Machine Backups	345
Module 10 Lab and Review Questions	355
Module 11 Monitoring	361
Azure Monitor	361
Azure Alerts	367
Log Analytics	372
Network Watcher	379
Module 11 Lab and Review Questions	387

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 on operating systems, virtualization, cloud infrastructure, storage structures, and networking.

- Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.
- Understanding of network configuration, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- Understanding of Active Directory concepts, including domains, forests, domain controllers, replication, Kerberos protocol, and Lightweight Directory Access Protocol (LDAP).
- Understanding of resilience and disaster recovery, including backup and restore operations.

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 module review questions.

Module 01 - Identity

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

- Azure Active Directory
- Users and Groups
- Lab 01 - Manage Azure Active Directory Identities

Module 02 – 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:

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

Module 03 – Azure Administration

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:

- Resource Manager
- Azure Portal and Cloud Shell
- Azure PowerShell and CLI
- 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
- Lab 03d - Manage Azure resources by Using Azure CLI

Module 04 – 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:

- Virtual Networks
- IP Addressing
- Network Security groups
- Azure Firewall
- Azure DNS
- Lab 04 - Implement Virtual Networking

Module 05 – 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:

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

Module 06 – 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:

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

Module 07 – 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:

- Storage Accounts
- Blob Storage
- Storage Security
- Azure Files and File Sync
- Managing Storage
- Lab 07 - Manage Azure storage

Module 08 – Azure Virtual Machines

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

- Virtual Machine Planning
- Creating Virtual Machines
- Virtual Machine Availability
- Virtual Machine Extensions
- Lab 08 - Manage Virtual Machines

Module 09 - Serverless Computing

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

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

Module 10 – Data Protection

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

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

Module 11 – Monitoring

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

- Azure Monitor
- Azure Alerts

- Log Analytics
- Network Watcher
- Lab 11 - Implement Monitoring

AZ-104 Certification Exam

The AZ-104, **Microsoft Azure Administrator¹**, 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	10-15%
Deploy and manage Azure compute resources	25-30%
Configure and manage virtual networking	30-35%
Monitor and backup Azure resources	10-15%

Microsoft Learn

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can also search for additional content that might be helpful.

Module 01 - Identity

- [Create Azure users and groups in Azure Active Directory²](#)
- [Manage users and groups in Azure Active Directory³](#)
- [Secure your Azure resources with role-based access control⁴](#)
- [Secure Azure Active Directory users with Multi-Factor Authentication⁵](#)
- [Allow users to reset their password with Azure Active Directory self-service password reset⁶](#)
- [Secure your application by using OpenID Connect and Azure AD⁷](#)

Module 02 - Governance and Compliance

- [Analyze costs and create budgets with Azure Cost Management⁸](#)

¹ <https://www.microsoft.com/en-us/learning/exam-AZ-103.aspx>

² <https://docs.microsoft.com/en-us/learn/modules/create-users-and-groups-in-azure-active-directory/>

³ <https://docs.microsoft.com/en-us/learn/modules/manage-users-and-groups-in-aad/>

⁴ <https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/>

⁵ <https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/>

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

⁷ <https://docs.microsoft.com/en-us/learn/modules/secure-app-with-oidc-and-azure-ad/>

⁸ <https://docs.microsoft.com/en-us/learn/modules/analyze-costs-create-budgets-azure-cost-management/>

- Predict costs and optimize spending for Azure⁹
- Control and organize Azure resources with Azure Resource Manager¹⁰
- Apply and monitor infrastructure standards with Azure Policy¹¹
- Create custom roles for Azure resources with role-based access control¹²
- Manage access to an Azure subscription by using Azure role-based access control¹³
- Secure your Azure resources with role-based access control¹⁴

Module 03 - Azure Administration

- Core Cloud Services - Manage services with the Azure portal¹⁵
- Control and organize Azure resources with Azure Resource Manager¹⁶
- Build Azure Resource Manager templates¹⁷
- Automate Azure tasks using scripts with PowerShell¹⁸
- Manage virtual machines with the Azure CLI¹⁹

Module 04 - Virtual Networking

- Networking Fundamentals - Principles²⁰
- Design an IP addressing schema for your Azure deployment²¹
- Secure and isolate access to Azure resources by using network security groups and service endpoints²²

Module 05 - Intersite Connectivity

- Distribute your services across Azure virtual networks and integrate them by using virtual network peering²³
- Connect your on-premises network to Azure with VPN Gateway²⁴
- Connect your on-premises network to the Microsoft global network by using ExpressRoute²⁵

⁹ <https://docs.microsoft.com/en-us/learn/modules/predict-costs-and-optimize-spending/>

¹⁰ <https://docs.microsoft.com/en-us/learn/modules/control-and-organize-with-azure-resource-manager/>

¹¹ <https://docs.microsoft.com/en-us/learn/modules/intro-to-governance/>

¹² <https://docs.microsoft.com/en-us/learn/modules/create-custom-azure-roles-with-rbac/>

¹³ <https://docs.microsoft.com/en-us/learn/modules/manage-subscription-access-azure-rbac/>

¹⁴ <https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/>

¹⁵ <https://docs.microsoft.com/en-us/learn/modules/tour-azure-portal/>

¹⁶ <https://docs.microsoft.com/en-us/learn/modules/control-and-organize-with-azure-resource-manager/>

¹⁷ <https://docs.microsoft.com/en-us/learn/modules/build-azure-vm-templates/>

¹⁸ <https://docs.microsoft.com/en-us/learn/modules/automate-azure-tasks-with-powershell/>

¹⁹ <https://docs.microsoft.com/en-us/learn/modules/manage-virtual-machines-with-azure-cli/>

²⁰ <https://docs.microsoft.com/en-us/learn/modules/network-fundamentals/>

²¹ <https://docs.microsoft.com/en-us/learn/modules/design-ip-addressing-for-azure/>

²² <https://docs.microsoft.com/en-us/learn/modules/secure-and-isolate-with-nsg-and-service-endpoints/>

²³ <https://docs.microsoft.com/en-us/learn/modules/integrate-vnets-with-vnet-peering/>

²⁴ <https://docs.microsoft.com/en-us/learn/modules/connect-on-premises-network-with-vpn-gateway/>

²⁵ <https://docs.microsoft.com/en-us/learn/modules/connect-on-premises-network-with-expressroute/>

Module 06 - Network Traffic Management

- Manage and control traffic flow in your Azure deployment with routes²⁶
- Improve application scalability and resiliency by using Azure Load Balancer²⁷
- Load balance your web service traffic with Application Gateway²⁸
- Enhance your service availability and data locality by using Azure Traffic Manager²⁹

Module 07 - Azure Storage

- Create an Azure Storage account³⁰
- Secure your Azure Storage³¹
- Optimize storage performance and costs using Blob storage tiers³²
- Make your application storage highly available with read-access geo-redundant storage³³
- Copy and move blobs from one container or storage account to another from the command line and in code³⁴
- Move large amounts of data to the cloud by using Azure Data Box family³⁵
- Monitor, diagnose, and troubleshoot your Azure storage³⁶

Module 08 - Azure Virtual Machines

- Build a scalable application with virtual machine scale sets³⁷
- Deploy Azure virtual machines from VHD templates³⁸
- Choose the right disk storage for your virtual machine workload³⁹
- Add and size disks in Azure virtual machines⁴⁰
- Protect your virtual machine settings with Azure Automation State Configuration⁴¹

Module 09 - Serverless Computing

- Host a web application with Azure App service⁴²
- Stage a web app deployment for testing and rollback by using App Service deployment slots⁴³

²⁶ <https://docs.microsoft.com/en-us/learn/modules/control-network-traffic-flow-with-routes/>

²⁷ <https://docs.microsoft.com/en-us/learn/modules/improve-app-scalability-resiliency-with-load-balancer/>

²⁸ <https://docs.microsoft.com/en-us/learn/modules/load-balance-web-traffic-with-application-gateway/>

²⁹ <https://docs.microsoft.com/en-us/learn/modules/distribute-load-with-traffic-manager/>

³⁰ <https://docs.microsoft.com/en-us/learn/modules/create-azure-storage-account/>

³¹ <https://docs.microsoft.com/en-us/learn/modules/secure-azure-storage-account/>

³² <https://docs.microsoft.com/en-us/learn/modules/optimize-archive-costs-blob-storage/>

³³ <https://docs.microsoft.com/en-us/learn/modules/ha-application-storage-with-grs/>

³⁴ <https://docs.microsoft.com/en-us/learn/modules/copy-blobs-from-command-line-and-code/>

³⁵ <https://docs.microsoft.com/en-us/learn/modules/move-data-with-azure-data-box/>

³⁶ <https://docs.microsoft.com/en-us/learn/modules/monitor-diagnose-and-troubleshoot-azure-storage/>

³⁷ <https://docs.microsoft.com/en-us/learn/modules/build-app-with-scale-sets/>

³⁸ <https://docs.microsoft.com/en-us/learn/modules/deploy-vms-from-vhd-templates/>

³⁹ <https://docs.microsoft.com/en-us/learn/modules/choose-the-right-disk-storage-for-vm-workload/>

⁴⁰ <https://docs.microsoft.com/en-us/learn/modules/add-and-size-disks-in-azure-virtual-machines/>

⁴¹ <https://docs.microsoft.com/en-us/learn/modules/protect-vm-settings-with-dsc/>

⁴² <https://docs.microsoft.com/en-us/learn/modules/host-a-web-app-with-azure-app-service/>

⁴³ <https://docs.microsoft.com/en-us/learn/modules/stage-deploy-app-service-deployment-slots/>

- **Scale an App Service web app to efficiently meet demand with App Service scale up and scale out⁴⁴**
- **Dynamically meet changing web app performance requirements with autoscale rules⁴⁵**
- **Capture and view page load times in your Azure web app with Application Insights⁴⁶**
- **Run Docker containers with Azure Container Instances⁴⁷**
- **Introduction to the Azure Kubernetes Service⁴⁸**

Module 10 - Data Protection

- **Protect your virtual machines by using Azure Backup⁴⁹**
- **Back up and restore your Azure SQL database⁵⁰**
- **Protect your Azure infrastructure with Azure Site Recovery⁵¹**
- **Protect your on-premises infrastructure from disasters with Azure Site Recovery⁵²**

Module 11 - Monitoring

- **Analyze your Azure infrastructure by using Azure Monitor logs⁵³**
- **Improve incident response with alerting on Azure⁵⁴**
- **Monitor the health of your Azure virtual machine by collecting and analyzing diagnostic data⁵⁵**
- **Monitor, diagnose, and troubleshoot your Azure storage⁵⁶**

✓ These links are also found at the end of each Module.

Additional Study Resources

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

- **Azure forums⁵⁷**. The Azure forums are very active. You can search the threads for a specific area of interest. You can also browse categories like Azure Storage, Pricing and Billing, Azure Virtual Machines, and Azure Migrate.
- **Microsoft Learning Community Blog⁵⁸**. Get the latest information about the certification tests and exam study groups.
- **Channel 9⁵⁹**. Channel 9 provides a wealth of informational videos, shows, and events.

⁴⁴ <https://docs.microsoft.com/en-us/learn/modules/app-service-scale-up-scale-out/>

⁴⁵ <https://docs.microsoft.com/en-us/learn/modules/app-service-autoscale-rules/>

⁴⁶ <https://docs.microsoft.com/en-us/learn/modules/capture-page-load-times-application-insights/>

⁴⁷ <https://docs.microsoft.com/en-us/learn/modules/run-docker-with-azure-container-instances/>

⁴⁸ <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-kubernetes-service/>

⁴⁹ <https://docs.microsoft.com/en-us/learn/modules/protect-virtual-machines-with-azure-backup/>

⁵⁰ <https://docs.microsoft.com/en-us/learn/modules/backup-restore-azure-sql/>

⁵¹ <https://docs.microsoft.com/en-us/learn/modules/protect-infrastructure-with-site-recovery/>

⁵² <https://docs.microsoft.com/en-us/learn/modules/protect-on-premises-infrastructure-with-azure-site-recovery/>

⁵³ <https://docs.microsoft.com/en-us/learn/modules/analyze-infrastructure-with-azure-monitor-logs/>

⁵⁴ <https://docs.microsoft.com/en-us/learn/modules/incident-response-with-alerting-on-azure/>

⁵⁵ <https://docs.microsoft.com/en-us/learn/modules/monitor-azure-vm-using-diagnostic-data/>

⁵⁶ <https://docs.microsoft.com/en-us/learn/modules/monitor-diagnose-and-troubleshoot-azure-storage/>

⁵⁷ <https://social.msdn.microsoft.com/Forums/en-US/home?category=windowsazureplatform>

⁵⁸ <https://www.microsoft.com/en-us/learning/community-blog.aspx>

⁵⁹ <https://channel9.msdn.com/>

- **Azure Tuesdays with Corey**⁶⁰. Corey Sanders answers your questions about Microsoft Azure - Virtual Machines, Web Sites, Mobile Services, Dev/Test etc.
- **Azure Fridays**⁶¹. Join Scott Hanselman as he engages one-on-one with the engineers who build the services that power Microsoft Azure, as they demo capabilities, answer Scott's questions, and share their insights.
- **Microsoft Azure Blog**⁶². Keep current on what's happening in Azure, including what's now in preview, generally available, news & updates, and more.
- **Azure Documentation**⁶³. Stay informed on the latest products, tools, and features. Get information on pricing, partners, support, and solutions.

60 <https://channel9.msdn.com/Shows/Tuesdays-With-Corey/>
61 <https://channel9.msdn.com/Shows/Azure-Friday>
62 <https://azure.microsoft.com/en-us/blog/>
63 <https://docs.microsoft.com/en-us/azure/>

MCT USE ONLY. STUDENT USE PROHIBITED

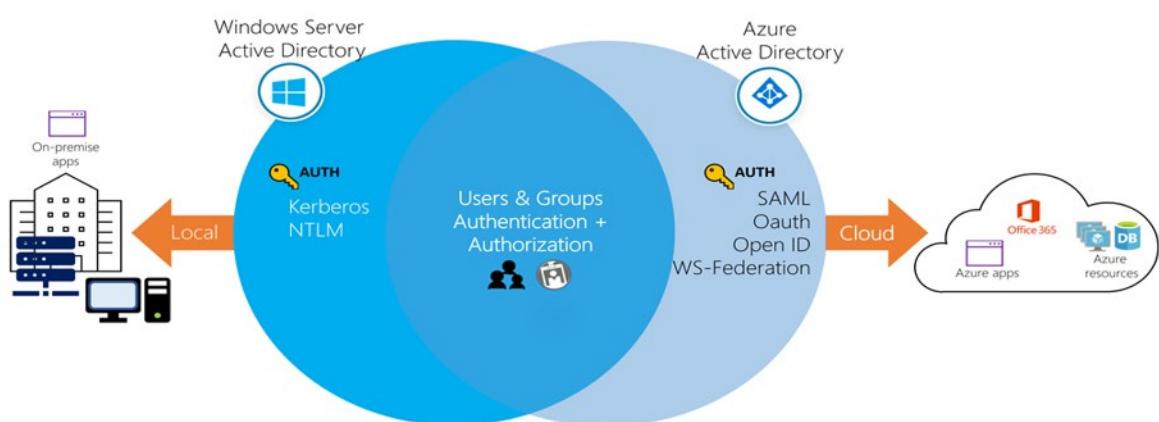
Module 1 Identity

Azure Active Directory

Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's multi-tenant cloud-based directory and identity management service. For IT Admins, Azure AD provides an affordable, easy to use solution to give employees and business partners single sign-on (SSO) access to thousands of cloud SaaS Applications like Office365, Salesforce, DropBox, and Concur.

For application developers, Azure AD lets you focus on building your application by making it fast and simple to integrate with a world class identity management solution used by millions of organizations around the world.



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 including Microsoft Office 365 and thousands of SaaS applications such as Salesforce, Workday, DocuSign, ServiceNow, and Box.
 - **Works with iOS, Mac OS X, Android, and Windows devices.** Users can launch applications from a personalized web-based access panel, mobile app, Office 365, or custom company portals using their existing work credentials—and have the same experience whether they're working on iOS, Mac OS X, 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.** Connect Active Directory and other on-premises directories to Azure Active Directory in just a few clicks and maintain a consistent set of users, groups, passwords, and devices across both environments.
 - **Protect sensitive data and applications.** Enhance application access security with unique identity protection capabilities that provide a consolidated view into suspicious sign-in activities and potential vulnerabilities. Take advantage of advanced security reports, notifications, remediation recommendations and risk-based policies to protect your business from current and future threats.
 - **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.
- ✓ If you are an Office365, Azure or Dynamics CRM Online customer, you might not realize that you are already using Azure AD. Every Office365, 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.

For more information, [Azure Active Directory Documentation¹](https://docs.microsoft.com/en-us/azure/active-directory/)

Azure AD Concepts

- **Identity.** A thing 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 cannot have an account without an identity.
- **Azure AD Account.** An identity created through Azure AD or another Microsoft cloud service, such as Office 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.** A dedicated and trusted instance of Azure AD that's automatically created when your organization signs up for a Microsoft cloud service subscription, such as Microsoft Azure, Microsoft Intune, or Office 365. An Azure tenant represents a single organization.

¹ <https://docs.microsoft.com/en-us/azure/active-directory/>

- **Azure AD directory.** Each Azure tenant has a dedicated and trusted Azure AD directory. The Azure AD directory includes the tenant's users, groups, and apps and is used to perform identity and access management functions for tenant resources.

AD DS vs 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).
 - ✓ 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.

Azure Active Directory Editions

Azure Active Directory comes in four editions—**Free**, **Office 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 Office 365 subscribers can also buy Azure Active Directory Premium P1 and P2 online.

Feature	Free	Office 365 Apps	Premium P1	Premium P2
Directory Objects	500,000	Unlimited	Unlimited	Unlimited
Single Sign-On	Up to 10 apps	Up to 10 apps	Unlimited	Unlimited

Feature	Free	Office 365 Apps	Premium P1	Premium P2
Core Identity and Access Management	X	X	X	X
Business to Business Collaboration	X	X	X	X
Identity & Access Management for Office 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, Office 365, and many popular SaaS apps.

Azure Active Directory Office 365 Apps. This edition is included with O365. In addition to the Free features, this edition provides Identity & Access Management for Office 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.

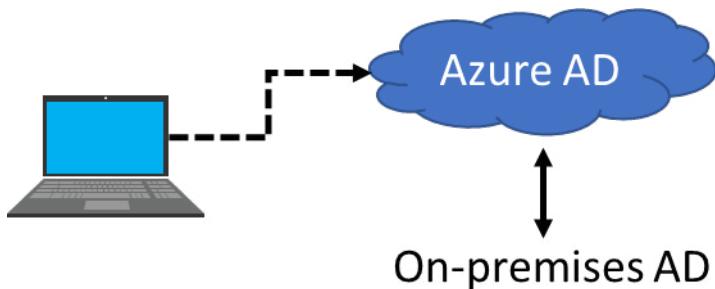
Azure Active Directory Premium P2. In addition to the Free and P1 features, P2 also offers Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators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

✓ The **Azure Active Directory Pricing**² page has detailed information on what is included in each of the editions. Based on the feature list which edition does your organization need?

Azure AD Join

Azure Active Directory (Azure AD) enables single sign-on to devices, apps, and services from anywhere. The proliferation of devices - including Bring Your Own Device (BYOD) – empowers end users to be productive wherever and whenever. But, IT administrators must ensure corporate assets are protected and that devices meet standards for security and compliance.

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



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 will not 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.
- **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. When a device is registered, 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. This means, it provides you with all the benefits of registering a device and in addition to this, 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.
- ✓ Registration combined with a mobile device management (MDM) solution such as Microsoft Intune, provides additional device attributes in Azure AD. This allows you to create conditional access rules that enforce access from devices to meet your standards for security and compliance.
- ✓ 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.

For more information, [Introduction to device management³](#)

³ <https://docs.microsoft.com/en-us/azure/active-directory/device-management-introduction>

Azure Multi-Factor Authentication

Azure Multi-Factor Authentication (MFA) helps safeguard access to data and applications while maintaining simplicity for users. It provides additional security by requiring a second form of authentication and delivers strong authentication through a range of easy to use authentication methods.

For organizations that need to be compliant with industry standards, such as PCI DSS version 3.2, MFA is a must have capability to authenticate users. Beyond being compliant with industry standards, enforcing MFA to authenticate users can also help organizations to mitigate credential theft attacks.



The security of MFA two-step verification lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the additional authentication method. Authentication methods include:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)

MFA Features

Get more security with less complexity. Azure MFA helps safeguard access to data and applications and helps to meet customer demand for a simple sign-in process. Get strong authentication with a range of easy verification options—phone call, text message, or mobile app notification—and allow customers to choose the method they prefer.

Mitigate threats with real-time monitoring and alerts. MFA helps protect your business with security monitoring and machine-learning-based reports that identify inconsistent sign-in patterns. To help mitigate potential threats, real-time alerts notify your IT department of suspicious account credentials.

Deploy on-premises or on Azure. Use MFA Server on your premises to help secure VPNs, Active Directory Federation Services, IIS web applications, Remote Desktop, and other remote access applications using RADIUS and LDAP authentication. Add an extra verification step to your cloud-based applications and services by turning on Multi-Factor Authentication in Azure Active Directory.

Use with Office 365, Salesforce, and more. MFA for Office 365 helps secure access to Office 365 applications at no additional cost. Multi-Factor Authentication is also available with Azure Active Directory Premium and thousands of software-as-a-service (SaaS) applications, including Salesforce, Dropbox, and other popular services.

Add protection for Azure administrator accounts. MFA adds a layer of security to your Azure administrator account at no additional cost. When it's turned on, you need to confirm your identity to create a virtual machine, manage storage, or use other Azure services.

Authentication Methods

Method	Description
Call to phone	Places an automated voice call. The user answers the call and presses # in the phone keypad to authenticate. The phone number is not synchronized to on-premises Active Directory. A voice call to phone is important because it persists through a phone handset upgrade, allowing the user to register the mobile app on the new device.
Text message to phone	Sends a text message that contains a verification code. The user is prompted to enter the verification code into the sign-in interface. This process is called one-way SMS. Two-way SMS means that the user must text back a particular code. Two-way SMS is deprecated and not supported after November 14, 2018. Users who are configured for two-way SMS are automatically switched to call to phone verification at that time.
Notification through mobile app	Sends a push notification to your phone or registered device. The user views the notification and selects Approve to complete verification. The Microsoft Authenticator app is available for Windows Phone, Android, and iOS. Push notifications through the mobile app provide the best user experience.
Verification code from mobile app	The Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The Microsoft Authenticator app is available for Windows Phone, Android, and iOS. Verification code from mobile app can be used when the phone has no data connection or cellular signal.

- ✓ There is also a selection to cache passwords so that users do not have to authenticate on trusted devices. The number of days before a user must re-authenticate on trusted devices can also be configured with the value from 1 to 60 days. The default is 14 days.

For more information, **Multi-Factor Authentication**⁴

Self-Service Password Reset

The large majority of helpdesk calls in most companies 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**.

⁴ <https://azure.microsoft.com/en-us/services/multi-factor-authentication/>

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. The Azure documentation recommends creating a specific group for purposes of testing or proof of concept before deploying to a larger group within the Azure AD tenant. 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, but it is a good idea to have additional 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.

Regarding the security questions, these can be configured to require a certain number of questions to be registered for the users in your AD tenant. In addition, you must configure the number of correctly answered security question that are required for a successful password reset. There are a large number of security questions. Note that security questions can be less secure than other methods because some people might know the answers to another user's questions.

-
- ✓ Azure Administrator accounts will always be able to reset their passwords no matter what this option is set to.

MCT USE ONLY. STUDENT USE PROHIBITED

Users and Groups

User accounts

To view the Azure AD users, simply access the All users blade.

	Name	User name	User type	Source
<input type="checkbox"/>	Ziaulla	ziaulla@mac...	Guest	External Azure Active Directory
<input type="checkbox"/>	Retail Crisis Notificati...	rscrisis@mic...	Member	Windows Server AD
<input type="checkbox"/>	"Planning & Launch Se...	plsoem@mi...		Windows Server AD
<input type="checkbox"/>	'amckenziec...	'amckenziec...	Guest	Invited user
<input type="checkbox"/>	'Evento FY20 Colombia	kickcolo@mi...	Member	Windows Server AD

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. Their source is Azure Active Directory or External Azure Active Directory if the user is defined in another Azure AD instance but needs access to subscription resources controlled by this directory. 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.
- ✓ Have you given any thought as to the type of users you will need?

Managing 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.

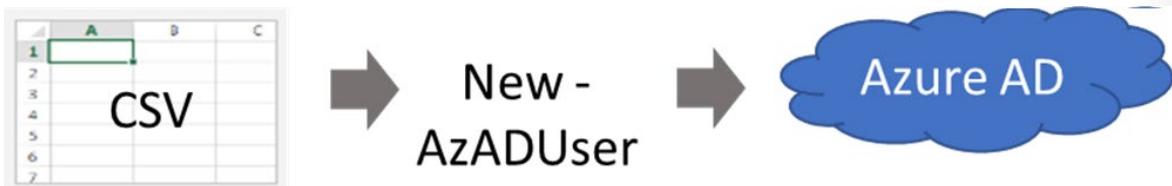
The screenshot shows the 'New user' page from Microsoft. At the top, there are several navigation links: '+ New user', '+ New guest user', 'Bulk create', 'Bulk invite', 'Bulk delete', and 'Download users'. Below these, the title 'New user' and the Microsoft logo are displayed. There are two main options: 'Create user' (radio button) and 'Invite user' (radio button, selected). The 'Create user' section describes creating a new user in the organization with a sample email like 'alice@Microsoft.onmicrosoft.com'. The 'Invite user' section describes inviting a guest user to collaborate, mentioning they will be emailed an invitation that needs to be accepted. Both sections have a link 'I want to [action] users in bulk'.

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

Bulk User Accounts

There are several ways you can use PowerShell to import data into your directory, but the most commonly used method is to use a comma-separated values (CSV) file. This file can either be manually created, for example using Excel, or it can be exported from an existing data source such as a SQL database or an HR application.



If you are going to use a CSV file here are some things to think about:

- **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 for this are generating a random password and emailing it to the new user or their manager.

Configuring bulk user accounts

The steps for using the CSV file are very straightforward.

1. Use **Connect-AzAccount** to create a PowerShell connection to your directory You should connect with an admin account that has privileges on your directory.

2. Create a new Password Profile for the new users. The password for the new users needs to conform to the password complexity rules you have set for your directory.
3. Use **Import-CSV** to import the csv file. You will need to specify the path and file name of the CSV file.
4. Loop through the users in the file constructing the user parameters required for each user. For example, User Principal Name, Display Name, Given Name, Department, and Job Title.
5. Use **New-AzADUser** to create each user. Be sure to enable each account.

For more information, [Importing data into my directory⁵](#)

Group Accounts

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

- **Security groups.** These are the most common and 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.
- **Office 365 groups.** These groups provide collaboration opportunities by giving members access to a shared mailbox, calendar, files, SharePoint site, and more. This option also lets you give people outside of your organization access to the group. This option is available to users as well as admins.

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

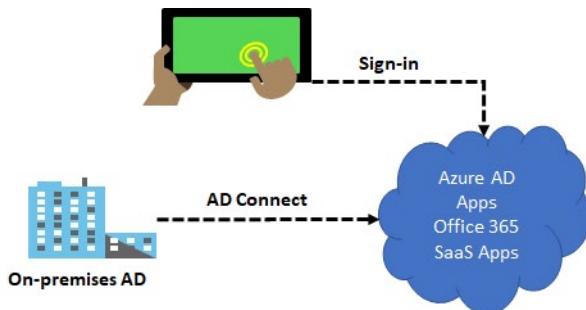
There are different ways you can assign access rights:

- **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. If a member's attributes change, the system looks at your dynamic group rules for the directory to see if the member meets the rule requirements (is added) or no longer meets the rules requirements (is removed).
 - **Dynamic Device (Security groups only).** Lets you use dynamic group rules to automatically add and remove devices. If a device's attributes change, the system looks at your dynamic group rules for the directory to see if the device meets the rule requirements (is added) or no longer meets the rules requirements (is removed).
- ✓ Have you given any thought to which groups you need to create? Would you directly assign or dynamically assign membership?

⁵ <https://docs.microsoft.com/en-us/powershell/azure/active-directory/importing-data?view=azureadps-2.0>

Azure AD Connect

Azure AD Connect will integrate your on-premises directories with Azure Active Directory. This allows you to provide a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD.



Azure AD Connect features

Azure AD Connect provides the following features:

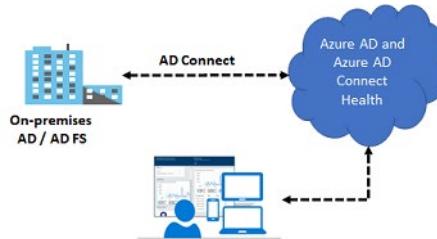
- **Password hash synchronization.** A sign-in method that synchronizes a hash of a user's on-premises AD password with Azure AD.
- **Pass-through authentication.** A sign-in method that allows users to use the same password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.
- **Federation integration.** Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
- **Synchronization.** Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.
- **Health Monitoring.** Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

For more information, [Integrate your on-premises directories with Azure Active Directory⁶](#)

Azure AD Connect Health

When you integrate your on-premises directories with Azure AD, your users are more productive because there's a common identity to access both cloud and on-premises resources. However, this integration creates the challenge of ensuring that this environment is healthy so that users can reliably access resources both on-premises and in the cloud from any device.

⁶ <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect>



Azure Active Directory (Azure AD) Connect Health provides robust monitoring of your on-premises identity infrastructure. It enables you to maintain a reliable connection to Office 365 and Microsoft Online Services. This reliability is achieved by providing monitoring capabilities for your key identity components. Also, it makes the key data points about these components easily accessible.

Azure AD Connect Health helps you:

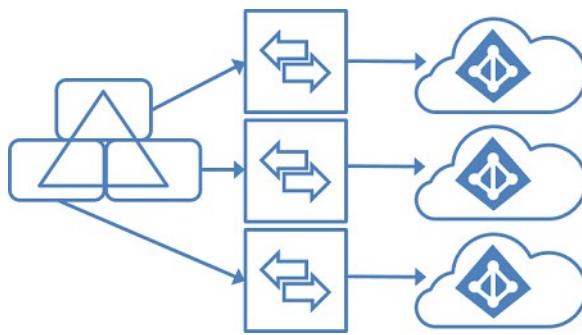
- Monitor and gain insights into AD FS servers, Azure AD Connect, and AD domain controllers.
- Monitor and gain insights into the synchronizations that occur between your on-premises AD DS and Azure AD.
- Monitor and gain insights into your on-premises identity infrastructure that is used to access Office 365 or other Azure AD applications

With Azure AD Connect the key data you need is easily accessible. You can view and act on alerts, setup email notifications for critical alerts, and view performance data.

- ✓ Using AD Connect Health works by installing an agent on each of your on-premises sync servers.

Managing Multiple Directories

In Azure Active Directory (Azure AD), each tenant is a fully independent resource: a peer that is logically independent from the other tenants that you manage. There is no parent-child relationship between tenants. This independence between tenants includes resource independence, administrative independence, and synchronization independence.



Resource independence

- If you create or delete a resource in one tenant, it has no impact on any resource in another tenant, with the partial exception of external users.
- If you use one of your domain names with one tenant, it cannot be used with any other tenant.

Administrative independence

If a non-administrative user of tenant 'Contoso' creates a test tenant 'Test,' then:

- By default, the user who creates a tenant is added as an external user in that new tenant, and assigned the global administrator role in that tenant.
- The administrators of tenant 'Contoso' have no direct administrative privileges to tenant 'Test,' unless an administrator of 'Test' specifically grants them these privileges. However, administrators of 'Contoso' can control access to tenant 'Test' if they control the user account that created 'Test.'
- If you add/remove an administrator role for a user in one tenant, the change does not affect the administrator roles that the user has in another tenant.

Synchronization independence

You can configure each Azure AD tenant independently to get data synchronized from a single instance of either:

- The Azure AD Connect tool, to synchronize data with a single AD forest.
- The Azure Active tenant Connector for Forefront Identity Manager, to synchronize data with one or more on-premises forests, and/or non-Azure AD data sources.

Add an Azure AD tenant

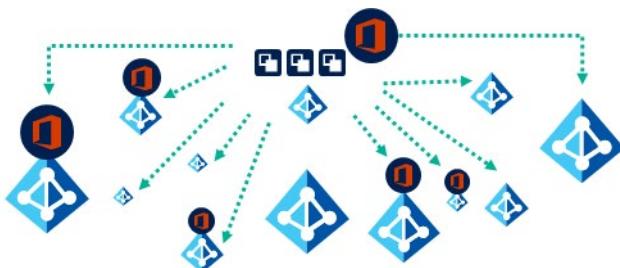
To add an Azure AD tenant in the Azure portal, sign in to the Azure portal with an account that is an Azure AD global administrator, and, on the left, select New.

Note: Unlike other Azure resources, your tenants are not child resources of an Azure subscription. If your Azure subscription is canceled or expired, you can still access your tenant data using Azure PowerShell, the Microsoft Graph API, or the Microsoft 365 admin center. You can also associate another subscription with the tenant.

Azure B2B and B2C

Azure AD B2B

Azure Active Directory (Azure AD) business-to-business (B2B) collaboration lets you securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data. Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources. Developers can use Azure AD business-to-business APIs to customize the invitation process or write applications like self-service sign-up portals.



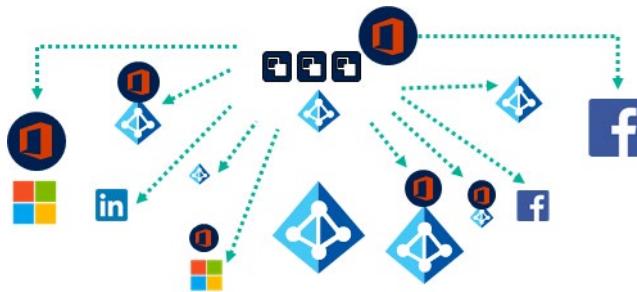
With Azure AD B2B:

- There is no external administrative overhead for your organization.
- The partner uses their own identities and credentials; Azure AD is not required.

- You don't need to manage external accounts or passwords.
- You don't need to sync accounts or manage account lifecycles.

Azure AD B2C

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs. Azure Active Directory B2C (Azure AD B2C) is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring and automatically handling threats like denial-of-service, password spray, or brute force attacks.



With Azure AD B2C:

- You invite users from other social media Identity Tenants into your own organization tenant.
- User provisioning is done by the invited party; you are in control to invite the other side's users.
- Standards-based authentication protocols are used including OpenID Connect, OAuth 2.0, and SAML. Integrates with most modern applications and commercial off-the-shelf software.
- Provides a directory that can hold 100 custom attributes per user. However, you can also integrate with external systems. For example, use Azure AD B2C for authentication, but delegate to an external customer relationship management (CRM) or customer loyalty database as the source of truth for customer data
- Facilitate identity verification and proofing by collecting user data, then passing it to a third party system to perform validation, trust scoring, and approval for user account creation.

Demonstration - Users and Groups

In this demonstration, we will explore Active Directory users and groups.

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

Determine domain information

1. Access the Azure portal, and navigate to the **Azure Active Directory** blade.
2. Make a note of your available domain name. For example, usergmail.onmicrosoft.com.

Explore user accounts

1. Select the **Users** blade.
2. Select **New user**. Notice the selection to create a **New guest user**.
3. Add a new user reviewing the information: **User**, **User Name**, **Groups**, **Directory Role**, and **Job Info**.

4. After the user is created, review additional information about the user.

Explore group accounts

1. Select the **Groups** blade.
2. Add a **New group**.

- **Group type:** *Security*
- **Group name:** *Managers*
- **Membership type:** *Assigned*
- **Members:** Add your new user to the group.

3. After the group is created, review additional information about the group.

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"" -TargetGroupDisplay-  
Name """MyGroupDisplayName""
```

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

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

Module 01 Lab and Review

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

Module 01 Review Questions

Review Question 1

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.
- Connect the device to Azure AD.
- Register the device with Azure AD.

Review Question 2

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com and an Azure Active Directory (Azure AD) domain named contoso.onmicrosoft.com.

Azure AD Connect is installed and Active Directory Federation Services (AD FS) is configured. Password-writeback is enabled. You need to monitor synchronization events generated by Azure AD Connect. Select one.

- Install Azure AD Connect Health.
- Deploy a domain controller for contoso.com on a virtual machine in the contoso.onmicrosoft.com tenant.
- Configure Authentication Caching.
- Launch Synchronization Service Manager and edit the properties of the connector.

Review Question 3

Identify three differences from the following list between Azure Active Directory (AD) and Active Directory Domain Services (AD DS). Select three.

- Azure AD uses HTTP and HTTPS communications
- Azure AD uses Kerberos authentication
- There are no Organizational Units (OUs) or Group Policy Objects (GPOs) in Azure AD
- Azure AD includes Federation Services
- Azure AD can be queried through LDAP

Review Question 4

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
- Provider identity
- Guest User
- Hosted identity

Review Question 5

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

Review Question 6

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.

- Global administrator
- Password administrator
- Security administrator
- User administrator

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Create Azure users and groups in Azure Active Directory⁷**
- **Manage users and groups in Azure Active Directory⁸**
- **Secure your Azure resources with role-based access control⁹**
- **Secure Azure Active Directory users with Multi-Factor Authentication¹⁰**
- **Allow users to reset their password with Azure Active Directory self-service password reset¹¹**
- **Secure your application by using OpenID Connect and Azure AD¹²**

⁷ <https://docs.microsoft.com/en-us/learn/modules/create-users-and-groups-in-azure-active-directory/>

⁸ <https://docs.microsoft.com/en-us/learn/modules/manage-users-and-groups-in-aad/>

⁹ <https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/>

¹⁰ <https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/>

¹¹ <https://docs.microsoft.com/en-us/learn/modules/allow-users-reset-their-password/>

¹² <https://docs.microsoft.com/en-us/learn/modules/secure-app-with-oidc-and-azure-ad/>

Answers

Review Question 1

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.
- Connect 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.

Review Question 2

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com and an Azure Active Directory (Azure AD) domain named contoso.onmicrosoft.com.

Azure AD Connect is installed and Active Directory Federation Services (AD FS) is configured. Password-writeback is enabled. You need to monitor synchronization events generated by Azure AD Connect. Select one.

- Install Azure AD Connect Health.
- Deploy a domain controller for contoso.com on a virtual machine in the contoso.onmicrosoft.com tenant.
- Configure Authentication Caching.
- Launch Synchronization Service Manager and edit the properties of the connector.

Explanation

Install Azure AD Connect Health. Azure AD Connect Health is a feature that will monitor on-premises AD DS identities and provide alerts. This requires an agent on each server being monitored.

Review Question 3

Identify three differences from the following list between Azure Active Directory (AD) and Active Directory Domain Services (AD DS). Select three.

- Azure AD uses HTTP and HTTPS communications
- Azure AD uses Kerberos authentication
- There are no Organizational Units (OUs) or Group Policy Objects (GPOs) in Azure AD
- Azure AD includes Federation Services
- Azure AD can be queried through LDAP

Explanation

Although the list is by no means conclusive, and you may identify others not listed, here are several characteristics of Azure AD that make it different to AD DS: Azure AD is primarily an identity solution, and it is designed for Internet-based applications by using HTTP and HTTPS communications; because Azure AD is HTTP/HTTPS based, it cannot be queried through LDAP. Instead, Azure AD uses the REST API over HTTP and HTTPS. 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). Azure AD users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs). While Azure AD includes federation services, and many third-party services (such as Facebook), AD DS supports federation.

Review Question 4

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
- Provider identity
- Guest User
- Hosted identity

Explanation

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

Review Question 5

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.

Review Question 6

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.

- Global administrator
- Password administrator
- Security administrator
- User administrator

Explanation

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

Module 2 Governance and Compliance

Subscriptions and Accounts

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**¹ is a geographical area on the planet containing at least one, but potentially multiple datacenters that 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 50+ regions and available in 140 countries.



¹ <https://azure.microsoft.com/en-us/global-infrastructure/regions/>

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.
- There are also some global Azure services that do not require you to select a region, such as Microsoft Azure Active Directory, Microsoft Azure Traffic Manager, or Azure DNS.
- Each Azure region is paired with another region within the same geography, together making a region pair . The exception is Brazil South, which is paired with a region outside its geography.

Things to know about regional pairs

A regional pair consists of two regions within the same geography. Azure serializes platform updates (planned maintenance) across regional pairs, ensuring that only one region in each pair updates at a time. If an outage affects multiple regions, at least one region in each pair will be prioritized for recovery.

- **Physical isolation.** When possible, 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.** In the event of 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) to minimize downtime, the effect of 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.
- ✓ View the latest [Azure regions map](#).²
- ✓ View the complete list of [region pairs](#)³.

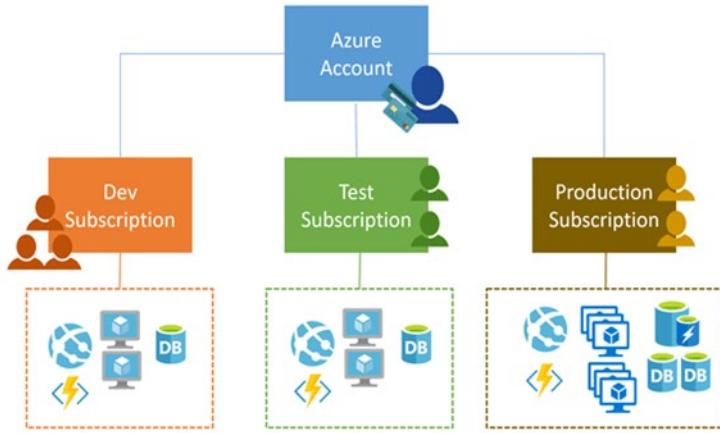
Azure Subscriptions

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.

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

³ <https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions#what-are-paired-regions>

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.



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.

Typically to grant a user access to your Azure resources, you would add them to the Azure AD directory associated with your subscription. The user will now have access to all the resources in your subscription. This is an all-or-nothing operation that may give that user access to more resources than you anticipated.

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

Getting a Subscription

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



Enterprise agreements

Any **Enterprise Agreement**⁴ 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 from its global datacenters. Enterprise agreements have a 99.95% monthly SLA.

Reseller

Buy Azure through the **Open Licensing program**⁵, 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](#)⁶.

Partners

Find a **Microsoft partner**⁷ 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**⁸ you can get started using Azure right away and you won't be charged until you choose to upgrade.

- ✓ Which subscription model are you most interested in?

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

⁴ <https://azure.microsoft.com/en-us/pricing/enterprise-agreement/>

⁵ <https://www.microsoft.com/en-us/licensing/licensing-programs/open-license.aspx>

⁶ <https://azure.microsoft.com/en-us/offers/ms-azr-0111p/>

⁷ <https://azure.microsoft.com/en-us/partners/directory/>

⁸ <https://azure.microsoft.com/en-us/free/>

- 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. This 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.

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

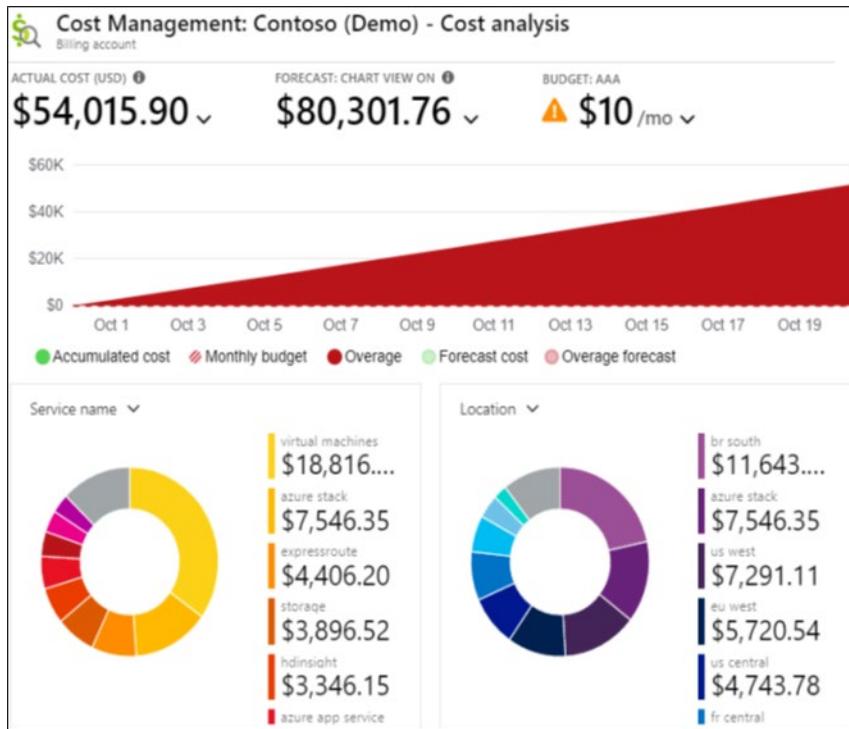
An Enterprise Agreement provides flexibility to buy cloud services and software licenses under one agreement, with discounts for new licenses and Software Assurance. It's targeted at enterprise-scale organizations.

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.

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 Marketplace 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.

Resource Tags

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.

Name ⓘ	Value ⓘ
<input type="text"/>	<input type="text"/>

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 consider 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.
- ✓ If you need to create a lot of tags you will want to do that programmatically. You can use PowerShell or the CLI.

Cost Savings

Reservations helps you save money by pre-paying 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, which helps maximize the value of existing on-premises Windows Server and/or SQL Server license investments when migrating to Azure. There is a 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.

Additionally, consider:

The **Pricing Calculator**⁹ 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 "Your Estimate" and "Virtual Machines". Below that, there are dropdown menus for "REGION", "OPERATING SYSTEM", "TYPE", "TIER", and "INSTANCE". The "REGION" is set to "West US", "OPERATING SYSTEM" is "Windows", "TYPE" is "(OS Only)", "TIER" is "Standard", and the "INSTANCE" is "D1: 1 Cores(s), 3.5 GB RAM, 50 GB Temporary storage, \$0.140/hour".

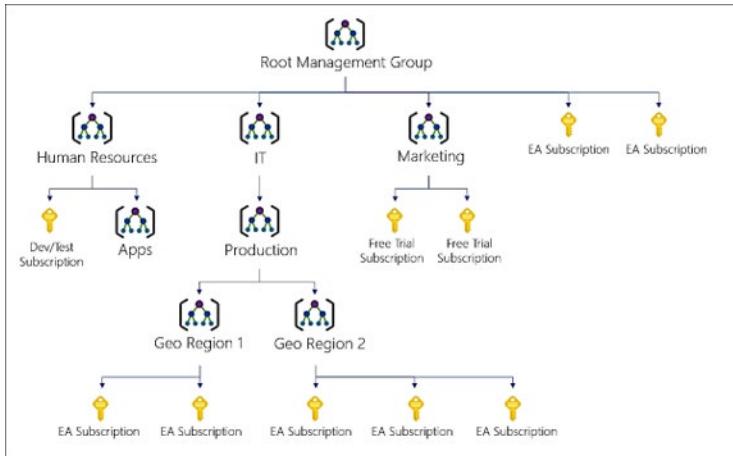
⁹ <https://azure.microsoft.com/en-us/pricing/calculator/>

Azure Policy

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).



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.

Creating 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.

The screenshot shows the Azure Management Groups interface. At the top, there's a red box highlighting the '+ New management group' button and a 'Refresh' button. Below that, the navigation bar shows 'Root Management G... > Contoso Redmond'. A search bar says 'Search by name or ID'. To the right, there's a blue icon of three people connected by lines. A text box says 'Using management groups helps you manage access, policy, and compliance by grouping multiple subscriptions together. [Learn more.](#)' Below this, a table lists three 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.
- ✓ Do you think you will want to use Management Groups?

For more information, [Organize your resources with Azure management groups¹⁰](#)

Azure Policy

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 does this by running evaluations of your resources and scanning for those not compliant with the policies you have created.

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

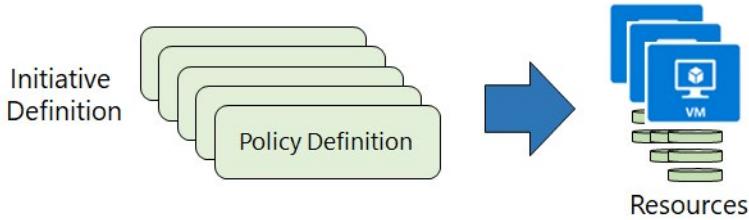
- Specify the resource types that your organization can deploy.

¹⁰ <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management-groups-overview>

- 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.

For more information, [Azure Policy Documentation¹¹](#)

Implementing Azure Policy



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

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. This can be used to enforce your geo-compliance requirements.

¹¹ <https://docs.microsoft.com/azure/azure-policy/>

+ Initiative definition	+ Policy definition	Refresh			
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

If there isn't an applicable policy you can add a new Policy Definition. The easiest way to do this is to Import a policy from [GitHub](#)¹². 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

Import sample policy definition from GitHub

- ✓ Policy Definitions have a **specific JSON format**¹³. As a Azure Administrator you will not need to create files in this format, but you may want to review the format, just so you are familiar.

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.

¹² <https://github.com/Azure/azure-policy/tree/master/samples>

¹³ <https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

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

- ✓ Currently, an Initiative Definition can have up to 100 policies.
- ✓ What planning will be needed to organize your policy definitions?

Scope the Initiative

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.

Total Assignments	Initiative Assignments	Policy Assignments		
2	2	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.

Scope

Subscription

ASC DEMO

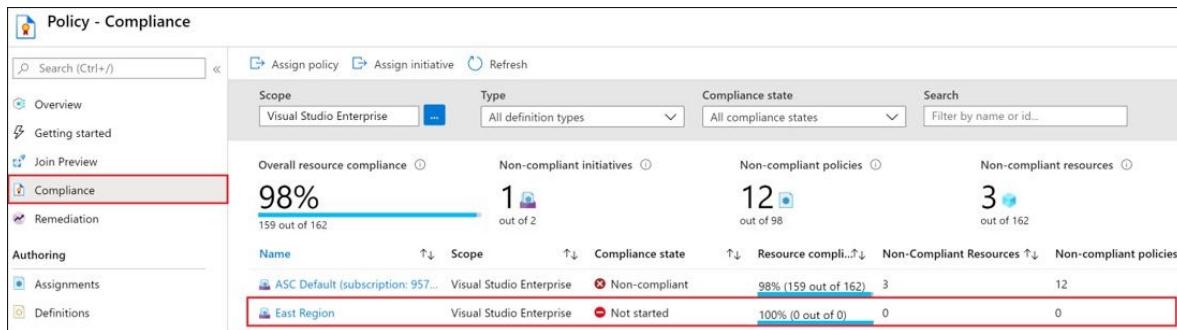
Resource Group

Optionally choose a Resource Group

AppServiceRG
ASCDEMO
ASCDDEMORG
ASCDEMORGasclogs
AzureBackupRG_eastus_1

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.



When a condition is evaluated against your existing resources and found true, then those resources are marked as non-compliant with the policy. 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.

- ✓ Policy evaluation happens about once an hour, which means that if you make changes to your policy definition and create a policy assignment then it will be re-evaluated over your resources within the 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. Select **Definitions** under Authoring in the left side of the Azure Policy page.
2. Select **+ Initiative Definition** at the top of the page to open the Initiative definition 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**.

MCT USE ONLY. STUDENT USE PROHIBITED

Role-Based Access Control

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.

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

What can I do with RBAC?

Here are some examples of what you can do with 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

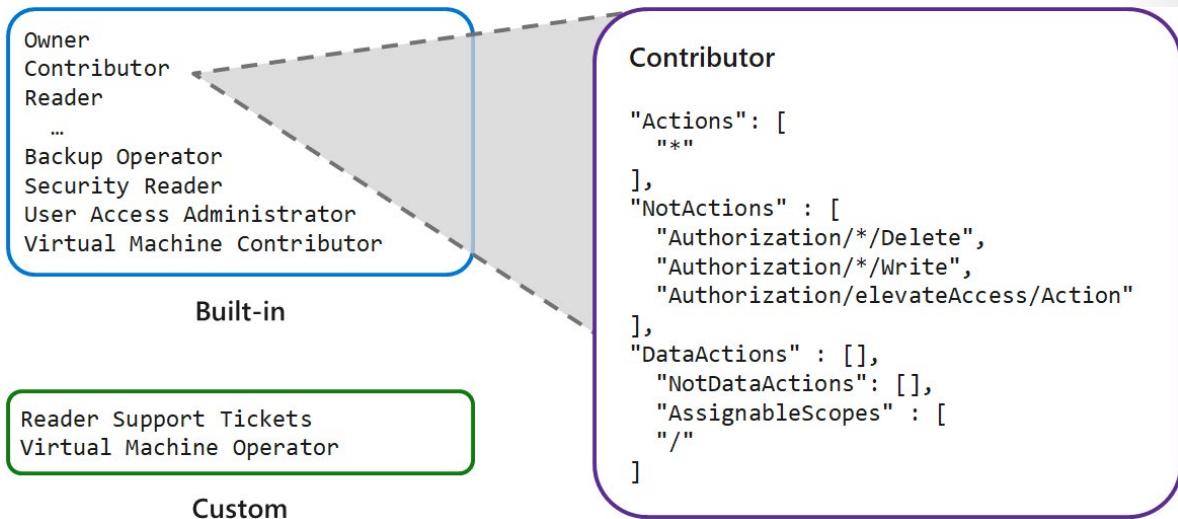
- **Security principal.** Object that represents something that is requesting access to resources. Examples: user, group, service principal, managed identity
- **Role definition.** Collection of permissions that lists the operations that can be performed. Examples: Reader, Contributor, Owner, User Access 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.

Best practices for using RBAC

Using 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 RBAC.

Role Definitions



Contributor

```
"Actions": [
  "*"
],
"NotActions" : [
  "Authorization/*/Delete",
  "Authorization/*/Write",
  "Authorization/elevateAccess/Action"
],
"DataActions" : [],
"NotDataActions": [],
"AssignableScopes" : [
  "/"
]
```

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

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

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

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

Defining the Actions and NotActions properties is not enough to fully implement a role. You must also properly scope your role.

The `AssignableScopes` property of the role specifies the scopes (subscriptions, resource groups, or resources) within which the custom role is available for assignment. You can make the custom role available for assignment in only the subscriptions or resource groups that require it, and not clutter the user experience for the rest of the subscriptions or resource groups.

```
* /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

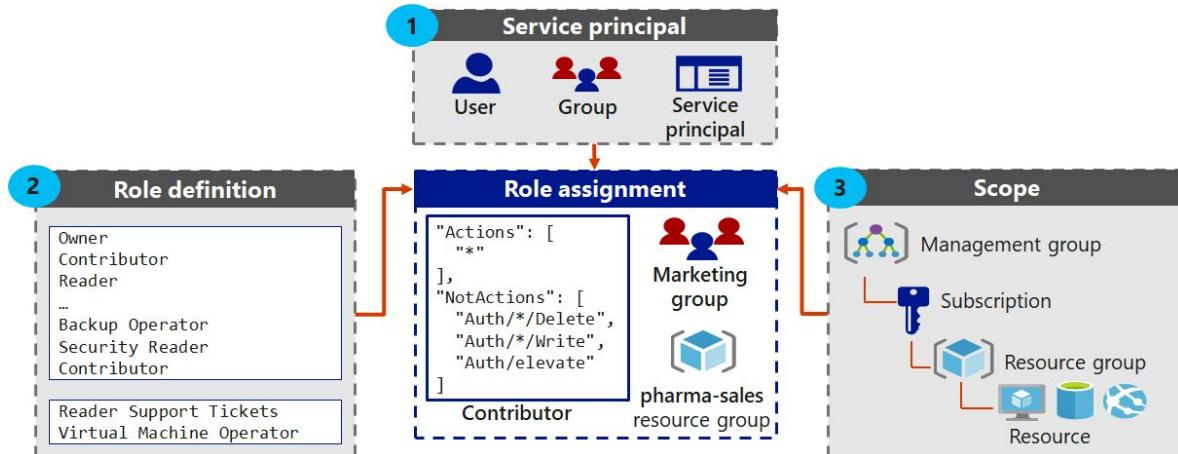
Makes a role available for assignment only in the Network resource group.

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

Role Assignment

A role assignment is the process of attaching a role definition to a user, group, service principal, or managed identity at a particular scope for the purpose of granting access. Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

This diagram shows an example of a role assignment. In this example, the Marketing group has been assigned the Contributor role for the pharma-sales resource group. This means that users in the Marketing group can create or manage any Azure resource in the pharma-sales resource group. Marketing users do not have access to resources outside the pharma-sales resource group, unless they are part of another role assignment.



Notice that access does not need to be granted to the entire subscription. Roles can also be assigned for resource groups as well as for individual resources. In Azure RBAC, a resource inherits role assignments from its parent resources. So if a user, group, or service is granted access to only a resource group within a subscription, they will be able to access only that resource group and resources within it, and not the other resources groups within the subscription.

As another example, a security group can be added to the Reader role for a resource group, but be added to the Contributor role for a database within that resource group.

Azure RBAC Roles vs Azure AD Administrator Roles

If 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 administrator 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.

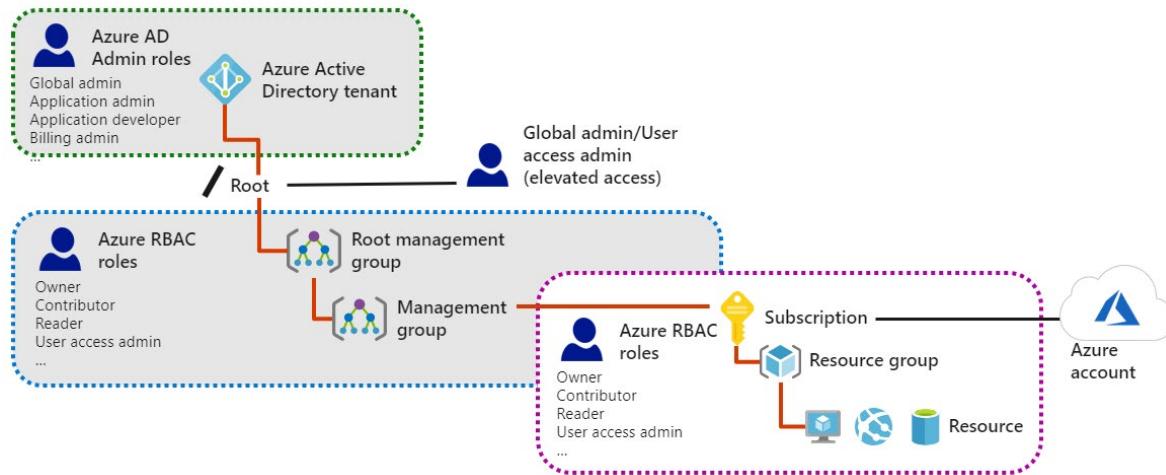
Azure RBAC roles	Azure AD administrator roles
Manage access to Azure resources.	Manage access to Azure Active Directory resources.
Supports custom roles.	Cannot create your own roles.
Scope can be specified at multiple levels (management group, subscription, resource group, resource).	Scope is at the 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, Office 365 admin portal, Microsoft Graph AzureAD PowerShell.

- ✓ Classic administrator roles should be avoided if you are using Azure Resource Manager.

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.



Do you see how Azure AD Admin roles and Azure RBAC roles work together to authenticate users?

Azure RBAC Roles

Azure includes several built-in roles that you can use. The following lists 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. This applies to all resource types.
- **Contributor.** Can create and manage all types of Azure resources but can't grant access to others. This applies to all resource types.
- **Reader.** Can view existing Azure resources. This applies to all resource types.
- **User Access Administrator.** Lets you manage user access to Azure resources. This applies to managing access, rather than to managing resources.

The rest of the built-in roles allow management of specific Azure resources. For example, the **Virtual Machine Contributor** role allows a user to create and manage virtual machines. If the built-in roles don't meet the specific needs of your organization, you can create your own custom roles.

Azure has introduced data operations that enable you to 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 within that 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. Select **Add role assignment**.

- **Role:** Owner
- **Select:** Managers
- **Save** your changes.

2. Select **Check access**.
3. **Find** Chris Green.
4. Notice he is part of the Managers group and is an Owner.
5. Notice that you can **Deny assignments**.

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>
```

Module 02 Lab and Review Questions

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

Module 02 Review Questions

Review Question 1

You need to target policies and review spend budgets across several subscriptions you manage. What should you do? Select one.

- Create resource groups
- Create management groups
- Create billing groups
- Create Azure policies

Review Question 2

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. What should you do? {Choose two to complete a solution}.

- Create tags for each department.
- Create a billing group for each department.
- Create an Azure policy.
- Add the groups into a single resource group.
- Create a subscription account rule.

Review Question 3

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.

Review Question 4

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 resource group
- Create a new subscriptions

Review Question 5

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.
- Role-based access control can be applied to the resource group.

Review Question 6

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

- An 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.
- A resource group for a new branch office that is just starting up.

Review Question 7

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

Review Question 8

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.
- Assign the user to the Contributor role on the resource group, then assign the user to the Owner role on VM3.

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Analyze costs and create budgets with Azure Cost Management¹⁴**
- **Predict costs and optimize spending for Azure¹⁵**
- **Control and organize Azure resources with Azure Resource Manager¹⁶**
- **Apply and monitor infrastructure standards with Azure Policy¹⁷**
- **Create custom roles for Azure resources with role-based access control¹⁸**
- **Manage access to an Azure subscription by using Azure role-based access control¹⁹**
- **Secure your Azure resources with role-based access control²⁰**

¹⁴ <https://docs.microsoft.com/en-us/learn/modules/analyze-costs-create-budgets-azure-cost-management/>

¹⁵ <https://docs.microsoft.com/en-us/learn/modules/predict-costs-and-optimize-spending/>

¹⁶ <https://docs.microsoft.com/en-us/learn/modules/control-and-organize-with-azure-resource-manager/>

¹⁷ <https://docs.microsoft.com/en-us/learn/modules/intro-to-governance/>

¹⁸ <https://docs.microsoft.com/en-us/learn/modules/create-custom-azure-roles-with-rbac/>

¹⁹ <https://docs.microsoft.com/en-us/learn/modules/manage-subscription-access-azure-rbac/>

²⁰ <https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/>

Answers

Review Question 1

You need to target policies and review spend budgets across several subscriptions you manage. What should you do? Select one.

- Create resource groups
- Create management groups
- Create billing groups
- Create Azure policies

Explanation

Create management groups. Management groups can be used to organize and manage subscriptions.

Review Question 2

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. What should you do? {Choose two to complete a solution}.

- Create tags for each department.
- Create a billing group for each department.
- Create an Azure policy.
- Add the groups into a single resource group.
- 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.

Review Question 3

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.

Review Question 4

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 resource 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.

Review Question 5

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.
- Role-based access control can be applied to the resource group.

Explanation

Resource groups cannot be nested.

Review Question 6

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

- An 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.
- A resource group for a new branch office that is just starting up.

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.

Review Question 7

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 Owner.
- 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.

Review Question 8

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.
- Assign the user to the Contributor role on the resource group, then assign the user to the Owner 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.

Module 3 Azure Administration

Azure Resource Manager

Resource Manager

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 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.

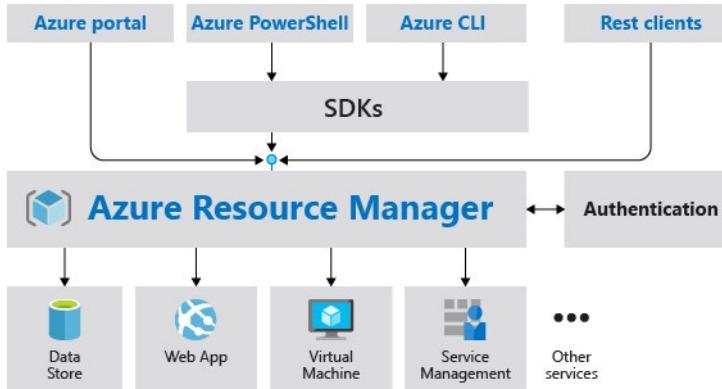
Azure Resource Manager enables you to work with the resources in your solution as a group. You can deploy, update, or delete all the resources for your solution in a single, coordinated operation. You use a template for deployment and that template can work for different environments such as testing, 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.

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**.

- ✓ Before getting started with 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.

Resource Group Deployments

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).

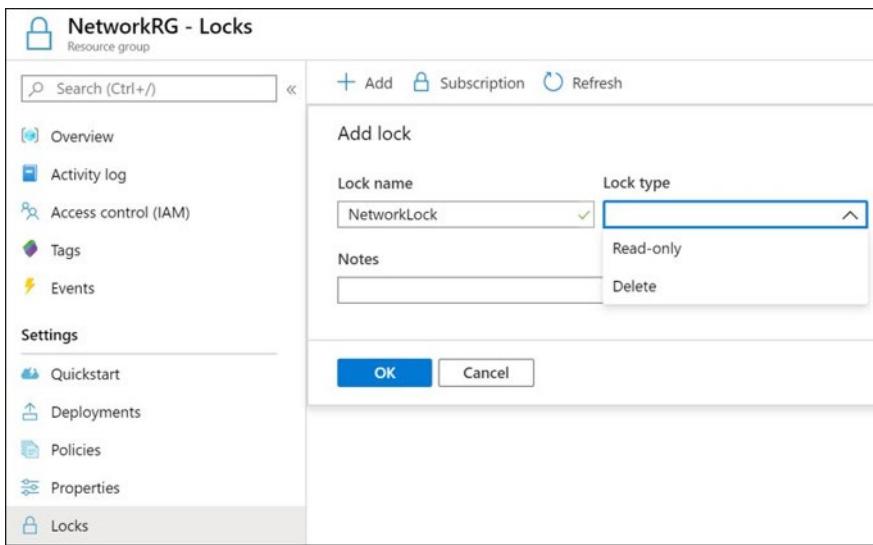
When creating a resource group, you need to provide a location for that resource group. You may be wondering, "Why does a resource group need a location? And, if the resources can have different locations than the resource group, why does the resource group location matter at all?" The resource group 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.

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

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 clicks. 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.



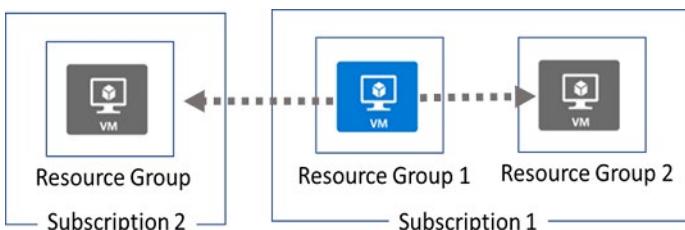
Lock types

There are two types of resource locks.

- **Read-Only locks**, which prevent any changes to the resource.
- **Delete locks**, which prevent deletion.
- ✓ Only the Owner and User Access Administrator roles can create or delete management locks.

Moving 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, but it doesn't mean the resources are frozen. For example, if you move a virtual machine to a new resource group, an application accessing the virtual machine experiences no downtime.

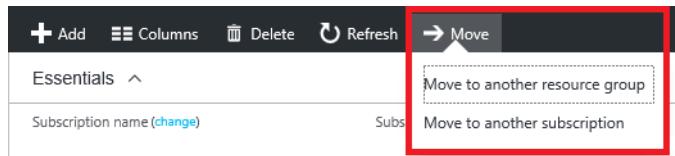
Limitations

Before beginning this process be sure to read the **Move operation support for resources¹** page. This page details what resources can be moved between resources groups and subscriptions.

¹ <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources>

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.



- ✓ 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.

Removing 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.



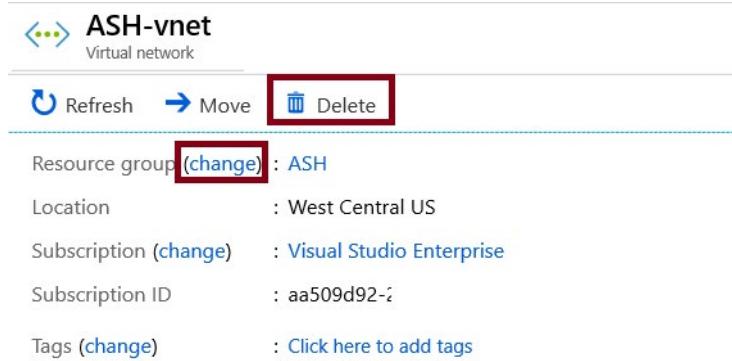
Using PowerShell to delete resource groups

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.



Resource Limits

Azure provides the ability to observe the number of each network resource type that you've deployed in your subscription and what your subscription limits are. The ability to view resource usage against limits is helpful to track current usage, and plan for future use.

Quota	Provider	Location	Usage	
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.
- If you need to increase a default limit, there is a Request Increase link. You will complete and submit the support request.
- All resources have a maximum limit listed in Azure **limits²**. If your current limit is already at the maximum number, 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**.
- 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.
- Give the lock a **name** and **lock type**. Optionally, you can add notes that describe the lock.
- To delete the lock, select the ellipsis and **Delete** from the available options.

Manage resource groups with PowerShell

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

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

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

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.

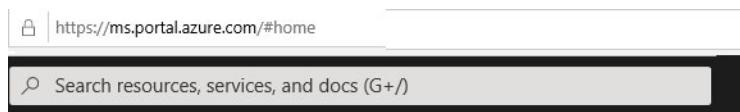
```
Get-AzResourceLock
```

- ✓ Configure resource locks, move resources across resource groups, and remove resource groups are part of the certification exam.

Azure Portal and Cloud Shell

Azure Portal

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



Azure services



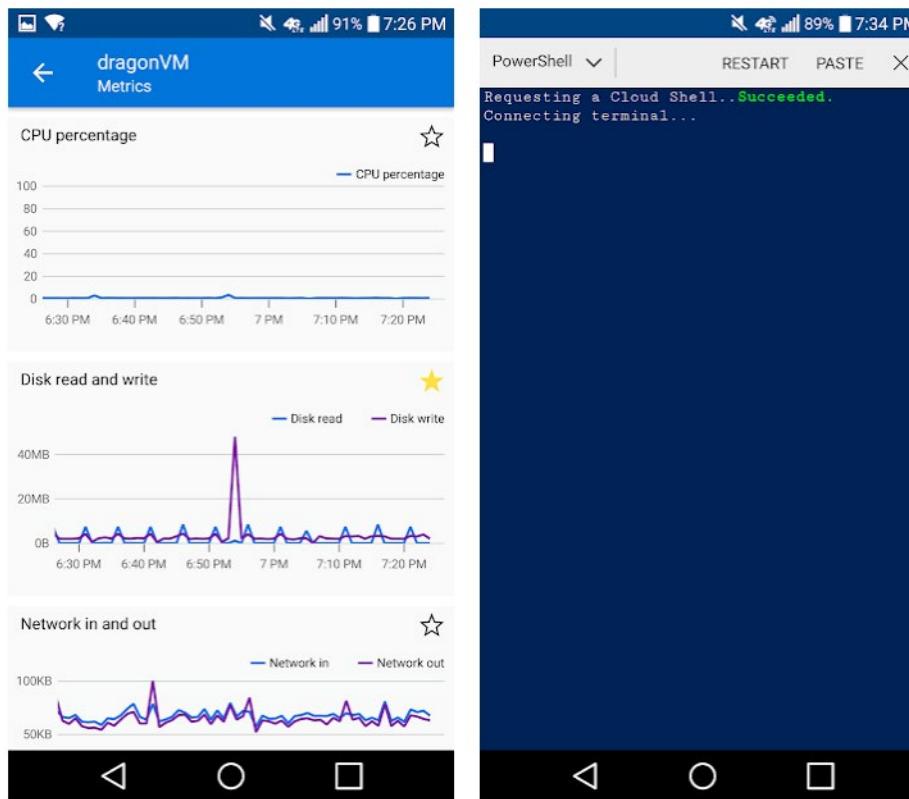
Recent resources

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

Azure Mobile App

The **Azure Mobile App** helps you keep track of your resources while on-the-go:



- **Stay connected to the cloud and check status and critical metrics anytime, anywhere.** With the Azure mobile app, you don't need to be in front of your computer to keep an eye on your Azure resources such as VMs and web apps. Stay connected no matter where you are from your iOS or Android mobile device.
- **Diagnose and fix issues quickly with Azure Mobile.** Check for alerts, view metrics, and take corrective actions to fix common issues. Restart a web app or connect to a VM directly. Be agile and respond to issues faster with the Azure mobile app.
- **Run commands to manage your Azure resources.** Want to use the command line? Run ad hoc Azure CLI or PowerShell commands from the Azure mobile app. Stay in control of your resources and take corrective actions, like starting and stopping VMs and web apps.

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, and hold **G** and press **D** to go your Dashboard.

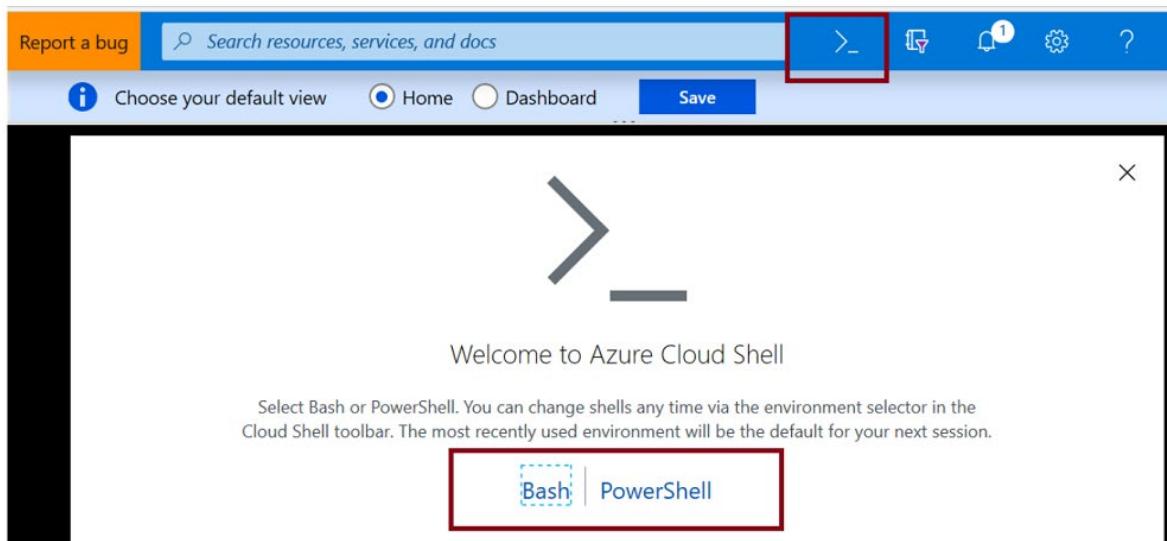
Customizing your experience

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.

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. Leverage 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 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.

MCT USE ONLY. STUDENT USE PROHIBITED

Azure PowerShell and CLI

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 GitHub³](#).

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. However, going forward you should transition to the Az module and use the **-Az** commands.

- ✓ Bookmark the [Azure PowerShell Reference⁴](#)

³ <https://github.com/Azure/azure-powershell>

⁴ <https://docs.microsoft.com/en-us/powershell/module/az.compute/get-azvm?view=azps-3.3.0>

PowerShell Cmdlets and Modules

A PowerShell command is called a *cmdlet* (pronounced “command-let”). A *cmdlet* is a command that manipulates a single feature. The term cmdlet is intended to imply that it is a small command. By convention, cmdlet authors are encouraged to keep cmdlets simple and single purpose.

The base PowerShell product ships with cmdlets that work with features such as sessions and background jobs. You add modules to your PowerShell installation to get cmdlets that manipulate other features. For example, there are third-party modules to work with ftp, administer your operating system, and access the file system.

Cmdlets follow a verb-noun naming convention; for example, **Get-Process**, **Format-Table**, and **Start-Service**.

There is also a convention for verb choice. You can use **Get-Verb** to retrieve examples, such as:

- **get** retrieves data.
- **set** inserts or updates data.
- **format** formats data.
- **out** directs output to a destination.

Cmdlet authors are encouraged to include a help file for each cmdlet. The **Get-Help** cmdlet displays the help file for any cmdlet. For example, you could get help on the `Get-ChildItem` cmdlet with the following statement:

```
Get-Help Get-ChildItem -detailed
```

Cmdlets are shipped in `_modules`. A *PowerShell module* is a DLL file that includes the code to process each available cmdlet. You load cmdlets into PowerShell by loading the module containing them. You can get a list of loaded modules using the `Get-Module` command:

```
Get-Module
```

This will output something like the following code:

ModuleType	Version	Name	ExportedCommands
Manifest	3.1.0.0	Microsoft.PowerShell.Management	{Add-Computer, Add-Content, Check- point-Computer, Clear-Con...}
Manifest	3.1.0.0	Microsoft.PowerShell.Utility	{Add-Member, Add-Type, Clear-Variable, Com- pare-Object...}
Binary	1.0.0.1	PackageManagement	{Find-Package, Find-PackageProvider, Get-Package, Get-Pack...}
Script	1.0.0.1	PowerShellGet	{Find-Command, Find-DscResource, Find-Module, Find-RoleCap...}
Script	2.0.0	PSReadline	{Get-PSReadLineKeyHandler, Get-PSReadLineOption, Remove-PS...

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

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

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
```

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 or a 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 -q 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
```

- ✓ Bookmark the **Azure CLI Reference**⁵.

⁵ <https://docs.microsoft.com/en-us/cli/azure/?view=azure-cli-latest>

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>
```

Verify the resource group

1. 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
```

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

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

3. 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>']"
```

ARM Templates

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.

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 utilizing 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.

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.

For more information, **Understand the structure and syntax of Azure Resource Manager Templates⁶**.

⁶ <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-authoring-templates>

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 (VM'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."
        }
    }
}
```

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

Template Variables

This template section is where you define values that are used throughout the template. Variables can help make your templates easier to maintain. For example, you might define a storage account name one time as a variable, and then use that variable throughout the template. If the storage account name changes, you need to only update the variable once.

Here's an example that illustrates a few variables that describe networking features for a VM:

```
"variables": {
    "nicName": "myVMNic",
```

```

    "addressPrefix": "10.0.0.0/16",
    "subnetName": "Subnet",
    "subnetPrefix": "10.0.0.0/24",
    "publicIPAddressName": "myPublicIP",
    "virtualNetworkName": "MyVNET"
}

```

Template Functions

This section is where you define procedures that you don't want to repeat throughout the template. Similar to variables, functions can help make your templates easier to maintain.

When defining a user function, there are some restrictions:

- The function can't access variables.
- The function can only use parameters that are defined in the function. When you use the parameters function within a user-defined function, you're restricted to the parameters for that function.
- The function can't call other user-defined functions.
- The function can't use the reference function.
- Parameters for the function can't have default values.

Here's a function that creates a unique name. You could use this function when creating resources that have globally unique naming requirements.

```

"functions": [
{
  "namespace": "contoso",
  "members": {
    "uniqueName": {
      "parameters": [
        {
          "name": "namePrefix",
          "type": "string"
        }
      ],
      "output": {
        "type": "string",
        "value": "[concat(toLower(parameters('namePrefix')), uniqueString(resourceGroup().id))]"
      }
    }
  }
},
]

```

Template Resources

This section is where you define the Azure resources that make up your deployment.

Here's an example that creates a public IP address resource.

```
{
  "type": "Microsoft.Network/publicIPAddresses",
  "name": "[variables('publicIPAddressName')]",
  "location": "[parameters('location')]",
  "apiVersion": "2018-08-01",
  "properties": {
    "publicIPAllocationMethod": "Dynamic",
    "dnsSettings": {
      "domainNameLabel": "[parameters('dnsLabelPrefix')]"
    }
  }
}
```

The type of resource is `Microsoft.Network/publicIPAddresses`. The name is read from the variables section. The location, or Azure region, and domainNameLabel are provided from the parameters section. The IP address will be dynamically allocated.

Because resource types can change over time, `apiVersion` refers to the version of the resource type you want to use. As resource types evolve, you can modify your templates to work with the latest features.

Template Outputs

This section is where you define any information you'd like to receive when the template runs. For example, you might want to receive your VM's IP address or fully qualified domain name (FQDN), information you do not know until the deployment runs.

Here is the structure of an output definition:

```
"outputs": {
  "<output-name>": {
    "condition": "<boolean-value-whether-to-output-value>",
    "type": "<type-of-output-value>",
    "value": "<output-value-expression>",
    "copy": {
      "count": <number-of-iterations>,
      "input": <values-for-the-variable>
    }
  }
}
```

Here's an example that illustrates an output named **hostname**. The FQDN value is read from the VM's public IP address settings:

```
"outputs": {
  "hostname": {
    "type": "string",
    "value": "[reference(variables('publicIPAddressName')).dnsSettings.fqdn]"
  }
}
```

- ✓ It is a good practice to comment your templates. For inline comments, you can comment a single line with //. You can comment a block of lines with /* ... */. This can vary across different tools so be sure to check what works for you.

QuickStart Templates

Azure Quickstart templates⁷ are Resource Manager templates provided by the Azure community.

757 Quickstart templates are currently in the gallery.

Create Configuration Manager Tech Preview Lab in Azure	Create a Standard Storage Account
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...	This template creates a Standard Storage Account
Deploy a Django app	Create an new AD Domain with 2 Domain Controllers
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...	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.
- The azuredeploy.json file defines the resources that will be deployed.
- The azuredeploy.parameters.json file provides the values the template needs.
- ✓ 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 gallery**⁸. In the gallery you will find a number of 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**⁹ template.

⁷ <https://azure.microsoft.com/en-us/resources/templates/>

⁸ <https://azure.microsoft.com/resources/templates?azure-portal=true>

⁹ <https://azure.microsoft.com/resources/templates/101-vm-simple-windows?azure-portal=true>

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.
- ✓ 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 *dnslabelprefix* values, and then run the PowerShell file without input. Use the file **build.ps1¹⁰** 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. Note the VM name, then run the following command to obtain additional VM details:

¹⁰ <https://github.com/Microsoft/PartsUnlimited/blob/master/build.ps1?azure-portal=true>

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.

- ✓ 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.

Module 03 Lab and Review

Lab 03a - Manage Azure resources by Using the Azure 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.
- ✓ Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Lab 03b - Manage Azure resources by 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.
- ✓ Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Lab 03c - Manage Azure resources by Using Azure 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.
- ✓ Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Lab 03d - Manage Azure resources by Using Azure 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.
- ✓ Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Module 03 Review Questions

Review Question 1

You are creating a new resource group to use for testing. Which two of the following parameters are required when you create a resource group with PowerShell or the CLI? Select two.

- Location
- Name
- Region
- Subscription
- Tag

Review Question 2

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

- Authenticates automatically for instant access to your resources.
- Each user account can be assigned multiple machines.
- Provides both Bash and PowerShell sessions.
- Provides an editor.
- Requires an Azure file share.

Review Question 3

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
- New-AzResourceGroup

Review Question 4

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
- Virtual machine

Review Question 5

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

- Functions
- Inputs
- Outputs
- Parameters

Review Question 6

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

- A Markdown document with a pointer table
- A JSON document with key-value pairs
- A TXT document with key-value pairs
- An XML document with element-value pairs

Review Question 7

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
- Resize your virtual machines to handle larger workloads

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Core Cloud Services - Manage services with the Azure portal¹¹**
- **Control and organize Azure resources with Azure Resource Manager¹²**
- **Build Azure Resource Manager templates¹³**
- **Automate Azure tasks using scripts with PowerShell¹⁴**
- **Manage virtual machines with the Azure CLI¹⁵**

¹¹ <https://docs.microsoft.com/en-us/learn/modules/tour-azure-portal/>

¹² <https://docs.microsoft.com/en-us/learn/modules/control-and-organize-with-azure-resource-manager/>

¹³ <https://docs.microsoft.com/en-us/learn/modules/build-azure-vm-templates/>

¹⁴ <https://docs.microsoft.com/en-us/learn/modules/automate-azure-tasks-with-powershell/>

¹⁵ <https://docs.microsoft.com/en-us/learn/modules/manage-virtual-machines-with-azure-cli/>

Answers

Review Question 1

You are creating a new resource group to use for testing. Which two of the following parameters are required when you create a resource group with PowerShell or the CLI? Select two.

- Location
- Name
- Region
- Subscription
- Tag

Explanation

Location and Name are required by PowerShell (New-AzResourceGroup) and the CLI (az group create).

Review Question 2

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

- Authenticates automatically for instant access to your resources.
- Each user account can be assigned multiple machines.
- Provides both Bash and PowerShell sessions.
- Provides an editor.
- Requires an Azure file share.

Explanation

Each user account can be assigned multiple machines, is not true. The cloud shell is assigned one machine per user account.

Review Question 3

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
- New-AzResourceGroup

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.

Review Question 4

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
- Virtual machine

Explanation

Tenant. A tenant cannot be moved between subscriptions.

Review Question 5

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

- Functions
- Inputs
- Outputs
- Parameters

Explanation

Inputs. Inputs is not a part of the template schema.

Review Question 6

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

- A Markdown document with a pointer table
- 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.

Review Question 7

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
- Resize your virtual machines to handle larger workloads

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.

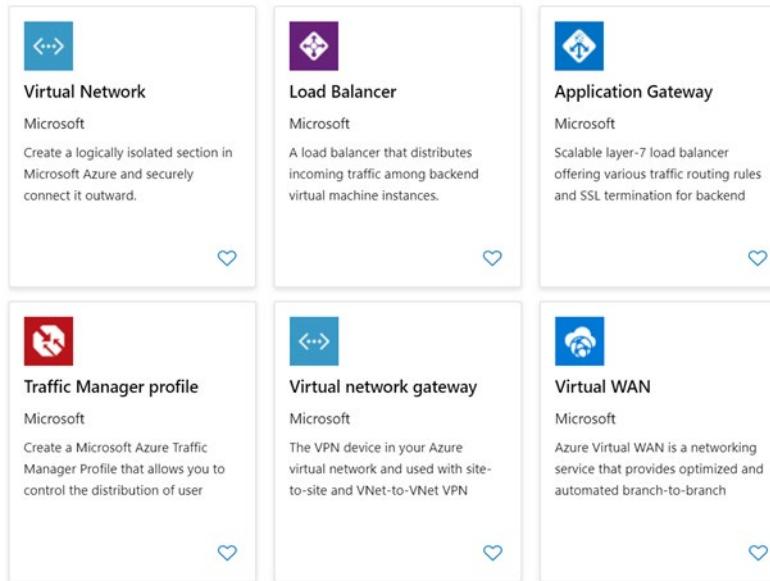
Module 4 Virtual Networking

Virtual Networks

Azure Networking Components

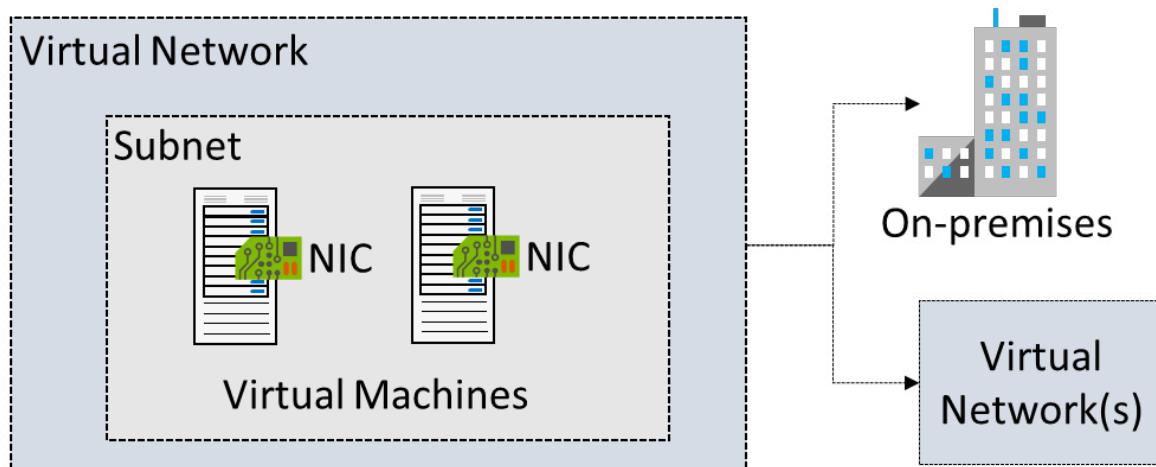
A major incentive for adopting cloud solutions such as Azure is to enable information technology (IT) departments to move server resources to the cloud. This can save money and simplify operations by removing the need to maintain expensive datacenters with uninterruptible power supplies, generators, multiple fail-safes, clustered database servers, and so on. 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 that can help organizations design and build cloud infrastructure services that meet their requirements. Azure has many networking components.



Virtual Networks

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.

For more information, [Virtual Network Documentation¹](#).

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. Each subnet must have a unique address range, specified in CIDR format. The address range cannot overlap with other subnets in the virtual network in the same subscription.



Name	Address range	IPv4 available addresses	Delegated to	Security group
subnet0	10.1.0.0/24	251	-	nsg0
subnet1	10.1.1.0/24	251	-	-
subnet2	10.1.2.0/24	251	-	nsg2
GatewaySubnet	10.1.255.0/24	251	-	-

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.

¹ <https://docs.microsoft.com/en-us/azure/virtual-network/>

- **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.
- ✓ Azure reserves the first three IP addresses and the last IP address in each subnet address range.

Implementing 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, although you can increase this limit to 500 by contacting Azure support.

- ✓ 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

The screenshot shows the 'Create virtual network' wizard in the Azure portal. The 'Basics' tab is selected. In the 'Project details' section, 'Subscription' is set to 'Visual Studio Enterprise'. Under 'Resource group', 'Lab04' is selected. In the 'Instance details' section, 'Name' is set to 'VNet2' and 'Region' is set to '(US) East US 2'.

- ✓ Always plan to use an address space that is not already in use in your organization, either on-premises or in other VNets. Even if you plan for a VNet to be cloud-only, you may want to make a VPN connection to it later. If there is any overlap in address spaces at that point, you will have to reconfigure or recreate the VNet. The next lesson will focus on IP addressing.

Demonstration - Creating 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.

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.

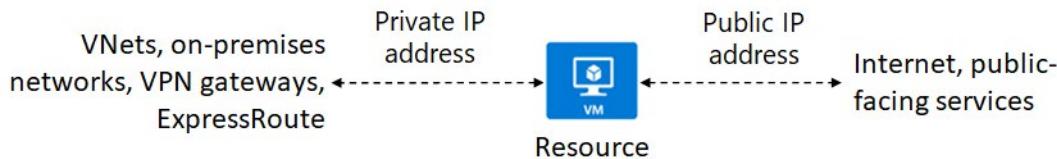
```
$mySubnet2 | Set-AzVirtualNetwork
```

6. Return to the portal and verify your new virtual network with subnet was created.

IP Addressing

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 IP addresses you can use in Azure. Virtual networks can contain both public and private IP address spaces.



- 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.

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 which require apps or services to have a static IP address.
 - 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.
- ✓ As a best practice you may decide to separate dynamically and statically assigned IP resources into different subnets. And, IP Addresses are never managed from within a virtual machine.

Creating 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 2 Public IP addresses being created- 1 IPv4 address and 1 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 it is associated to.
- **Static.** Static addresses are assigned when a public IP address is created. Static addresses are not released until a public IP address resource is deleted. If the address is not 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.

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

Feature	Basic SKU	Standard SKU
Redundancy	Not zone redundant	Zone redundant by default

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.

Network Security Groups

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.

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.

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	

- ✓ Generally, this is used for specific VMs with Network Virtual Appliances (NVAs) roles, otherwise it is recommended to link NSG to the subnet level and re-use across your VNETs and subnets.

For more information, [Network Security Groups²](#).

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), and Action (Allow or Deny). You cannot delete the default rules, but you can add other rules with a higher priority.

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.

² <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

Inbound rules

There are three default inbound security rules. The rules deny all inbound traffic except from the virtual network and Azure load balancers.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

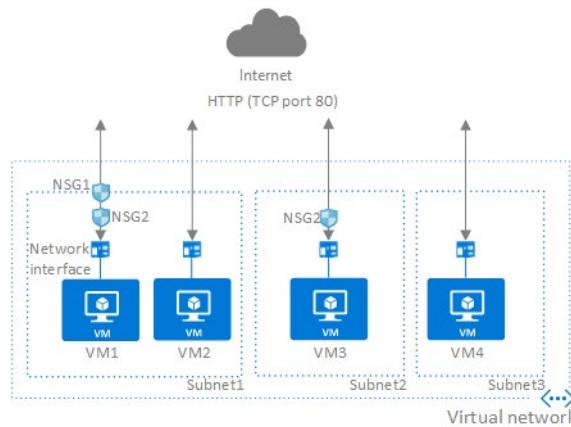
Outbound rules

There are three default outbound security rules. The rules only allow outbound traffic to the Internet and the virtual network.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

NSG Effective Rules

NSGs are evaluated independently, and an “allow” rule must exist at both levels otherwise traffic will not be admitted.



In the above example if there was incoming traffic on port 80, you would need to have the NSG at subnet level ALLOW port 80, and you would also need another NSG with 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 converse.

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.



Creating NSG Rules

It is easy to add inbound and outbound rules. There is a Basic and Advanced page. The advanced option lets you select from a large variety of services such as HTTPS, RDP, FTP, and DNS.

Add inbound security rule
UbuntuServer-nsg

Advanced

Service: Custom

* port ranges: 8080

* Priority: 310

* Name: Port_8080

HTTP
HTTPS
SSH
RDP
MS SQL
MySQL
PostgreSQL
Custom
FTP
SMTP
DNS (TCP)
DNS (UDP)

Service. The service specifies the destination protocol and port range for this rule. You can choose a predefined 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. If you choose a custom service then provide a single port, such as 80; a port range, such as 1024-65635; or a comma-separated list of single ports and/or port ranges, such as 80, 1024-65535. This specifies on which ports 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 – 100, 200, 300, etc. This is so it is easier to add new rules without editing existing rules. Enter a value between 100-4096 that is unique for all security rules within the network security group.

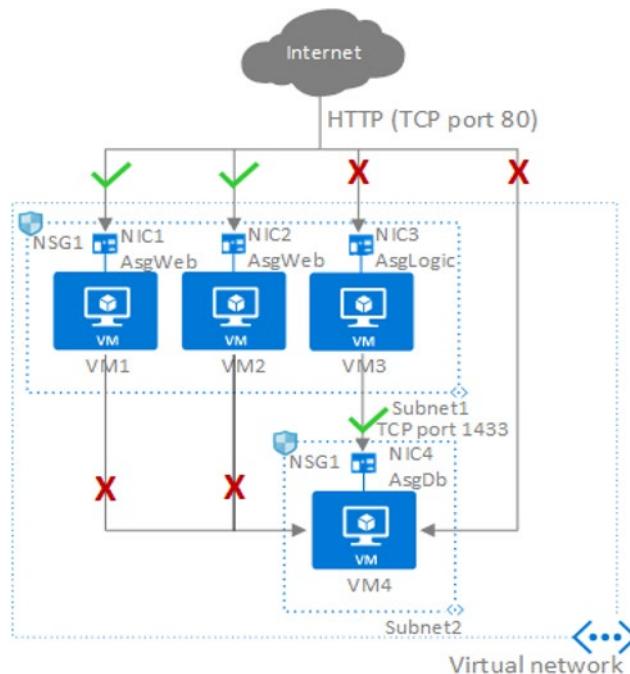
- ✓ Are there any services you are interested in?

Application Security Groups

Application Security Groups provide for the grouping of servers with similar port filtering requirements, and group together servers with similar functions, such as web servers.

- Allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses.
- Handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

Consider the following illustration.



In the illustration, NIC1 and NIC2 are members of the AsgWeb ASG. NIC3 is a member of the AsgLogic ASG. NIC4 is a member of the AsgDb ASG. Though each network interface in this example is a member of only one ASG, a network interface can be a member of multiple ASGs, up to the Azure limits. None of the network interfaces have an associated network security group. NSG1 is associated to both subnets and contains the following rules:

- Allow-HTTP-Inbound-Internet
- Deny-Database-All
- Allow-Database-BusinessLogic

The rules that specify an ASG as the source or destination are only applied to the network interfaces that are members of the ASG. If the network interface is not a member of an ASG, the rule is not applied to the network interface even though the network security group is associated to the subnet.

ASGs have the following constraints

- There are limits to the number of ASGs you can have in a subscription, in addition to other limits related to ASGs.
- You can specify one ASG as the source and destination in a security rule. You cannot specify multiple ASGs in the source or destination.

- All network interfaces assigned to an ASG have to exist in the same virtual network that the first network interface assigned to the ASG is in. For example, if the first network interface assigned to an ASG named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same ASG.
- If you specify an ASG as the source and destination in a security rule, the network interfaces in both ASGs must exist in the same virtual network. For example, if AsgLogic contained network interfaces from VNet1, and AsgDb contained network interfaces from VNet2, you could not assign AsgLogic as the source and AsgDb as the destination in a rule. All network interfaces for both the source and destination ASGs need to exist in the same virtual network.

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

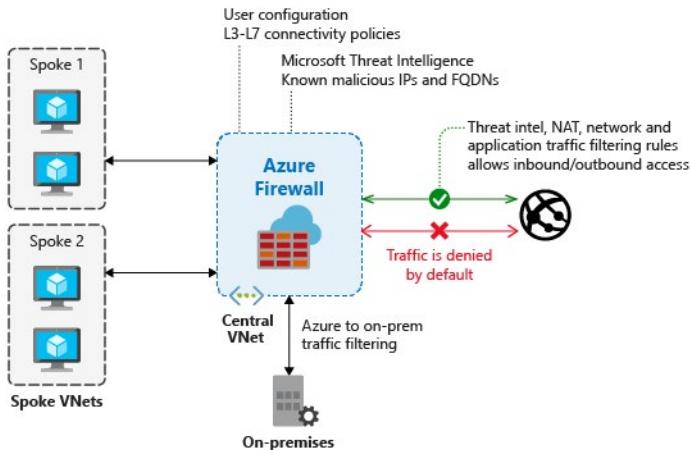
1. Select your new NSG.
2. Notice the NSG can be associated with subnets and network interfaces (summary information above the rules).
3. Notice the three inbound and three outbound NSG rules.
4. Under **Settings** select **Inbound security rules**.
5. Notice you can use **Default rules** to hide the 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.

Azure Firewall

Azure Firewall

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.

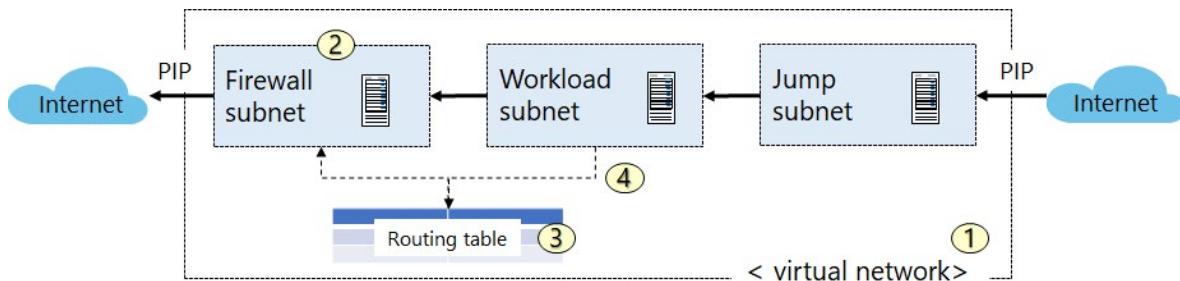


Azure Firewall features

- **Built-in high availability.** High availability is built in, so no additional load balancers are required and 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.

Implementing Azure Firewall

Let's consider a simple example where we want to use Azure Firewall to route protect our workload server by controlling the network traffic.



- Create the network infrastructure.** In this case, we have one virtual network with three subnets.
- Deploy the firewall.** The firewall is associated with the virtual network. In this case, it is in a separate subnet with a public and private IP address. The private IP address will be used in a new routing table.
- Create a default route.** Create a routing table to direct network workload traffic to the firewall. The route will be associated with the workload subnet. All traffic from that subnet will be routed to the firewall's private IP address.
- Configure an application rule.**

In production deployments, a **Hub and Spoke model**³ is recommended, where the firewall is in its own VNET, and workload servers are in peered VNETs in the same region with one or more subnets.

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
Rules			
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.

³ <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke>

- **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:** This can be 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:** Whether this is for 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. Note that wildcards can be used. An FQDN tag represents a group of fully qualified domain names (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)

The rules are terminating. Once a positive match is found, allowing the traffic through, no more rules are checked.

Azure DNS

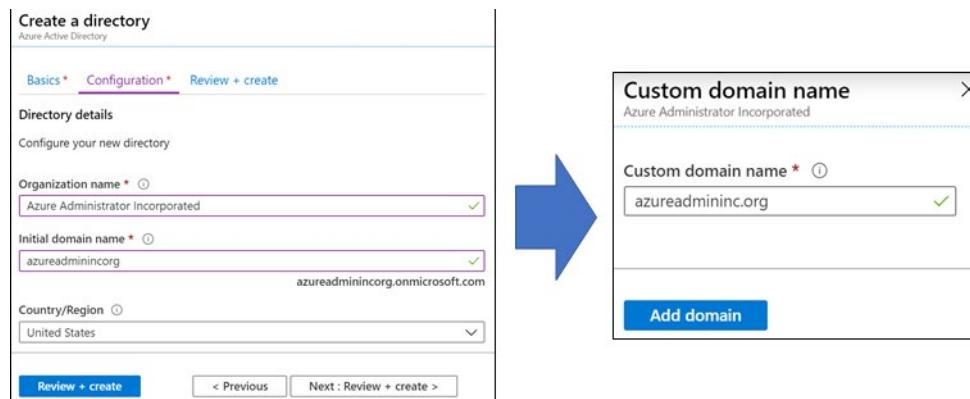
Domains and Custom Domains

Initial domain name

By default, when you create an Azure subscription an Azure AD domain is created for you. This instance of the domain has *initial domain name* in the form *domainname.onmicrosoft.com*. The initial domain name, while fully functional, is intended primarily to be used as a bootstrapping mechanism until a custom domain name is verified.

Custom domain name

Although the initial domain name for a directory can't be changed or deleted, you can add any routable custom domain name you control. This simplifies the user sign-on experience by allowing user to logon with credentials they are familiar with. For example, a contosogold.onmicrosoft.com, could be assigned a simpler custom domain name of contosogold.com.



Practical information about domain names

- Only a global administrator can perform domain management tasks in Azure AD, by default this is the user who created the subscription.
- Domain names in Azure AD are globally unique. If one Azure AD directory has verified a domain name, then no other Azure AD directory can verify or use that same domain name.
- Before a custom domain name can be used by Azure AD, the custom domain name must be added to your directory and verified. This is covered in the next topic.

For more information, [Managing custom domain names in your Azure Active Directory⁴](#).

Verifying Custom Domain Names

When an administrator adds a custom domain name to an Azure AD, it is initially in an unverified state. Azure AD will not allow any directory resources to use an unverified domain name. This ensures that only one directory can use a domain name, and the organization using the domain name owns that domain name.

⁴ <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-domains-manage-azure-portal>

So, after adding the custom domain name, you must demonstrate ownership of the domain name. This is called verification, and is done by adding a DNS record (MX or TXT) that is provided by Azure into your company's DNS zone. Once this record is added, Azure will query the DNS domain for the presence of the record. This could take several minutes or several hours. If Azure verifies the presence of the DNS record, it will then add the domain name to the subscription.

azureadmininc.org
Custom domain name

Delete | Got feedback?

Record type

TXT MX

Alias or host name

@

Destination or points to address

MS=ms79094380

TTL

3600

[Share these settings via email](#)

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

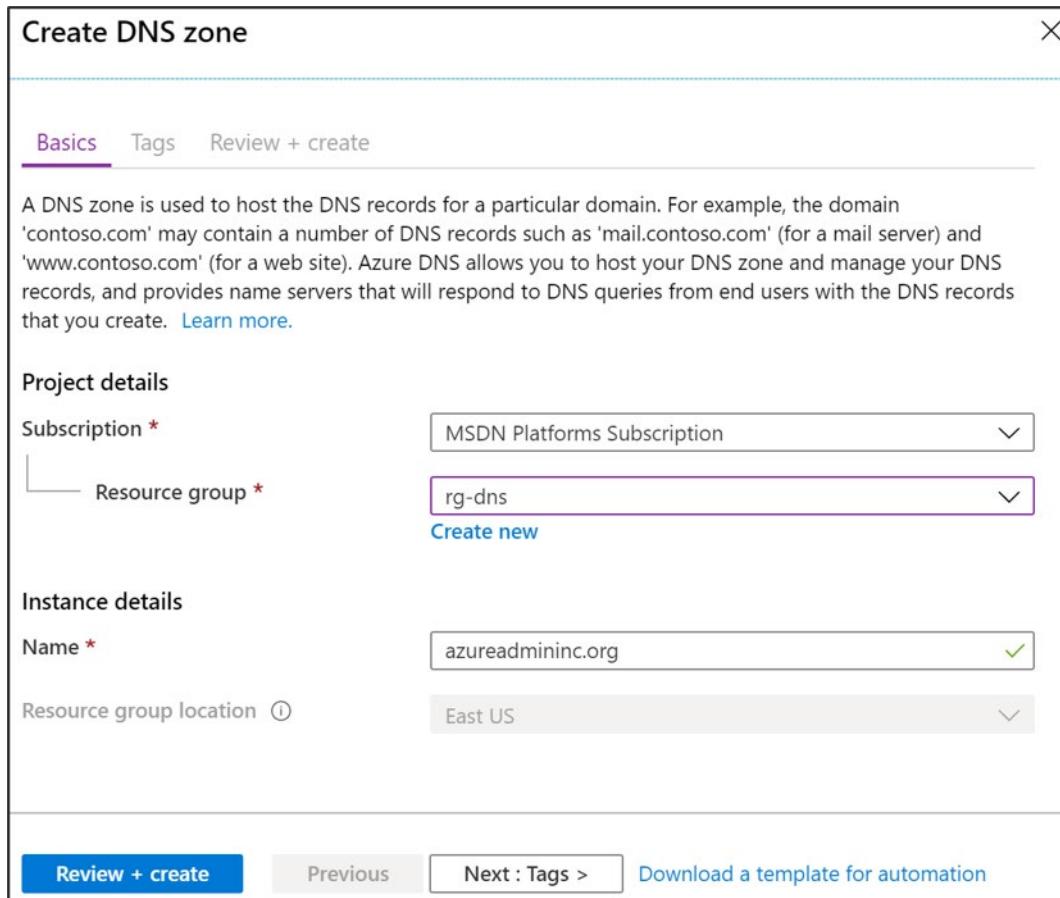
- ✓ Notice you can use a TXT or MX record.

Azure DNS Zones

Azure DNS provides a reliable, secure DNS service to manage and resolve domain names in a virtual network without your 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 portal you can easily add a DNS zone and then view information including name, number of records, resource group, location (always global), subscription, and name servers.



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.
- Only one set of addresses can be configured with the domain name registrar.
- ✓ 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.

DNS Delegation

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.

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':

The screenshot shows the Azure DNS zone configuration for the domain `azureadmininc.org`. It includes the following details:

- Resource group:** rg-dns (change)
- Subscription:** MSDN Platforms Subscription
- Subscription ID:** [Redacted]
- Tags:** Click here to add tags
- Name servers:**
 - Name server 1: ns1-02.azure-dns.com.
 - Name server 2: ns2-02.azure-dns.net.
 - Name server 3: ns3-02.azure-dns.org.
 - Name server 4: ns4-02.azure-dns.info.

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.

- ✓ 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 sub-domain 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 sub-domain 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.

- ✓ 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`.

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

You can add up to 20 records to any record set. 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.

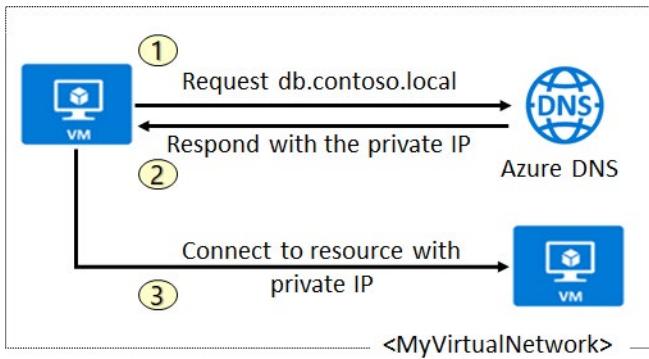
The **Add record set** page will change depending on the type of record you select. For an A record, you will need the TTL (Time to Live) and IP address. The time to live, or TTL, specifies how long each record is cached by clients before being requeried.

The dialog shows the following fields:

- Name:** helloworld (highlighted with a purple border)
- Type:** A (selected from a dropdown menu)
- Alias record set:** No (radio button selected)
- TTL *:** 1 (input field)
- TTL unit:** Hours (dropdown menu)
- IP address:** 0.0.0.0 (input field)

DNS for Private Domains

By using private DNS zones, you can use your own custom domain names rather than the Azure-provided names available today. 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.



If you specify a registration virtual network, the DNS records for the VMs from that virtual network that are registered to the private zone are not viewable or retrievable from the Azure Powershell and Azure CLI APIs, but the VM records are indeed registered and will resolve successfully.

Azure DNS benefits

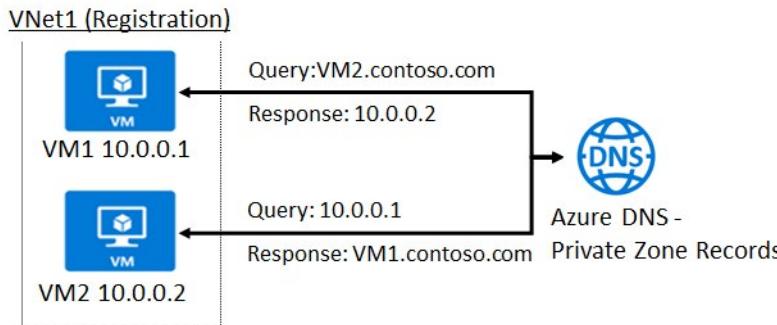
- **Removes the need for custom DNS solutions.** Previously, many customers created custom DNS solutions to manage DNS zones in their virtual network. You can now perform DNS zone management by using the native Azure infrastructure, which removes the burden of creating and managing custom DNS solutions.
- **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.

Private Zone scenarios

Scenario 1: Name resolution scoped to a single virtual network

In this scenario, you have a virtual network in Azure that has a number of Azure resources in it, including virtual machines (VMs). You want to resolve the resources from within the virtual network via a specific domain name (DNS zone), and you 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.

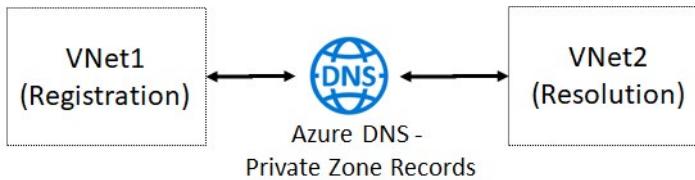


In this scenario, VNET1 contains two VMs (VM1 and VM2). Each of these VMs have Private IPs. So, if you create a Private Zone named contoso.com and link this virtual network as a Registration virtual network, Azure DNS will automatically create two A records in the zone. Now, DNS queries from VM1 to resolve VM2.contoso.com will receive a DNS response that contains the Private IP of VM2. Furthermore, a Reverse DNS query (PTR) for the Private IP of VM1 (10.0.0.1) 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.com*.
- 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.



With this setup, you will observe the following behavior for forward and reverse DNS queries:

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.

- ✓ There is also **Split-Horizon functionality⁵** scenario.

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. Make a note of your resource group name.

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 <resourcegroupname>
```

3. Get information about your DNS record set.

```
Get-AzDnsRecordSet -ResourceGroupName <resourcegroupname> -ZoneName contoso.internal.com
```

⁵ <https://docs.microsoft.com/en-us/azure/dns/private-dns-scenarios#scenario-split-horizon-functionality>

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. Make a note of the resource group.
4. Open the Cloud Shell.
5. 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, [Nslookup⁶](#)

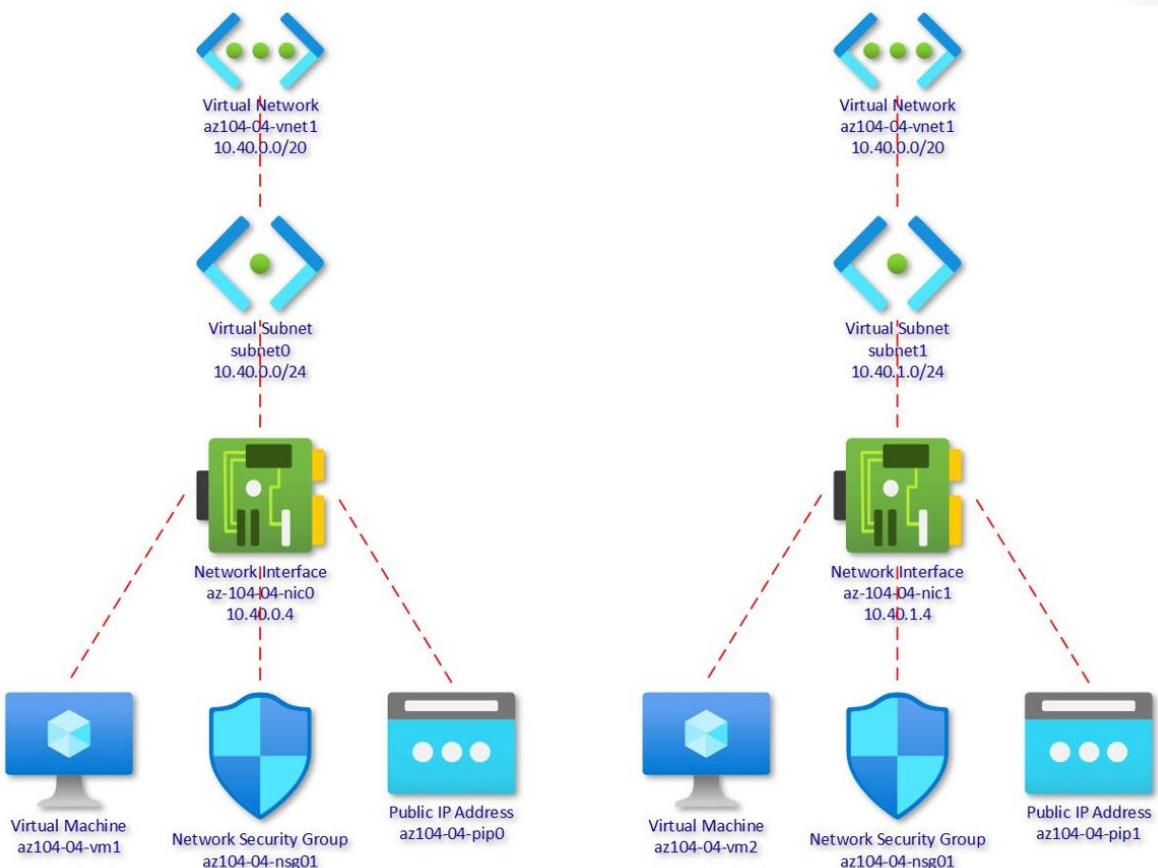
⁶ <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup>

Module 04 Lab and Review

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

Module 04 Review Questions

Review Question 1

Your company has an existing Azure tenant named `alpineskihouse.onmicrosoft.com`. The company wants to start using `alpineskihouse.com` for their Azure resources. You add a custom domain to Azure.

Now, you need to add a DNS record to prepare for verifying the custom domain. Which two of the following record types could you create?

- Add an PTR record to the DNS zone.
- Add a TXT record to the DNS zone.
- Add an MX record to the DNS zone.
- Add an SRV record to the DNS zone.
- Add a CNAME record to the DNS zone.

Review Question 2

You are planning to configure networking in Microsoft Azure. Your company has a new Microsoft Azure presence with the following network characteristics:

- 1 Virtual Network.
- 1 subnet using 192.168.0.0/23 (does not have existing resources).

Your on-premises data center has the following network characteristics:

- 10 subnets using 192.168.1.0/24 through 192.168.10.0/24.

The company intends to use 192.168.1.0/24 on-premises and 192.168.0.0/24 in Azure. You need to update your company's environment to enable the needed functionality. What should you do? (Each answer represents part of the solution. Choose two.)

- Delete 192.168.0.0/23 from Azure.
- Delete 192.168.1.0/24 in the on-premises environment.
- Create a matching public subnet in Azure and in the on-premises environment.
- Create a subnet for 192.168.0.0/23 in the on-premises environment.
- Create a subnet for 192.168.0.0/24 in Azure.

Review Question 3

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. The first set of VMs that you are deploying have the following requirements:

- Consumers on the internet must be able to communicate directly with the web application on the VMs.
- The IP configuration must be zone redundant.

You need to configure the environment to prepare for the first VM. Additionally, you need to 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.
- Create a basic public IP address. After the first VM is created, remove the private IP address and assign the public IP address to the NIC.

Review Question 4

You deploy a new domain named contoso.com to domain controllers in Azure. You have the following domain-joined VMs in Azure:

- VM1 at 10.20.30.10
- VM2 at 10.20.30.11
- VM3 at 10.20.30.12
- VM99 at 10.20.40.101

You need to add DNS records so that the hostnames resolve to their respective IP addresses. Additionally, you need to add a DNS record so that intranet.contoso.com resolves to VM99. What should you do? (Each answer presents part of the solution. Choose two.)

- Add AAAA records for each VM.
- Add A records for each VM.
- Add a TXT record for intranet.contoso.com with the text of VM99.contoso.com.
- Add an SRV record for intranet.contoso.com with the target pointing at VM99.contoso.com
- Add a CNAME record for intranet.contoso.com with a value of VM99.contoso.com.

Review Question 5

Your company is preparing to move some services and VMs to Microsoft Azure. The company has opted to use Azure DNS to provide name resolution. A project begins to configure the name resolution. The project identifies the following requirements:

- A new domain will be used.
- The domain will have DNS records for internal and external resources.
- Minimize ongoing administrative overhead.

You need to prepare and configure the environment with a new domain name and a test hostname of WWW. Which of the following steps should you perform? (Each answer presents part of the solution. Choose three.)

- Register a domain name with a domain registrar.
- Register a domain name with Microsoft Azure.
- Delegate the new domain name to Azure DNS.
- Add an Address (A) record for Azure name servers in the zone.
- Add DNS glue records to point to the Azure name servers.
- Add a record for WWW.

Review Question 6

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 to update the VM configuration to provide the following functionality:

- Enable direct communication from the internet to TCP port 443.
- Maintain existing communication across the 10.10.8.0/24 and 10.20.8.0/24 subnets.
- Maintain a simple configuration whenever possible.

You need to update the VM configuration to support the new functionality. 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.
- Add a third NIC and associate 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.

Review Question 7

You're currently using network security groups (NSGs) to control how your network traffic flows in and out of your virtual network subnets and network interfaces. You want to customize how your NSGs work. For all incoming traffic, you need to apply your security rules to both the virtual machine and subnet level. Which of the following options will let you accomplish this? (Choose two)

- Configure the AllowVNetInbound security rule for all new NSGs.
- Create rules for both NICs and subnets with an allow action.
- Delete the default rules.
- Add rules with a higher priority than the default rules.

Review Question 8

You have an Azure virtual machine that has a multi-network interface with private IP addressing. To which IP address in Azure managed DNS is the hostname mapped? Select one.

- each interface
- the most recently created network interface
- the primary network interface
- the first created network interface

Review Question 9

You need to ensure that Azure DNS can resolve names for your registered domain. What should you implement? Select one.

- zone delegation
- a CNAME record
- an MX record
- a secondary zone
- a primary zone with a NS record

Review Question 10

You are configuring the Azure Firewall. You need to allow Windows Update network traffic through the firewall. Which of the following should you use?

- Application rules
- Destination inbound rules
- NAT rules
- Network rules

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Networking Fundamentals - Principles⁷**
- **Design an IP addressing schema for your Azure deployment⁸**
- **Secure and isolate access to Azure resources by using network security groups and service endpoints⁹**

⁷ <https://docs.microsoft.com/en-us/learn/modules/network-fundamentals/>

⁸ <https://docs.microsoft.com/en-us/learn/modules/design-ip-addressing-for-azure/>

⁹ <https://docs.microsoft.com/en-us/learn/modules/secure-and-isolate-with-nsg-and-service-endpoints/>

Answers

Review Question 1

Your company has an existing Azure tenant named alpineskihouse.onmicrosoft.com. The company wants to start using alpineskihouse.com for their Azure resources. You add a custom domain to Azure.

Now, you need to add a DNS record to prepare for verifying the custom domain. Which two of the following record types could you create?

- Add an PTR record to the DNS zone.
- Add a TXT record to the DNS zone.
- Add an MX record to the DNS zone.
- Add an SRV record to the DNS zone.
- Add a CNAME record to the DNS zone.

Explanation

By default, Azure will prompt you to create a custom TXT record in your DNS zone to verify a custom domain. Optionally, you can use an MX record instead. The result is the same. Other record types are not supported.

Review Question 2

You are planning to configure networking in Microsoft Azure. Your company has a new Microsoft Azure presence with the following network characteristics:

Your on-premises data center has the following network characteristics:

The company intends to use 192.168.1.0/24 on-premises and 192.168.0.0/24 in Azure. You need to update your company's environment to enable the needed functionality. What should you do? (Each answer represents part of the solution. Choose two.)

- Delete 192.168.0.0/23 from Azure.
- Delete 192.168.1.0/24 in the on-premises environment.
- Create a matching public subnet in Azure and in the on-premises environment.
- Create a subnet for 192.168.0.0/23 in the on-premises environment.
- Create a subnet for 192.168.0.0/24 in Azure.

Explanation

First, you need to delete 192.168.0.0/23 from Azure. It overlaps with 192.168.1.0/24, which you intend to use for on-premises. Second, you need to create a subnet for 192.168.0.0/24 in Azure to enable usage in Azure.

Review Question 3

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. The first set of VMs that you are deploying have the following requirements:

You need to configure the environment to prepare for the first VM. Additionally, you need to 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.
- Create a basic public IP address. After the first VM is created, remove the private IP address and assign the public IP address to the NIC.

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.

Review Question 4

You deploy a new domain named contoso.com to domain controllers in Azure. You have the following domain-joined VMs in Azure:

You need to add DNS records so that the hostnames resolve to their respective IP addresses. Additionally, you need to add a DNS record so that intranet.contoso.com resolves to VM99. What should you do? (Each answer presents part of the solution. Choose two.)

- Add AAAA records for each VM.
- Add A records for each VM.
- Add a TXT record for intranet.contoso.com with the text of VM99.contoso.com.
- Add an SRV record for intranet.contoso.com with the target pointing at VM99.contoso.com
- Add a CNAME record for intranet.contoso.com with a value of VM99.contoso.com.

Explanation

In this scenario, the hostnames have IPv4 IP addresses. Thus, to resolve those hostnames, you must add A records for each of the VMs. To enable intranet.contoso.com to resolve to VM99.contoso.com, you need to add a CNAME record. A CNAME record is often referred to as an "alias".

Review Question 5

Your company is preparing to move some services and VMs to Microsoft Azure. The company has opted to use Azure DNS to provide name resolution. A project begins to configure the name resolution. The project identifies the following requirements:

You need to prepare and configure the environment with a new domain name and a test hostname of WWW. Which of the following steps should you perform? (Each answer presents part of the solution. Choose three.)

- Register a domain name with a domain registrar.
- Register a domain name with Microsoft Azure.
- Delegate the new domain name to Azure DNS.
- Add an Address (A) record for Azure name servers in the zone.
- Add DNS glue records to point to the Azure name servers.
- Add a record for WWW.

Explanation

For private domain names, you must register with a registrar because Azure isn't a registrar. Thereafter, you need to delegate the new domain name to Azure DNS, which enables Azure DNS to be authoritative for the domain. After delegation, you should add a test hostname of WWW and test name resolution.

Review Question 6

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 to update the VM configuration to provide the following functionality:

You need to update the VM configuration to support the new functionality. 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.
- Add a third NIC and associate 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.

Review Question 7

You're currently using network security groups (NSGs) to control how your network traffic flows in and out of your virtual network subnets and network interfaces. You want to customize how your NSGs work. For all incoming traffic, you need to apply your security rules to both the virtual machine and subnet level.

Which of the following options will let you accomplish this? (Choose two)

- Configure the AllowVNetInbound security rule for all new NSGs.
- Create rules for both NICs and subnets with an allow action.
- Delete the default rules.
- Add rules with a higher priority than the default rules.

Explanation

You should add rules with a higher priority than the default rules if needed, as you cannot delete the default rules. Also, in order to meet the requirement to apply security rules to both VM and subnet level, you should create rules with an allow action for both. There is no need to configure the AllowVnetInbound rule as it as a default rule for any new security group you create.

Review Question 8

You have an Azure virtual machine that has a multi-network interface with private IP addressing. To which IP address in Azure managed DNS is the hostname mapped? Select one.

- each interface
- the most recently created network interface
- the primary network interface
- the first created network interface

Explanation

When you create a virtual machine (VM), a mapping for the hostname to its private IP address is added to the Azure-managed DNS servers. In case of a multi-network interface VM, the hostname is mapped to the private IP address of the primary network interface.

Review Question 9

You need to ensure that Azure DNS can resolve names for your registered domain. What should you implement? Select one.

- zone delegation
- a CNAME record
- an MX record
- a secondary zone
- a primary zone with a NS record

Explanation

Once you create your DNS zone in Azure DNS, you need to set up NS records in the parent zone to ensure that Azure DNS is the authoritative source for name resolution for your zone. For domains purchased from a registrar, your registrar will offer the option to set up these NS records. When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS. Domain delegation does not require the name server name to use the same top-level domain as your domain.

Review Question 10

You are configuring the Azure Firewall. You need to allow Windows Update network traffic through the firewall. Which of the following should you use?

- Application rules
- Destination inbound rules
- NAT 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.

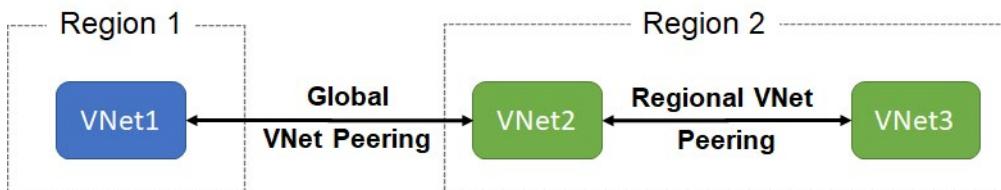
Module 5 Intersite Connectivity

VNet Peering

VNet Peering

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.

Global VNet peering special requirements

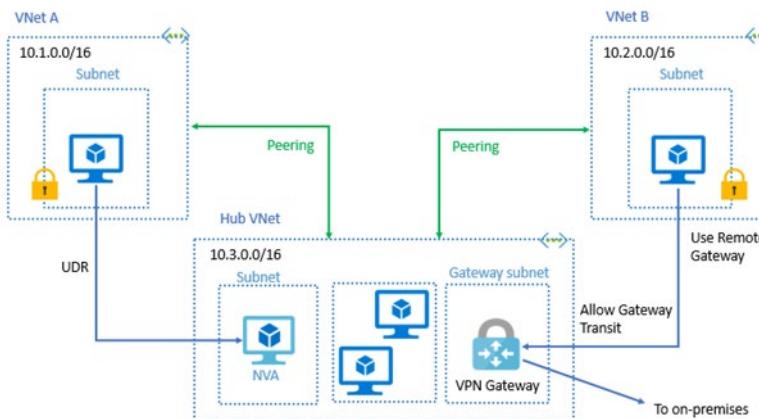
Global VNet peering has the same benefits and configuration steps as regional peering, but there are some special requirements.

- **Cloud 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.
- **Virtual network resources.** Resources in one virtual network cannot communicate with the IP address of an Azure internal load balancer in the peered virtual network. The load balancer and the resources that communicate with it must be in the same virtual network.

For more information, [Virtual network peering¹](#)

Gateway Transit and Connectivity

When virtual networks are peered, you can configure a VPN gateway in the peered virtual network as a transit point. In this case, a peered virtual network can use 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.

¹ <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

- ✓ The default VNet peering configuration provides full connectivity. Network security groups can be applied in either virtual network to block access to other virtual networks or subnets, if desired. When configuring virtual network peering, you can either open or close the network security group rules between the virtual networks.

Configure 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.

Configuration

Configure virtual network access settings

Allow virtual network access from vnet1 to vnet2 ⓘ

Disabled Enabled

Configure forwarded traffic settings

Allow forwarded traffic from vnet2 to vnet1 ⓘ

Disabled Enabled

Configure gateway transit settings

Allow gateway transit ⓘ

Configure Remote Gateways settings

Use remote gateways ⓘ

Allow forwarded traffic. Allows traffic not originating from within the peer virtual network into your virtual network.

Allow gateway transit. Allows the peer virtual network to use your virtual network gateway. The peer cannot already have a gateway configured.

- ✓ When you add a peering on one virtual network, the second virtual network configuration is automatically added.
- ✓ If you select 'Allow gateway transit' on one virtual network; then you should select 'Use remote gateways' on the other virtual network.

Service Chaining

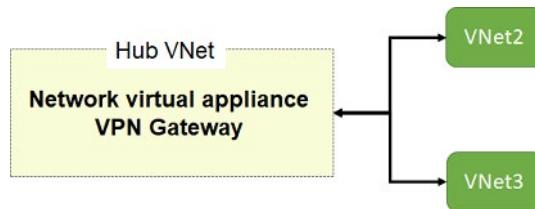
VNet Peering is nontransitive. This means that if you establish VNet Peering between VNet1 and VNet2 and between VNet2 and VNet3, VNet Peering capabilities do not apply between VNet1 and VNet3.

However, you can leverage user-defined routes and service chaining to implement custom routing that will provide 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

You can deploy hub-and-spoke networks, where the hub virtual network can host infrastructure components such as a 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 enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway, in a peered virtual network, through user-defined routes.

Checking connectivity

SETTINGS	NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
DNS servers Peering	myVirtualNetwork1-myVirtualNetwork2	Updating	myVirtualNetwork2	Disabled

You can check the status of the VNet peering. The peering is not successfully established until the peering status for both virtual network peerings shows **Updating**.

- **Updating.** 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, the status is changed from Initiated to 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 **name** for the first virtual network peering. For example, VNet1toVNet2.
 - In the **Virtual network** drop-down, select the second virtual network you would like to peer with.
 - Note the region, this will be needed when you configure the VPN gateway.
 - Provide a name for the second virtual network peering. For example, VNet2toVNet1.
 - Use the informational icons to review the network access, forwarded traffic, and gateway transit settings.
 - Check the box for **Allow gateway transit**. Note the error that the virtual network does not have a gateway.
 - Make sure the **Allow gateway transit** check box is not selected.
 - Click **OK** to save your settings.

Configure a VPN gateway

1. In the **Azure portal**, search for **virtual network gateways**.
2. Select **+ Add**.
 - Provide a **name** for your virtual network gateway. For example, VNet1Gateway.
 - Ensure the gateway is in the same region as the first virtual network.
 - In the **virtual network** drop-down select the first virtual network.
 - In the **Public IP address** area, **Create new** and give the IP address a name.
 - Click **Create and review**. Address any validation errors.
 - Click **Create**.
3. Monitor the notifications to ensure the gateway is successfully created.

Allow gateway transit

1. In the **Azure portal**, return to your first virtual network.
2. On the **Overview** blade, notice the new **Connected device** for your VPN gateway.
3. Select the gateway and notice you can perform a health check and review access statistics.
4. Return to the previous page and under **SETTINGS**, select **Peerings**.
 - Select the peering and enable **Allow gateway transit**. Notice the previous error has been resolved.
 - Notice after making this selection, **Use remote gateways** is disabled.
5. **Save** your changes.

Confirm VNet peering on the second virtual network

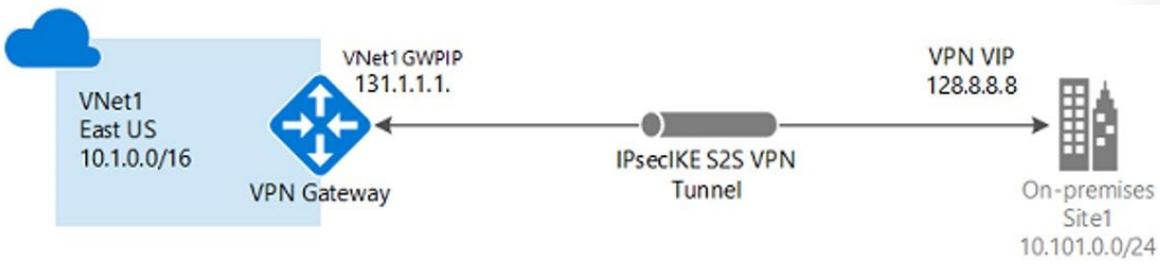
1. In the **Azure portal**, select the second virtual network.
2. Under **SETTINGS**, select **Peerings**.

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. Click the peering.
 - Notice that **Allow gateway transit** cannot be selected.
 - Use the informational icon to review the **Use remote gateways** setting.
6. **Discard** your changes.

VPN Gateway Connections

VPN Gateways

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. 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.



- **Site-to-site** connections connect on-premises datacenters to Azure virtual networks
- **Network-to-network** connections connect Azure virtual networks (custom)
- **Point-to-site (User VPN)** connections connect individual devices to Azure virtual networks

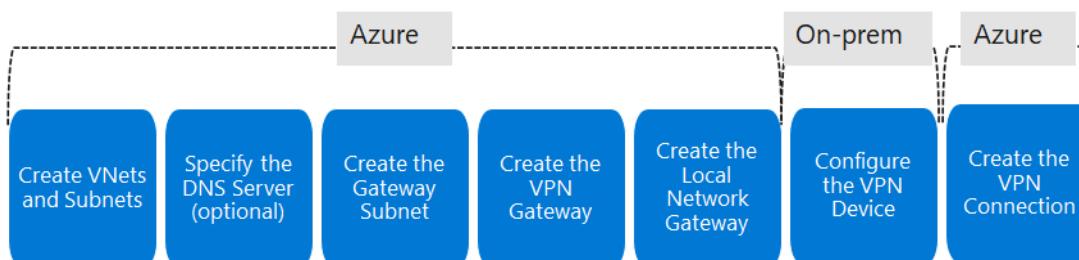
A virtual network gateway is composed of two or more VMs that are deployed to a specific subnet you create called the gateway subnet. Virtual network gateway VMs contain routing tables and run specific gateway services. These VMs are created when you create the virtual network gateway. You can't directly configure the VMs that are part of the virtual network gateway.

VPN gateways can be deployed in Azure Availability Zones. This brings resiliency, scalability, and higher availability to virtual network gateways. Deploying gateways in Azure Availability Zones physically and logically separates gateways within a region, while protecting your on-premises network connectivity to Azure from zone-level failures.

- ✓ Creating a virtual network gateway can take up to 45 minutes to complete.

Implement Site-to-Site Connections

Here are the steps to creating a VNet-to-VNet connections. The on-premises part is necessary only if 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. You need to coordinate with your

on-premises network administrator to reserve an IP address range that you can use specifically for this virtual network.

Specify the DNS server (optional). DNS is not required to create a Site-to-Site connection. However, if you want to have name resolution for resources that are deployed to your virtual network, you should specify a DNS server in the virtual network configuration.

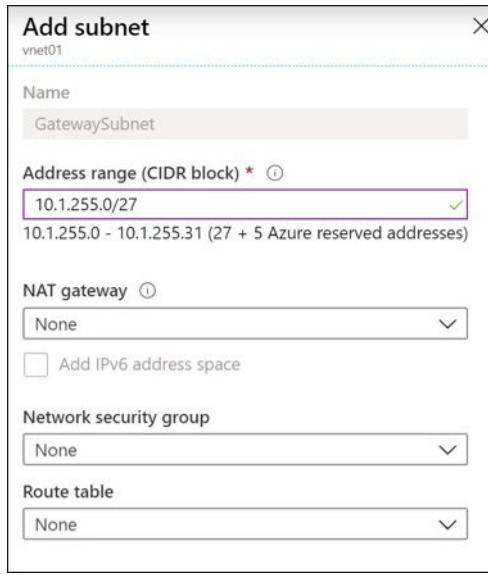
- ✓ Take time to carefully plan your network configuration. If a duplicate IP address range exists on both sides of the VPN connection, traffic will not route the way you may expect it to.

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 additional configuration requirements.

When you create your gateway subnet, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings. You must never deploy other resources (for example, additional VMs) to the gateway subnet. The gateway subnet must be named *GatewaySubnet*.

To deploy a gateway in your virtual network simply add a gateway subnet.



- ✓ When working with gateway subnets, avoid associating a network security group (NSG) to the gateway subnet. Associating a network security group to this subnet may cause your VPN gateway to stop functioning as expected.
- ✓ This is the same step in configuring VNet Peering.

VPN Gateway Configuration

The VPN gateway settings that you chose are critical to creating a successful connection.

Create virtual network gateway

Instance details

Name *	<input type="text"/>
Region *	(US) East US
Gateway type *	<input checked="" type="radio"/> VPN <input type="radio"/> ExpressRoute
VPN type *	<input checked="" type="radio"/> Route-based <input type="radio"/> Policy-based
SKU *	VpnGw1
Generation	Generation1
VIRTUAL NETWORK	
Virtual network *	<input type="text"/>
<small>Only virtual networks in the currently selected subscription and region are listed.</small>	
Enable active-active mode *	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Configure BGP ASN *	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

- **Gateway type.** VPN or ExpressRoute.
- **VPN Type.** Route based or Policy based. The type of VPN you can choose depends on the make and model of your VPN device, and the kind of VPN connection you intend to create. Choose a route-based gateway if you intend to use point-to-site, inter-virtual network, or multiple site-to-site connections; if you are creating a VPN type gateway to coexist with an ExpressRoute gateway; or if you need to use IKEv2. Policy-based gateways support only IKEv1. Most VPN types are Route-based.
- **SKU.** Use the drop-down to select a gateway SKU. Route-based VPN types are offered in three SKUs: Basic, Standard, and High performance. Standard or High performance must be chosen if you are using ExpressRoute. A high performance SKU must be selected if you are using active-active mode. 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. Changing generation or changing SKUs across generations is not allowed. 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.
- ✓ After the gateway is created, view the IP address that has been assigned to it by looking at the virtual network in the portal. The gateway should appear as a connected device.

VPN Gateway Types

When you create the virtual network gateway for a VPN gateway configuration, 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.

The VPN type you select must satisfy all the connection requirements for the solution you want to create. For example, if you want to create a S2S VPN gateway connection and a P2S VPN gateway connection for the same virtual network, you would use VPN type Route-based because P2S requires a Route-based VPN type. You would also need to verify that your VPN device supported a Route-based VPN connection.

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 usually 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 1 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.
- ✓ Once a virtual network gateway has been created, you can't change the VPN type.

Gateway SKUs and Generations

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.

- ✓ 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 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 *

IP address * ⓘ

Address space ⓘ

192.168.3.0/24	...
Add additional address range	...

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. For example: 192.168.0.0/16. 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.

Configure the On-Premises VPN device

Microsoft has validated a list of standard VPN devices that should work well with the VPN gateway. This list was created in partnership with device manufacturers like Cisco, Juniper, Ubiquiti, and Barracuda Networks. If you don't observe your device listed in the validated VPN devices table (reference link), your device may still work with a Site-to-Site connection. Contact your device manufacturer for additional support and configuration instructions.

To configure your VPN device, you need the following:

- **A shared key.** This is the same shared key that you will specify when creating the VPN connection (next step).
- **The public IP address of your VPN gateway.** When you created the VPN gateway you may have configured a new public IP address or used an existing IP address.
- ✓ Depending on the VPN device that you have, you may be able to **download a VPN device configuration script²**.

For more information, **Validated VPN devices list³**.

² <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-download-vpndevicescript>

³ <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices>

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.

The screenshot shows two overlapping windows in the Azure portal. The left window is titled 'Add connection' and has 'vng01' in the top right corner. It contains fields for 'Name' (set to 'Azure-to-OnPrem'), 'Connection type' (set to 'Site-to-site (IPSec)'), and 'Virtual network gateway' (set to 'vng01'). Below these are sections for 'Local network gateway' (set to 'Azure-to-OnPrem') and 'Shared key (PSK)' (set to 'abc123'). The right window is titled 'Choose local network gateway...' and shows a list with a single item: 'Azure-to-OnPrem NetworkRG'. A 'Create new' button is also visible in this window.

- **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. The concept is similar here, except that rather than connecting to a VPN device, you're connecting to another virtual network gateway.

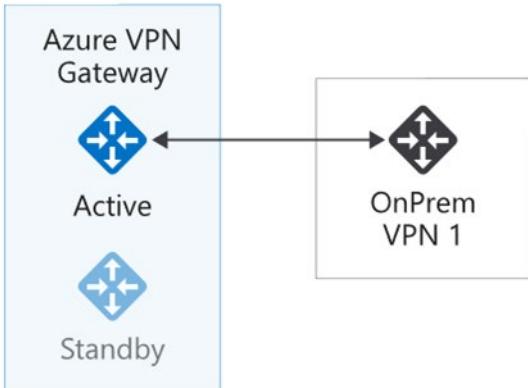
Verify the VPN Connection

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.

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.



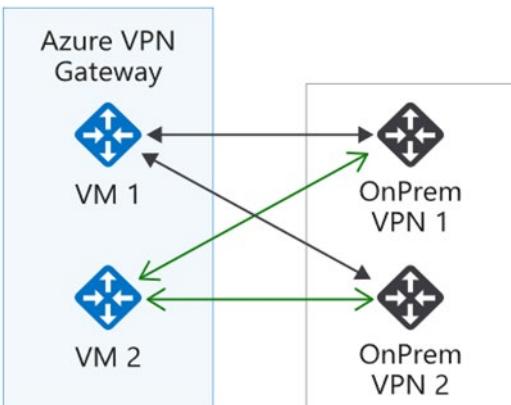
Active/active

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. Note that 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.

Because the Azure gateway instances are in active-active configuration, the traffic from your Azure virtual network to your on-premises network will be routed through both tunnels simultaneously, even if your on-premises VPN device may favor one tunnel over the other. Note though 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 Gateway Connections

In this demonstration, we will explore virtual network gateways.

Note: This demonstration works best with two virtual networks with subnets. All the steps are in the portal.

Explore the Gateway subnet blade

1. For one of your virtual network, 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 netowrk 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.

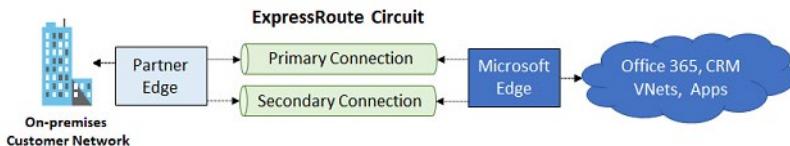
Explore adding a connection between the virtual networks

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.

ExpressRoute Connections

ExpressRoute

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a dedicated private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and CRM Online.



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, which makes it excellent for scenarios like periodic data migration, replication for business continuity, disaster recovery, and other high-availability strategies. It can be 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 environment in an Azure virtual private cloud and your on-premises production environments.

Extend and connect your datacenters

Use ExpressRoute to both 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.

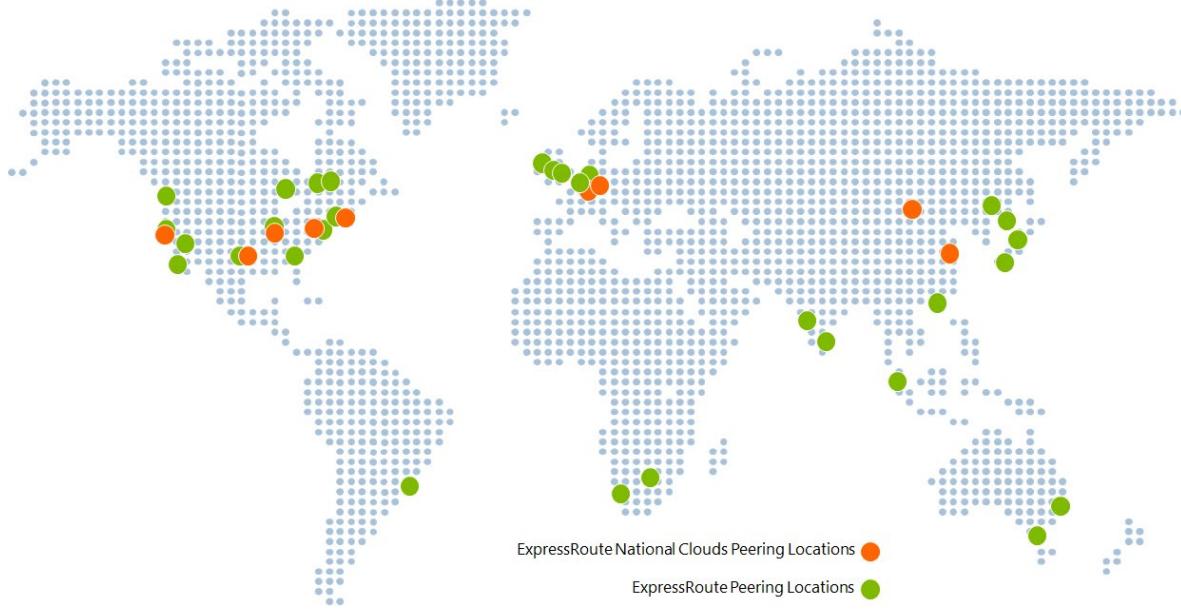
Build hybrid applications

With predictable, reliable, and high-throughput connections offered by ExpressRoute, 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, and serve all of your corporate customers without traffic ever routing through the public Internet.

For more information, [ExpressRoute⁴](#).

ExpressRoute Capabilities

ExpressRoute is supported across all Azure regions and locations. The following map provides a list of Azure regions and ExpressRoute locations. ExpressRoute locations refer to those where Microsoft peers with several service providers. You will have access to Azure services across all regions within a geopolitical region if you connected to at least one ExpressRoute location within the geopolitical region.



ExpressRoute benefits

Layer 3 connectivity

Microsoft uses BGP, an industry standard dynamic routing protocol, to exchange routes between your on-premises network, your instances in Azure, and Microsoft public addresses. We establish multiple BGP sessions with your network 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. The graphic on the previous topics shows the primary and secondary connection.

Connectivity to Microsoft cloud services

ExpressRoute connections enable access to the following services: Microsoft Azure services, Microsoft Office 365 services, and Microsoft Dynamics 365. Office 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

⁴ <https://azure.microsoft.com/en-us/services/expressroute/>

You can 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 can 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 (national clouds are excluded).

Across on-premises connectivity with ExpressRoute Global Reach

You can 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 can purchase ExpressRoute circuits for a wide range of bandwidths from 50 Mbps to 10 Gbps. Be sure to check with your connectivity provider to determine the bandwidths they support.

Flexible billing models

You can pick a billing model that works best for you. Choose between the billing models listed below.

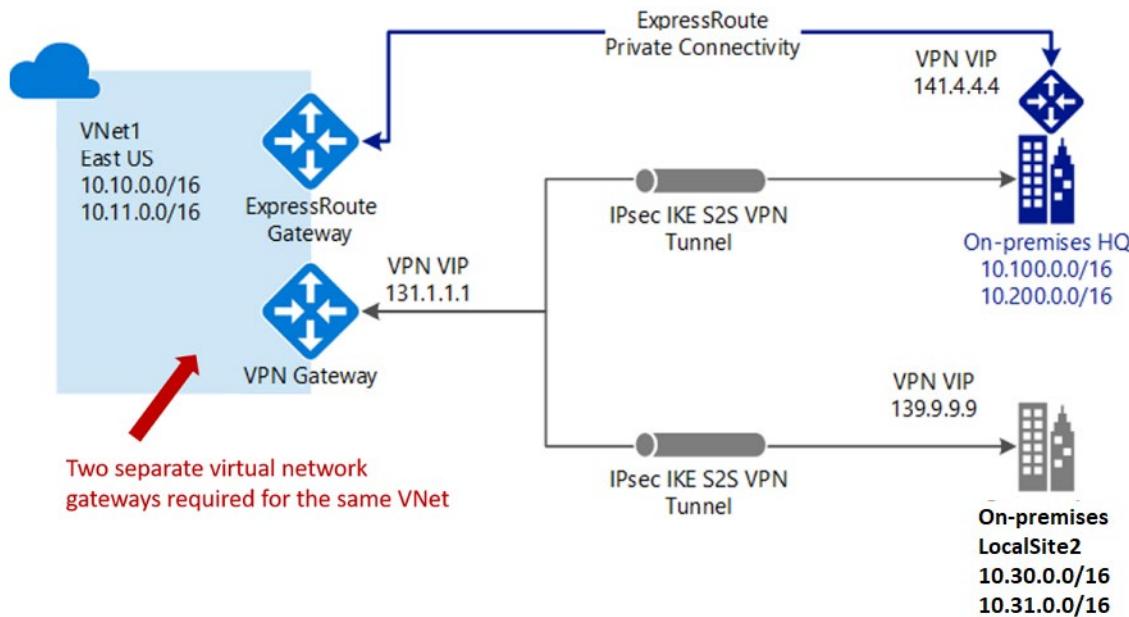
- **Unlimited data.** Billing is based on a monthly fee; all inbound and outbound data transfer is included free of charge.
- **Metered data.** Billing is based on a monthly fee; all inbound data transfer is free of charge. Outbound data transfer is charged per GB of data transfer. Data transfer rates vary by region.
- **ExpressRoute premium add-on.** This add-on includes increased routing table limits, increased number of VNets, global connectivity, and connections to Office 365 and Dynamics 365. Read more in the FAQ link.

Coexisting 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 can configure a Site-to-Site VPN as a secure failover path for ExpressRoute or use Site-to-Site VPNs to connect to sites that are not part of your network, but that are connected through ExpressRoute. Notice that 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 can create a connection between your on-premises network and the Microsoft cloud in three different ways, Co-located at a cloud exchange, Point-to-point Ethernet Connection, and Any-to-any (IPVPN) Connection. Connectivity providers can offer one or more connectivity models. You can work with your connectivity provider to pick the model that works best for you.

Co-located at a cloud exchange

If you are co-located in a facility with a cloud exchange, you can order virtual cross-connections to the Microsoft cloud through the co-location provider's Ethernet exchange. Co-location providers can offer either Layer 2 cross-connections, or managed Layer 3 cross-connections between your infrastructure in the co-location facility and the Microsoft cloud.

Point-to-point Ethernet connections

You can connect your on-premises datacenters/offices to the Microsoft cloud through point-to-point Ethernet links. Point-to-point Ethernet providers can offer Layer 2 connections, or managed Layer 3 connections between your site and the Microsoft cloud.

Any-to-any (IPVPN) networks

You can 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.

- ✓ Currently, the deployment options for S2S and ExpressRoute coexisting connections are only possible through PowerShell, and not the Azure portal.

Intersite Connections Comparison

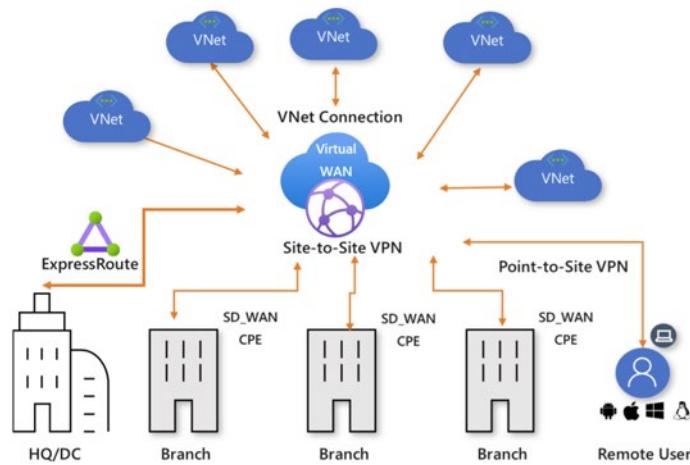
There are many intersite connection choices. This table summarizes how to make a selection.

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 Office 365 services	50 Mbps up to 100 Gbps	Active/active	Enterprise-class and mission-critical workloads. Big data solutions.

Virtual WANs

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 can leverage the Azure backbone to also 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. It enables global transit network architecture based on a classic hub-and-spoke connectivity model where 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
Basic	Basic	Site-to-site VPN only
Standard	Standard	ExpressRoute, User VPN (P2S), VPN (site-to-site), Inter-hub and VNet-to-VNet transiting through the virtual hub.

For more information, [About Azure Virtual WAN⁵](https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about).

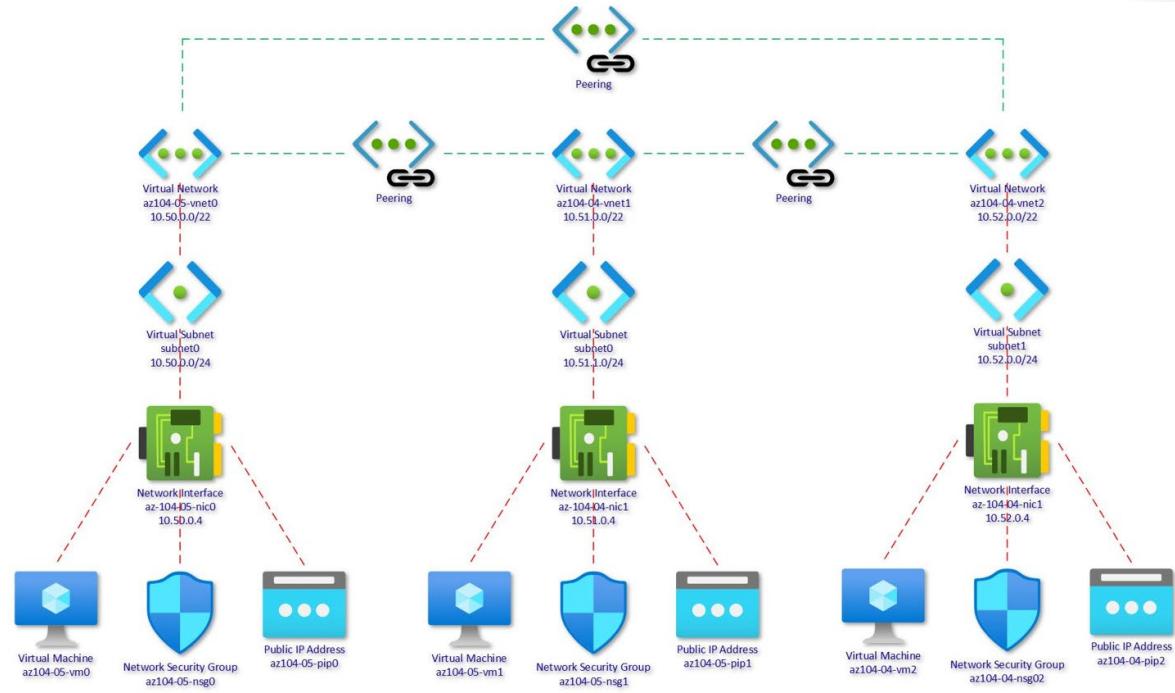
⁵ <https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

Module 05 Lab and Review

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

Module 05 Review Questions

Review Question 1

Which two statements regarding an Azure VPN gateway are true? Select two.

- You can only assign a dynamic public IP address to an Azure VPN Gateway.
- The gateway connects virtual machines within a VNet.
- The gateway connects an Azure VNet to an on-premises network.
- You can assign a static public IP address to an Azure VPN Gateway.

Review Question 2

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 are true benefits of VNet peering? Select two.

- The virtual networks can exist in any Azure cloud region.
- Network traffic between peered virtual networks is private.
- Peering is easy to configure and manage, requiring little to no downtime.
- Gateway transit can be configured regionally or globally.

Review Question 3

Your company is preparing to implement a Site-to-Site VPN to Microsoft Azure. You are selected to plan and implement the VPN. Currently, you have an Azure subscription, an Azure virtual network, and an Azure gateway subnet. You need to prepare the on-premises environment and Microsoft Azure to meet the prerequisites of the Site-to-Site VPN. Later, you will create the VPN connection and test it. What should you do? (Each answer presents part of the solution. Select three.

- 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.
- Create a virtual network gateway (ExpressRoute) in Azure.
- Obtain a public IPv4 IP address without NAT for the VPN device.
- Obtain a public IPv4 IP address behind NAT for the VPN device.

Review Question 4

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 establishes the following requirements for the connectivity:

- Connectivity must 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 Virtual Private Gateway (VGW).
- Implement a VNet-to-VNet VPN.
- Implement a Point-to-Site VPN.

Review Question 5

You are configuring VNet Peering across two Azure virtual networks, VNET1 and VNET2. You are configuring the VPN Gateways. You want VNET2 to be able to use 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.
- Do not select allow gateway transit or use remote gateways on either VNET1 or VNET2.

Review Question 6

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. You have checked to ensure the device is on the validated list of VPN devices. Before you proceed to configure the device what two pieces of information should you ensure you have? Select two.

- The shared access signature key from the recovery services vault.
- The shared key you provided when you created your site-to-site VPN connection.
- The gateway routing method provided when you created your site-to-site VPN connection.
- The static IP address of your virtual network gateway.
- The public IP address of your virtual network gateway.
- The user and password for the virtual network gateway.

Review Question 7

You manage a large datacenter that is running out of space. You propose extending the datacenter to Azure using a Multi-Protocol Label Switching virtual private network. Which connectivity option would you select? Select one.

- Point-to-Site
- VPN Peering
- Multi-site
- Site-to-Site
- ExpressRoute
- VNet-to-VNet

Review Question 8

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 specify a DNS server.
- Ensuring you select an appropriate Gateway SKU.

Review Question 9

Your manager asks you to verify some information about Azure Virtual WANs. Which of the following statements are true? Select three.

- You must use one of the approved connectivity partner providers.
- You must use a VPN device that provides IKEv2/IKEv1 IPsec support.
- Virtual WAN supports ExpressRoute.
- Virtual WAN supports site-to-site connections.
- Virtual WAN does not support point-to-site connections.
- You can switch between the Basic and Standard plans at any time.

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Distribute your services across Azure virtual networks and integrate them by using virtual network peering⁶**

⁶ <https://docs.microsoft.com/en-us/learn/modules/integrate-vnets-with-vnet-peering/>

- Connect your on-premises network to Azure with **VPN Gateway**⁷
- Connect your on-premises network to the Microsoft global network by using **ExpressRoute**⁸

MCT USE ONLY. STUDENT USE PROHIBITED

⁷ <https://docs.microsoft.com/en-us/learn/modules/connect-on-premises-network-with-vpn-gateway/>

⁸ <https://docs.microsoft.com/en-us/learn/modules/connect-on-premises-network-with-expressroute/>

Answers

Review Question 1

Which two statements regarding an Azure VPN gateway are true? Select two.

- You can only assign a dynamic public IP address to an Azure VPN Gateway.
- The gateway connects virtual machines within a VNet.
- The gateway connects an Azure VNet to an on-premises network.
- You can assign a static public IP address to an Azure VPN Gateway.

Explanation

Azure VPN Gateway is used to connect an Azure virtual network (VNet) to other Azure VNets, or to an on-premises network. You need to assign a public IP address to its IP configuration to enable it to communicate with the remote network. Currently, you can only assign a dynamic public IP address to a VPN gateway.

Review Question 2

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 are true benefits of VNet peering? Select two.

- The virtual networks can exist in any Azure cloud region.
- Network traffic between peered virtual networks is private.
- Peering is easy to configure and manage, requiring little to no downtime.
- Gateway transit can be configured regionally or globally.

Explanation

Peering is efficient as there is no downtime to resources in either virtual network when creating the peering, or after the peering is created. Also, for security, Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network. While virtual networks can exist in any Azure public cloud region, they cannot exist in Azure national clouds. National clouds have very specific customer requirements to their use and operation. These services are confined within the geographic borders of specific countries and operated by local personnel. Gateway transit only applies to regional VNet peering and not to global VNet peering.

Review Question 3

Your company is preparing to implement a Site-to-Site VPN to Microsoft Azure. You are selected to plan and implement the VPN. Currently, you have an Azure subscription, an Azure virtual network, and an Azure gateway subnet. You need to prepare the on-premises environment and Microsoft Azure to meet the prerequisites of the Site-to-Site VPN. Later, you will create the VPN connection and test it. What should you do? (Each answer presents part of the solution. Select three.)

- 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.
- Create a virtual network gateway (ExpressRoute) in Azure.
- Obtain a public IPv4 IP address without NAT for the VPN device.
- Obtain a public IPv4 IP address behind NAT for the VPN device.

Explanation

The prerequisites for a Site-to-Site VPN are having a compatible VPN device on-premises, having a public IPv4 IP without NAT on the on-premises VPN device, and creating a VPN gateway and local network gateway in Azure. IPv6 is not supported for VPNs. ExpressRoute is a different setup and not part of a Site-to-Site VPN.

Review Question 4

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 establishes the following requirements for the connectivity:

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 Virtual Private Gateway (VGW).
- Implement a VNet-to-VNet VPN.
- Implement a Point-to-Site VPN.

Explanation

In this scenario, only one of the answers provides persistent connectivity to Azure - the Site-to-Site VPN. A VNet-to-VNet connects two Azure virtual networks together. A Point-to-Site VPN is used for individual connections (such as for a developer). A VPC and VGW are relevant to Amazon AWS.

Review Question 5

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.
- Do not select allow gateway transit or use remote gateways on either VNET1 or 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.

Review Question 6

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. You have checked to ensure the device is on the validated list of VPN devices. Before you proceed to configure the device what two pieces of information should you ensure you have? Select two.

- The shared access signature key from the recovery services vault.
- The shared key you provided when you created your site-to-site VPN connection.
- The gateway routing method provided when you created your site-to-site VPN connection.
- The static IP address of your virtual network gateway.
- The public IP address of your virtual network gateway.
- The user and password for the virtual network gateway.

Explanation

You will need two things: shared key and the public IP address of your virtual network gateway. The shared key was provided when you created the site-to-site VPN connection.

Review Question 7

You manage a large datacenter that is running out of space. You propose extending the datacenter to Azure using a Multi-Protocol Label Switching virtual private network. Which connectivity option would you select? Select one.

- Point-to-Site
- VPN Peering
- Multi-site
- Site-to-Site
- ExpressRoute
- VNet-to-VNet

Explanation

ExpressRoute is the best choice for extending the datacenter, as it can use an any-to-any (IPVPN) connectivity model. An MPLS VPN, as typically provided by an IPVPN network, enables connectivity between the Microsoft cloud and your branch offices and datacenters.

Review Question 8

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 specify a DNS server.
- Ensuring you select an appropriate Gateway SKU.

Explanation

The Gateway SKU selection directly affects performance. Gateway SKUs control the number of tunnels and connections that are available. This affects the overall aggregate throughput of the connection.

Review Question 9

Your manager asks you to verify some information about Azure Virtual WANs. Which of the following statements are true? Select three.

- You must use one of the approved connectivity partner providers.
- You must use a VPN device that provides IKEv2/IKEv1 IPsec support.
- Virtual WAN supports ExpressRoute.
- Virtual WAN supports site-to-site connections.
- Virtual WAN does not support point-to-site connections.
- You can switch between the Basic and Standard plans at any time.

Explanation

Virtual WAN supports ExpressRoute and any VPN device that is IKEv2/IKEv1 IPSec compliant.

Module 6 Network Traffic Management

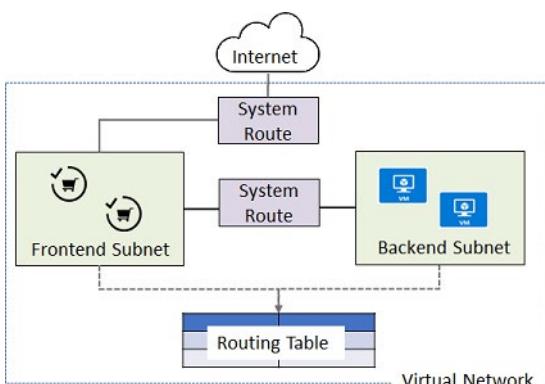
Network Routing and Endpoints

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.

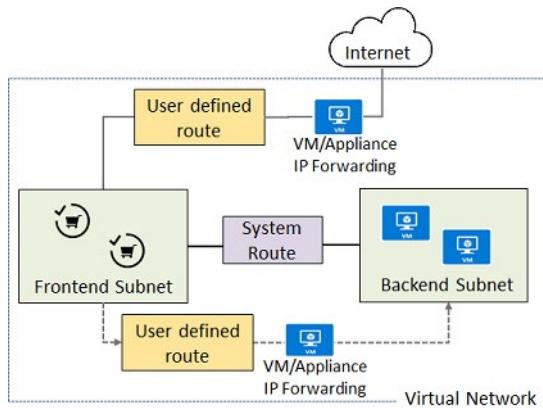


- ✓ Information about the system routes is recorded in a route table. A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network. Route tables are associated to subnets, and each packet leaving a subnet is handled based on the associated route 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.

User Defined Routes

As explained in the previous topic, 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. This 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 additional charges for creating route tables in Microsoft Azure. Do you think you will need to create custom routes?

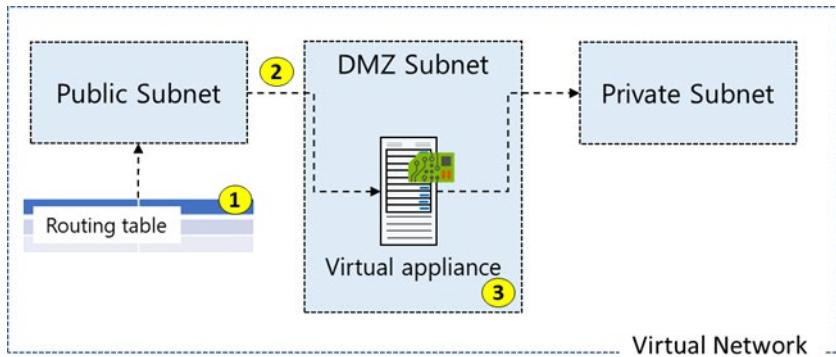
For more information, [Custom routes¹](#).

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.

¹ <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#custom-routes>



1. Create a routing table.
 2. Add a custom route that requires all private subnet traffic be directed to a network appliance.
 3. Associate the new route to the public subnet.
- ✓ 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.

Create a Routing Table

Creating a routing table is very straightforward. You must provide **Name**, **Subscription**, **Resource Group**, **Location**, and whether you want to use **Virtual network gateway route propagation**.

Create route table □ X

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
 Disabled Enabled

Create [Automation options](#)

A standard routing protocol is used to exchange routing and reachability information between two or more networks. Routes are automatically added to the route table for all subnets with Virtual network gateway propagation enabled. In most situations this is what you want. For example, if you are using ExpressRoute you would want all subnets to have that routing information.

For more information, [Overview of BGP with Azure VPN Gateways²](#).

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 * ✓

Address prefix * ⓘ ✓

Next hop type ⓘ

^

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.

² <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview?toc=%2fazure%2fvirtual-network%2ftoc.json>

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

- ✓ In this example remember that the virtual appliance should not have a public IP address and IP forwarding should be enabled on the device.

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. On the upper-left side of the screen, select **Services**, and then navigate to **Route tables**.
3. Select **+ Add**.
 - **Name:** *myRouteTablePublic*
 - **Subscription:** *select your subscription*
 - **Resource group:** *create or select a resource group*
 - **Location:** *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 note: 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

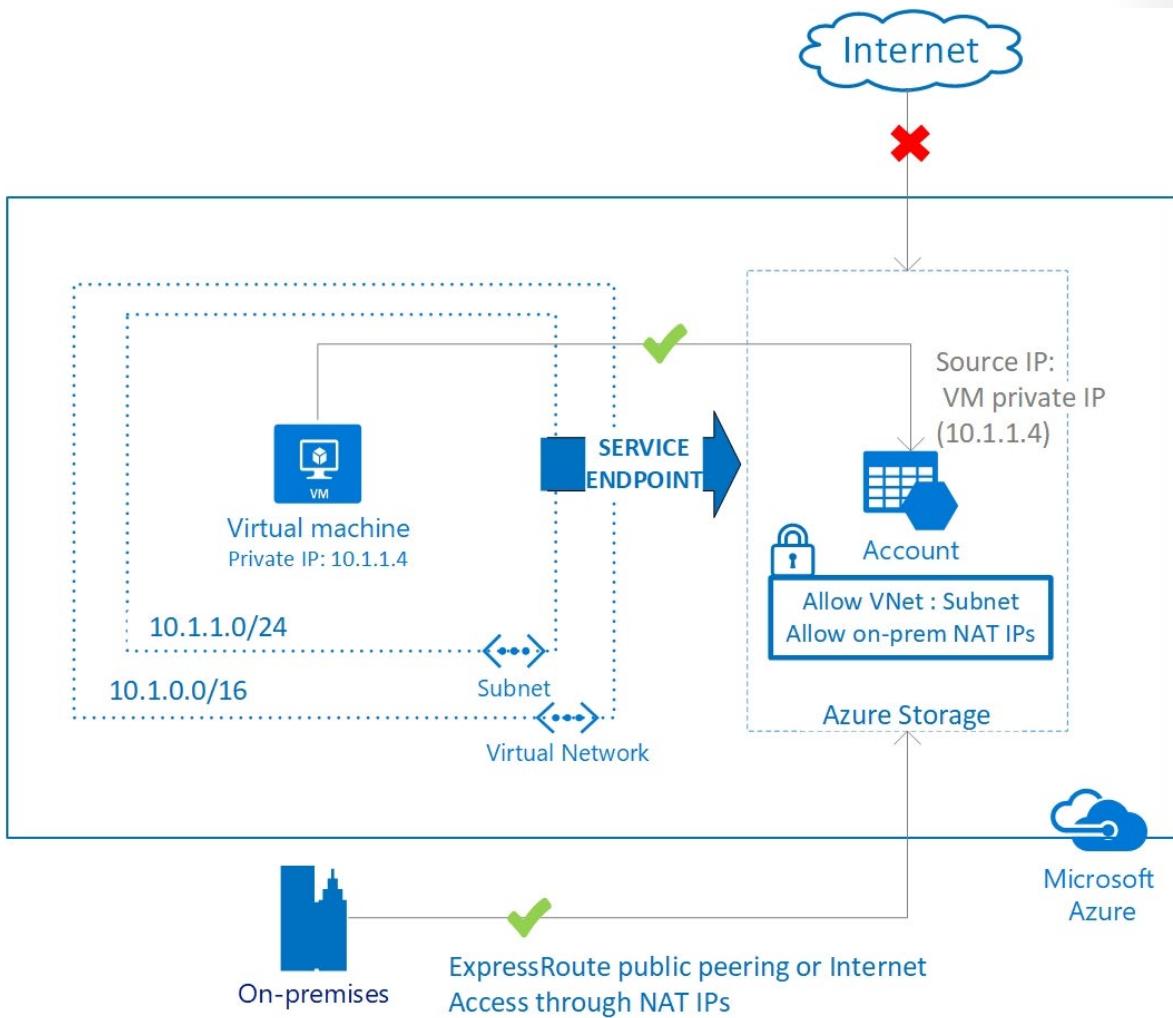
1. Open the Cloud Shell.
2. View information about your new routing table.
Get-AzRouteTable

3. Verify the **Routes** and **Subnet** information is correct.

Service Endpoints

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.



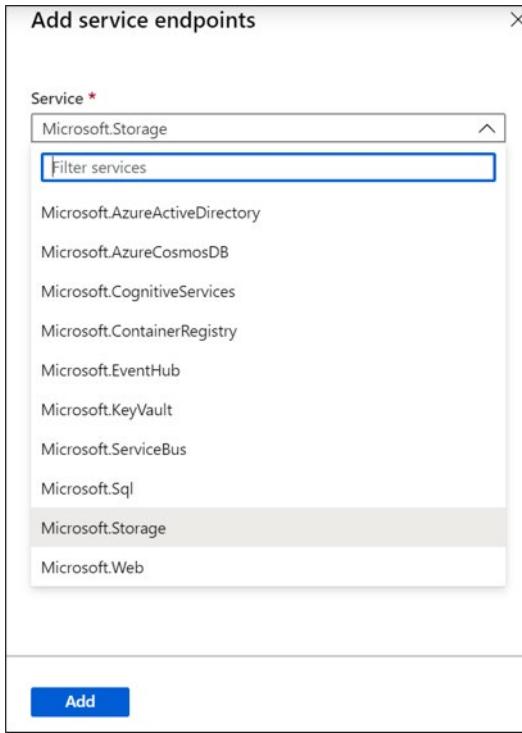
Why use a service endpoint?

- **Improved security for your Azure service resources.** VNet private address space can be overlapping and so, cannot be used to uniquely identify traffic originating from your VNet. Service endpoints provide the ability to secure Azure service resources to your virtual network, by extending VNet identity to the 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. This provides improved 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 a simple click on a subnet. There is no additional overhead to maintaining the endpoints.
- ✓ With service endpoints, the source IP addresses of the virtual machines in the subnet for service traffic switches from using public IPv4 addresses to using private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch. Please 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.

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

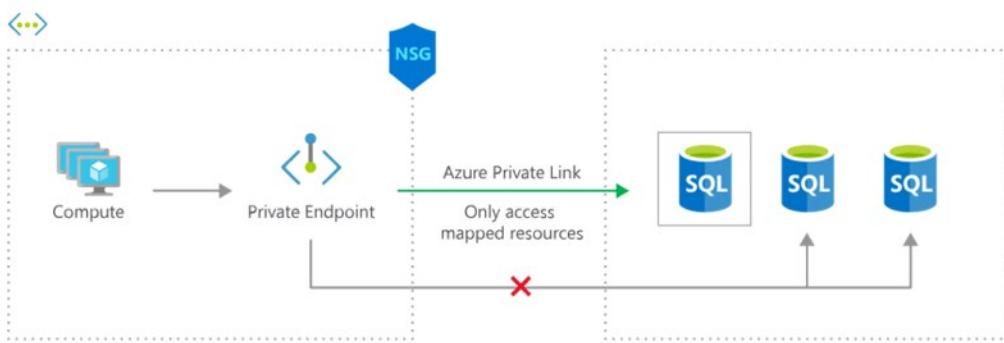
Azure Cosmos DB with the identity of the subnet and Virtual Network. Once the Azure Cosmos DB service endpoint is enabled, you can limit access to the subnet by adding it to your Azure Cosmos account.

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.

- ✓ Adding service endpoints can take up to 15 minutes to complete. Each service endpoint integration has its own Azure documentation page.

Private Link



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. In the event of 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.

For more information, **Private Link Documentation³**.

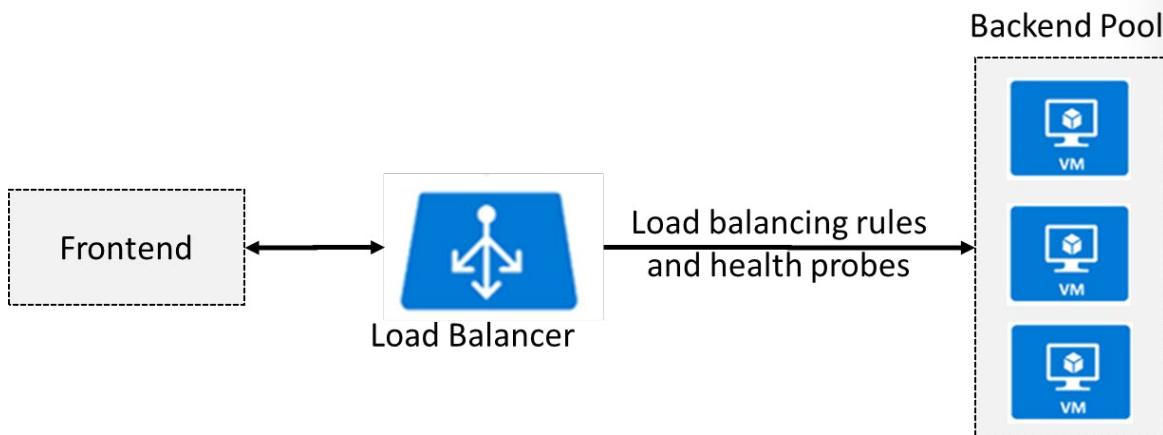
³ <https://docs.microsoft.com/en-us/azure/private-link/>

Azure Load Balancer

Azure Load Balancer

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 as well as outbound scenarios and scales up to millions of TCP and UDP application flows.

- ✓ 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**.

For more information, [Load Balancer documentation⁴](#).

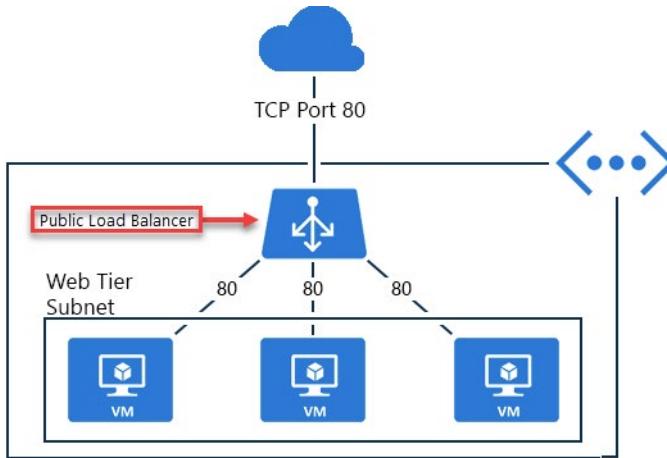
Public Load Balancer

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, and vice versa 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.

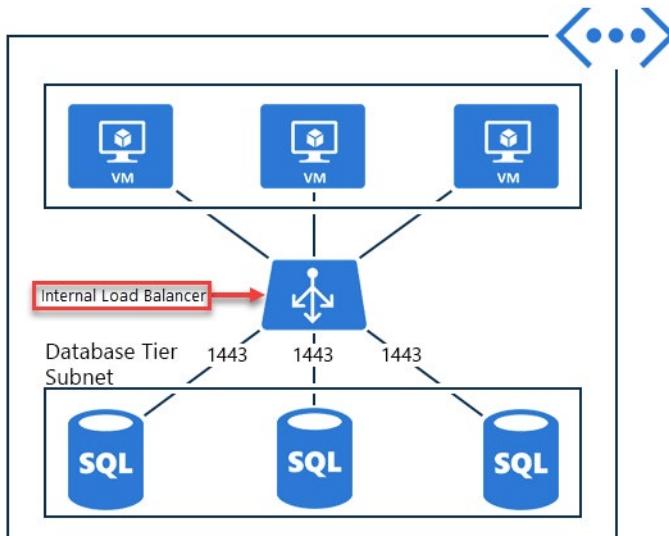
The following figure shows internet clients sending webpage requests to the public IP address of a web app on TCP port 80. Azure Load Balancer distributes the requests across the three VMs in the load-balanced set.

⁴ <https://docs.microsoft.com/en-us/azure/load-balancer/>



Internal Load Balancer

An internal load balancer directs traffic only 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.
- ✓ A public load balancer could be placed in front of the internal load balancer to create a multi-tier application.

Load Balancer SKUs

When you create an Azure Load Balancer you will select for the type (Internal or Public) of load balancer. You will 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

Considerations

- SKUs are not mutable. You may not change the SKU of an existing resource.
- A standalone virtual machine resource, availability set resource, or virtual machine scale set resource can reference one SKU, never both.
- A Load Balancer rule cannot span two virtual networks. Frontends and their related backend instances must be in the same virtual network.
- There is no charge for the Basic load balancer. The Standard load balancer is charged based on number of rules and data processed.
- Load Balancer frontends are not accessible across global virtual network peering.
- ✓ New designs and architectures should consider using Standard Load Balancer.

MCT USE ONLY. STUDENT USE PROHIBITED

Backend Pools

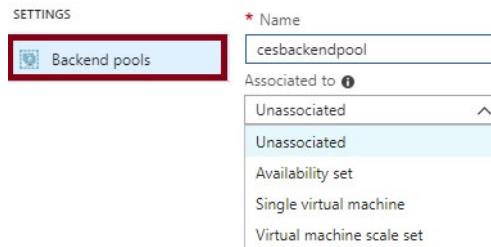
To distribute traffic, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer.



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 VM 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.



- ✓ In the Standard SKU you can have up to 1000 instances in the backend pool. In the Basic SKU you can have up to 100 instances.

Load Balancer Rules

A load balancer rule is used to define how traffic is distributed to the backend pool. The rule maps a given frontend IP and port combination to a set of backend IP addresses and port combination. To create the rule the frontend, backend, and health probe information should already be configured. Here is a rule that passes frontend TCP connections to a set of backend web (port 80) servers. The rule uses a health probe that checks on HTTP port 80.

Add load balancing rule

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

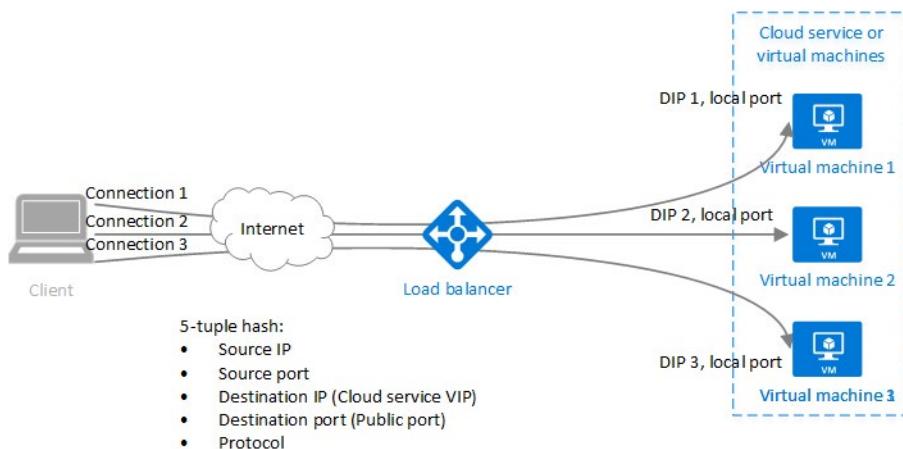
Idle timeout (minutes) 4

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. Notice in this case, the NAT rule is explicitly attached to a VM (or network interface) to complete the path to the target; whereas a Load Balancing rule need not be.

Session Persistence

By default, Azure Load Balancer distributes network traffic equally among multiple VM instances. The load balancer uses a 5-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.

- **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.
- ✓ Keeping session persistence information is very important in applications that use a shopping cart. Can you think of any other applications?

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**.

Add health probe	
lb01	
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 this 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).

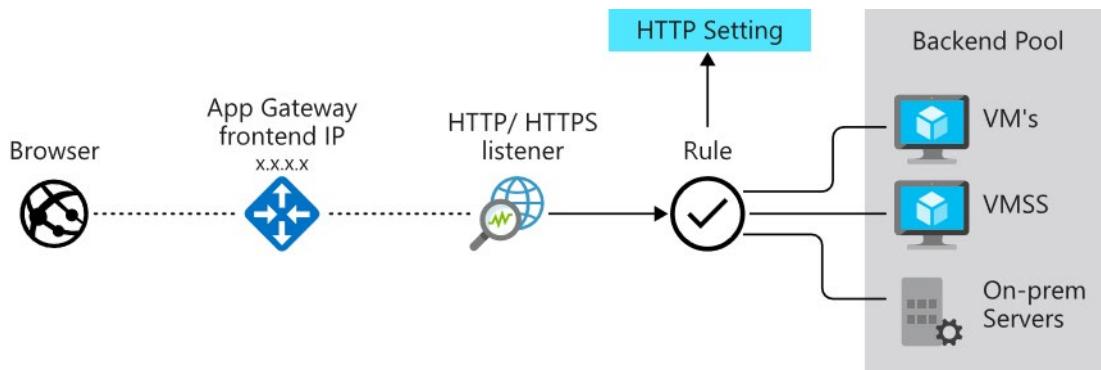
TCP custom probe. This probe relies on establishing a successful TCP session to a defined probe port. If the specified listener on the VM exists, the probe succeeds. If the connection is refused, the probe fails. You can specify the Port, Interval, and Unhealthy threshold.

- ✓ 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.

Azure Application Gateway

Application Gateway

Application Gateway manages the requests that client applications can send to a web app. Application Gateway routes traffic to a pool of web servers based on the URL of a request. This is known as application layer routing. The pool of web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers.



The Application Gateway will automatically load balance requests sent to the servers in each back-end pool using a round-robin mechanism. However, you can configure session stickiness, if you need to ensure that all requests for a client in the same session are routed to the same server in a back-end pool.

Load-balancing works with the OSI Layer 7 routing implemented by Application Gateway routing, which means that it load balances requests based on the routing parameters (host names and paths) used by the Application Gateway rules. In comparison, other load balancers, such as Azure Load Balancer, function at the OSI Layer 4 level, and distribute traffic based on the IP address of the target of a request.

Operating at OSI Layer 7 enables load balancing to take advantage of the other features that Application Gateway provides.

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.

For more information, [What is Azure Application Gateway⁵](#).

Application Gateway Routing

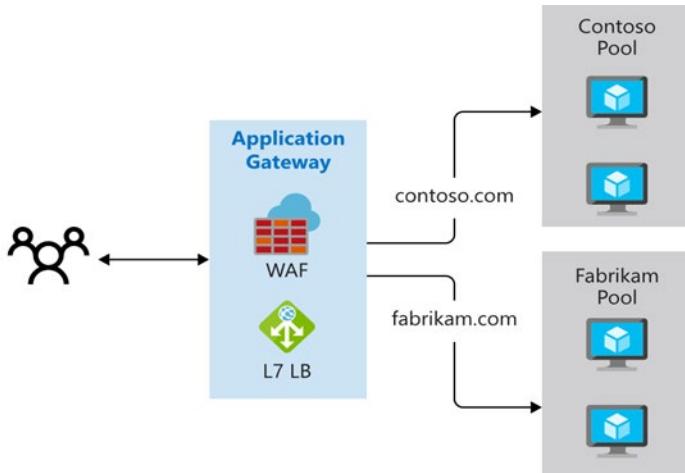
Clients send requests to your web apps to the IP address or DNS name of the gateway. The gateway routes requests to a selected web server in the back-end pool, using a set of rules configured for the gateway to determine where the request should go.

There are two primary methods of routing traffic, path-based routing and multiple site hosting.

⁵ <https://docs.microsoft.com/en-us/azure/application-gateway/overview>

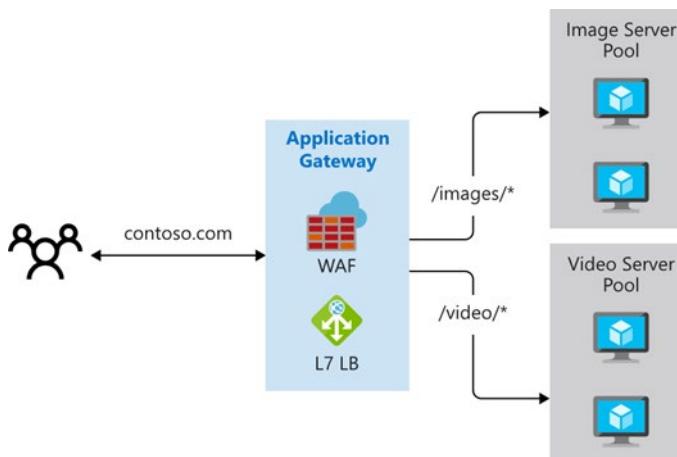
Path-based routing

Path-based routing enables you to send requests with different paths in the URL to a different pool 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 hosting enables you to configure 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 configure Application Gateway to 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.



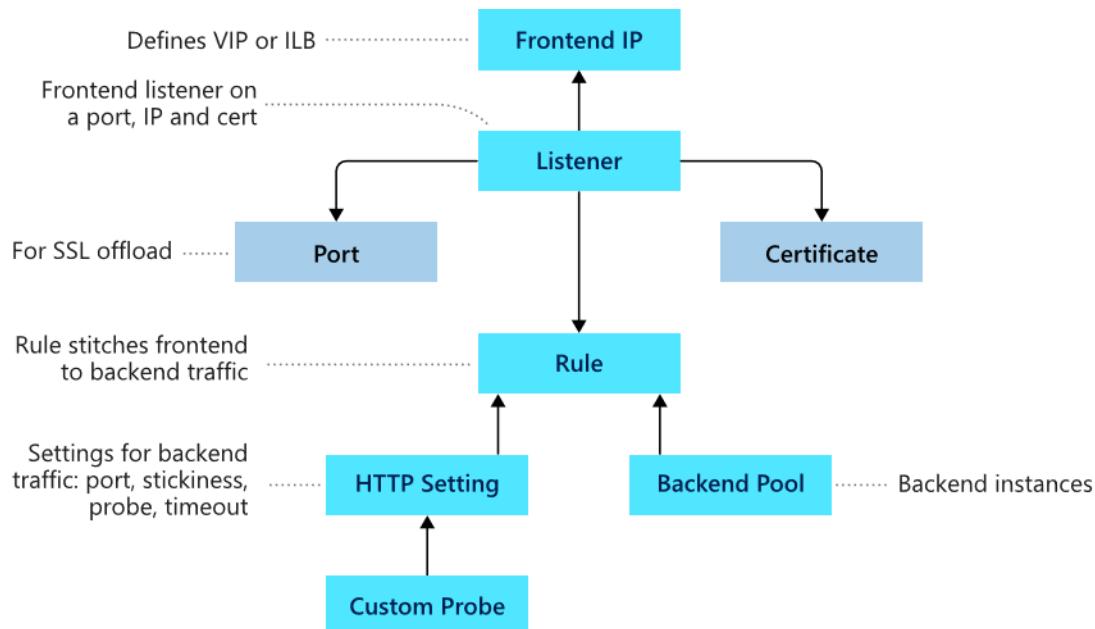
Multi-site configurations are useful for supporting multi-tenant applications, where each tenant has its own set of virtual machines or other resources hosting a web application.

Additional 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 additional 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.

Application Gateway Configuration

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 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 direct the request to the appropriate back-end pool. A routing rule also has an associated set of HTTP settings. These settings indicate whether (and how) traffic is encrypted between Application Gateway and the back-end servers, and other configuration information such as: 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). These 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

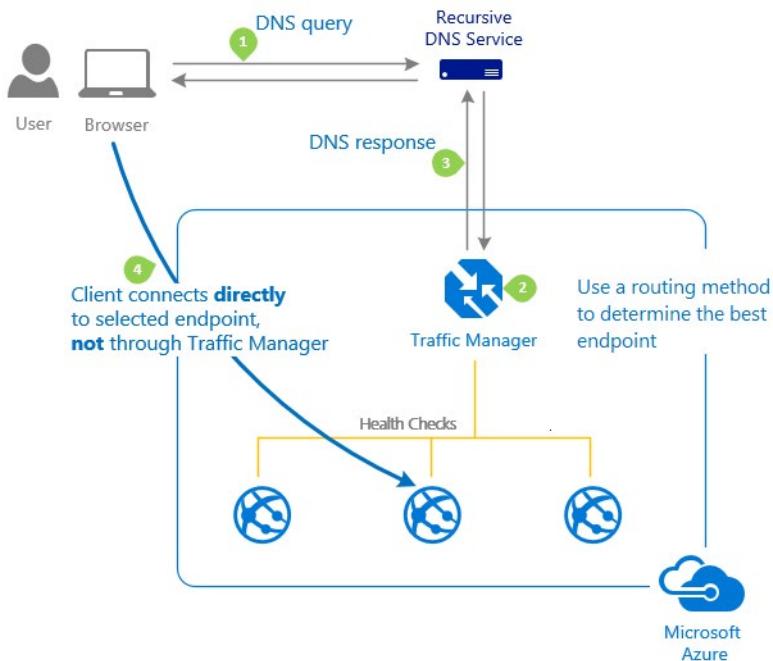
Health probes are an important part in assisting the load balancer to determine which servers are available for load balancing in a back-end pool. Application Gateway uses a health probe to send a request to a server. If the server returns an HTTP response with a status code between 200 and 399, the server is deemed 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.

Azure Traffic Manager

Azure Traffic Manager

Microsoft Azure Traffic Manager allows you to control the distribution of user traffic to your service endpoints running in different datacenters around the world.



- Traffic Manager works by using the Domain Name System (DNS) to direct end-user requests to the most appropriate endpoint. Service endpoints supported by Traffic Manager include Azure VMs, Web Apps, and cloud services. You can also use Traffic Manager with external, non-Azure endpoints.
- Traffic Manager selects an endpoint based on the configured traffic-routing method. Traffic Manager supports a range of traffic-routing methods to suit different application needs. Once the endpoint is selected the clients then connect directly to the appropriate service endpoint.
- Traffic Manager provides endpoint health checks and automatic endpoint failover, enabling you to build high-availability applications that are resilient to failure, including the failure of an entire Azure region.

Traffic Manager Benefits

Here are some specific ways you can use Traffic Manager.

- **Improve availability of critical applications.** Traffic Manager allows you to deliver high availability for your critical applications by monitoring your endpoints in Azure and providing automatic failover when an endpoint goes down.
- **Improve responsiveness for high performance applications.** Azure allows you to run cloud services or websites in datacenters located around the world. Traffic Manager provides faster page loads and better end-user experience by serving users with the hosted service that is "closest" to them.
- **Upgrade and perform service maintenance without downtime.** You can seamlessly carry out upgrade and other planned maintenance operations on your applications without downtime for end

users by using Traffic Manager to direct traffic to alternative endpoints when maintenance is in progress.

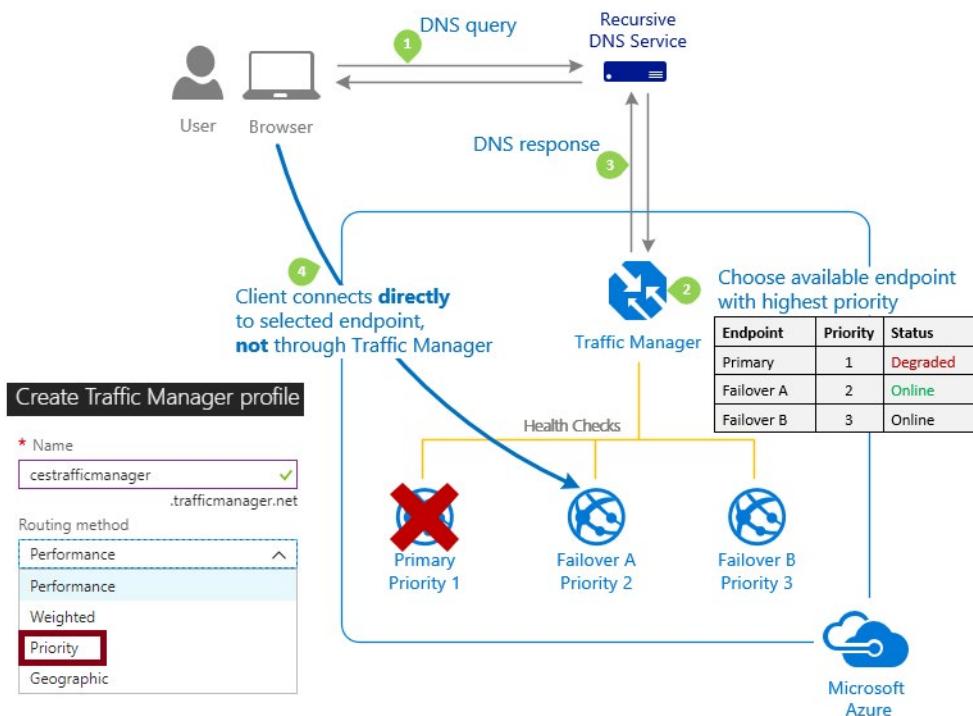
- **Combine on-premises and Cloud-based applications.** Traffic Manager supports external, non-Azure endpoints enabling it to be used with hybrid cloud and on-premises deployments.
- **Distribute traffic for large, complex deployments.** Traffic-routing methods can be combined using nested Traffic Manager profiles to create sophisticated and flexible traffic-routing configurations to meet the needs of larger, more complex deployments.

For more information, [Traffic Manager⁶](https://azure.microsoft.com/en-us/services/traffic-manager/)

Traffic Manager Routing Methods

Priority routing

When a Traffic Manager profile is configured for priority routing it contains a prioritized list of service endpoints. Traffic Manager sends all traffic to the primary (highest-priority) endpoint first. If the primary endpoint is not available, Traffic Manager routes the traffic to the second endpoint, and so on. Availability of the endpoint is based on the configured status (enabled or disabled) and the ongoing endpoint monitoring. The Priority traffic routing method allows you to easily implement a failover pattern. You configure the endpoint priority explicitly or use the default priority based on the endpoint order.

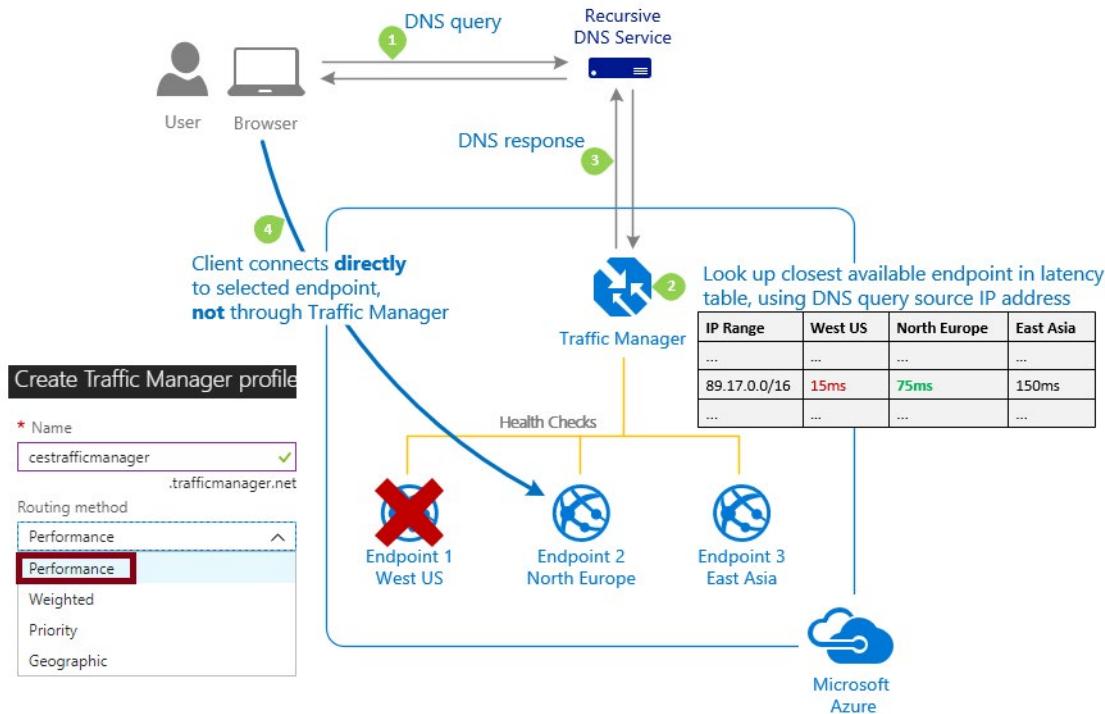


Performance routing

The Performance routing method is designed to improve the responsiveness by routing traffic to the location that is closest to the user. The closest endpoint is not necessarily measured by geographic

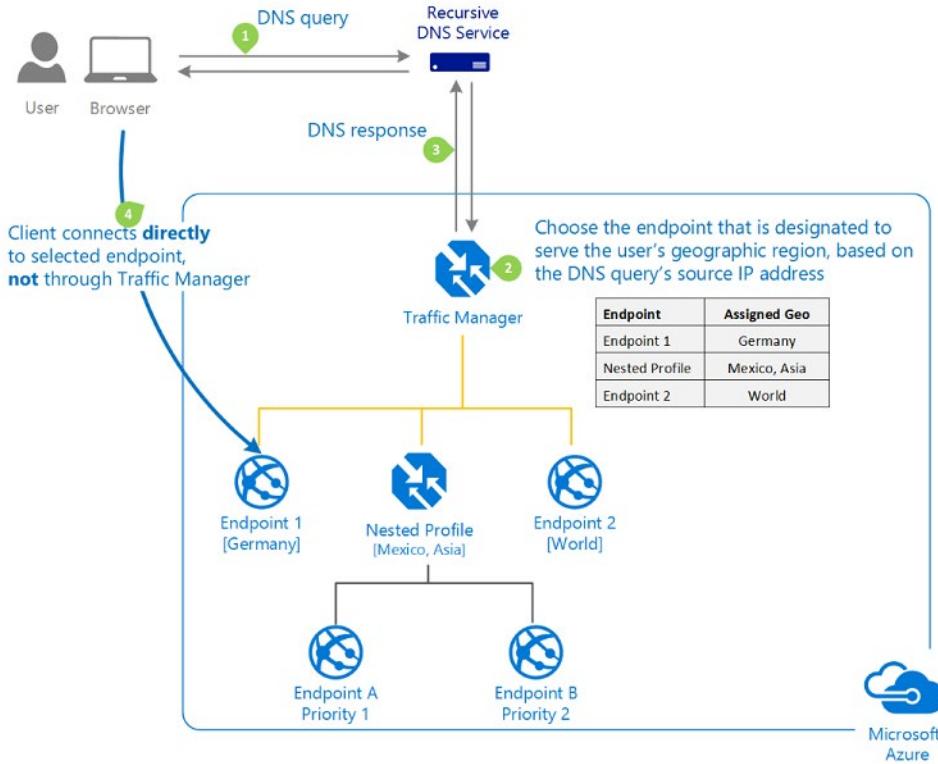
⁶ <https://azure.microsoft.com/en-us/services/traffic-manager/>

distance. Instead Traffic Manager determines closeness by measuring network latency. Traffic Manager maintains an Internet Latency Table to track the round-trip time between IP address ranges and each Azure datacenter. With this method Traffic Manager looks up the source IP address of the incoming DNS request in the Internet Latency Table. Traffic Manager chooses an available endpoint in the Azure datacenter that has the lowest latency for that IP address range, then returns that endpoint in the DNS response.



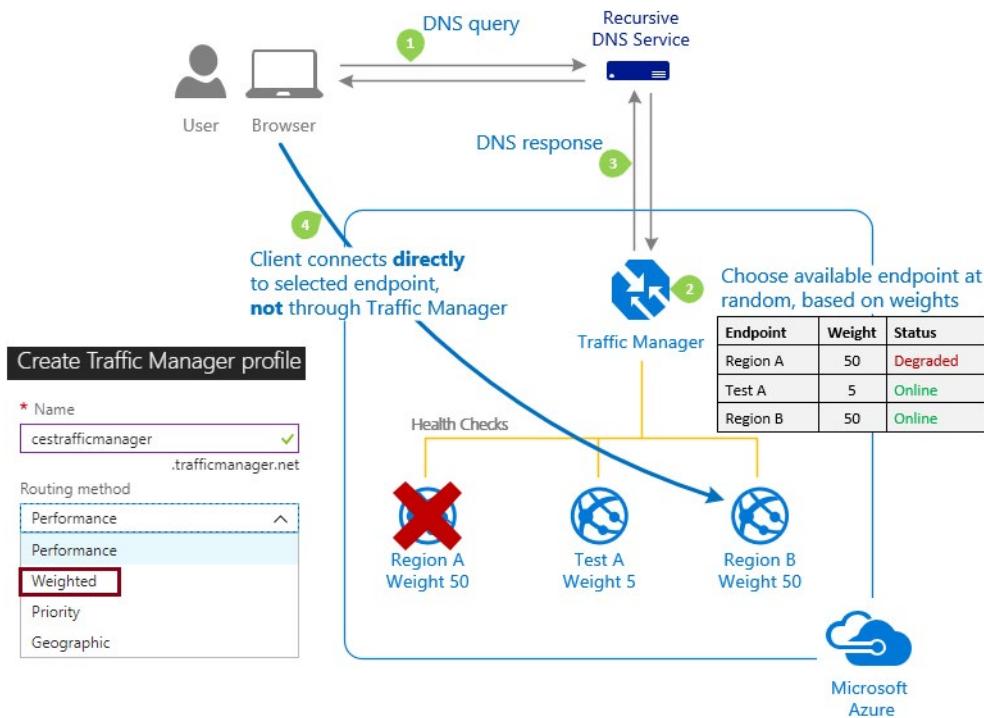
Geographic routing

When a Traffic Manager profile is configured for Geographic routing, each endpoint associated with that profile needs will have a set of geographic locations assigned to it. Any requests from those regions gets routed only to that endpoint. Some planning is required when you create a geographical endpoint. A location cannot be in more than one endpoint. You build the endpoint from a:



Weighted routing

The Weighted traffic-routing method allows you to distribute traffic evenly or to use a pre-defined weighting. In the Weighted traffic-routing method, you assign a weight to each endpoint in the Traffic Manager profile configuration. The weight is an integer from 1 to 1000. This parameter is optional. If omitted, Traffic Manager uses a default weight of '1'. The higher weight, the higher the priority.



- ✓ Additionally, MultiValue routing distributes traffic only to IPv4 and IPv6 endpoints and Subnet routing distributes traffic based on source IP ranges.

Distributing Network Traffic

This table compares the Azure Load Balancer with Traffic Manager. The technologies can be used in isolation or in combination.

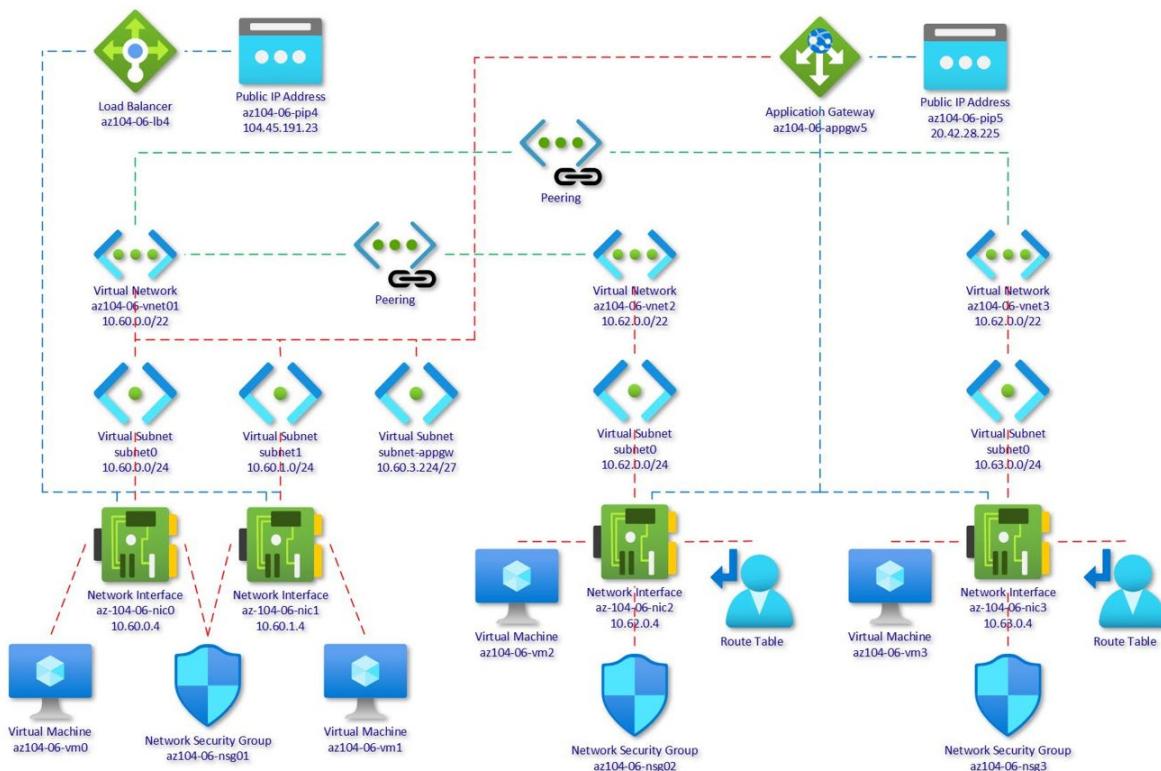
Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport Layer (level 4)	Transport Layer (level 7)	DNS Resolver
Protocols	Any TCP or UDP Protocol	HTTP, HTTPS, HTTP/2, & WebSockets	DNS Resolution
Backends and Endpoints	Azure VMs, and Azure VM Scale Sets	Azure VMs, Azure VM Scale Sets, Azure App Services, IP Addresses, and Hostnames	Azure Cloud Services, Azure App Services, Azure App Service Slots, and Public IP Addresses
Network connectivity	External and Internal	External and Internal	External

Module 06 Lab and Review

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

Module 06 Review Questions

Review Question 1

Which of the following two features of Azure networking provide the ability to redirect all Internet traffic back to your company's on-premises servers for packet inspection? Select two.

- User Defined Routes
- Cross-premises network connectivity
- Traffic Manager
- Forced Tunneling
- System Routes

Review Question 2

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 a private load balancer.
- Install a public load balancer.
- Install an external load balancer.
- Install an internal load balancer.
- Install a network load balancer.

Review Question 3

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
- Azure Cloud Services

MCT USE ONLY. STUDENT USE PROHIBITED

Review Question 4

You deploy an internal load balancer between your web tier and app tier servers. You configure a custom HTTP health probe. Which two of the following are not true? Select two.

- The load balancer manages the health probe.
- By default, the health probe checks the endpoint every 30 seconds.
- The instance is healthy if it responds with an HTTP 200 error.
- You can change the amount of time between health probe checks.
- You can change the number of failures within a time period.

Review Question 5

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 IP address of the web server that is the target of the request.
- The region in which the servers hosting the web application are located.
- The users authentication information.

Review Question 6

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.
- Uses one server in the backend pool until that server reaches 50% load, then moves to the next server.

Review Question 7

You have several websites and are using Traffic Manager to distribute the network traffic. You are bringing a new endpoint online but are not sure that it is ready to accept a full load of requests. Which Traffic Manager routing algorithm should you use? Select one.

- Round robin
- Priority
- Geographic
- Weighted
- Performance

Review Question 8

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.

- Configure Traffic Manager.
- Add a user-defined route.
- Create a local network gateway.
- Configure a new routing table.
- Add an application gateway.

Review Question 9

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 external load balancer
- Install an internal load balancer
- Install Azure Firewall
- Install the Web Application Firewall

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Manage and control traffic flow in your Azure deployment with routes⁷**
- **Improve application scalability and resiliency by using Azure Load Balancer⁸**
- **Load balance your web service traffic with Application Gateway⁹**
- **Enhance your service availability and data locality by using Azure Traffic Manager¹⁰**

⁷ <https://docs.microsoft.com/en-us/learn/modules/control-network-traffic-flow-with-routes/>

⁸ <https://docs.microsoft.com/en-us/learn/modules/improve-app-scalability-resiliency-with-load-balancer/>

⁹ <https://docs.microsoft.com/en-us/learn/modules/load-balance-web-traffic-with-application-gateway/>

¹⁰ <https://docs.microsoft.com/en-us/learn/modules/distribute-load-with-traffic-manager/>

Answers

Review Question 1

Which of the following two features of Azure networking provide the ability to redirect all Internet traffic back to your company's on-premises servers for packet inspection? Select two.

- User Defined Routes
- Cross-premises network connectivity
- Traffic Manager
- Forced Tunneling
- System Routes

Explanation

User defined routes and forced tunneling. You can use forced tunneling to redirect internet bound traffic back to the company's on-premises infrastructure. Forced tunneling is commonly used in scenarios where organizations want to implement packet inspection or corporate audits. Forced tunneling in Azure is configured via virtual network user defined routes (UDR).

Review Question 2

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 a private load balancer.
- Install a public load balancer.
- 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.

Review Question 3

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:

Which of the following would you select for this scenario? Select one.

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

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.

Review Question 4

You deploy an internal load balancer between your web tier and app tier servers. You configure a custom HTTP health probe. Which two of the following are not true? Select two.

- The load balancer manages the health probe.
- By default, the health probe checks the endpoint every 30 seconds.
- The instance is healthy if it responds with an HTTP 200 error.
- You can change the amount of time between health probe checks.
- You can change the number of failures within a time period.

Explanation

By default, the health probe checks the endpoints every 15 seconds, not 30 seconds. You can change the number of consecutive failures, but you cannot specify a time period for the failures.

Review Question 5

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 IP address of the web server that is the target 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.

Review Question 6

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.
- Uses one server in the backend pool until that server reaches 50% load, then moves to the next server.

Explanation

The Application Gateway distributes requests to each available server in the backend pool using the round-robin method.

Review Question 7

You have several websites and are using Traffic Manager to distribute the network traffic. You are bringing a new endpoint online but are not sure that it is ready to accept a full load of requests. Which Traffic Manager routing algorithm should you use? Select one.

- Round robin
- Priority
- Geographic
- Weighted
- Performance

Explanation

Use the weighted routing algorithm. This will put the endpoint into the rotation with a minimum amount of traffic.

Review Question 8

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.

- Configure Traffic Manager.
- Add a user-defined route.
- Create a local network gateway.
- Configure a new routing table.
- Add an application gateway.

Explanation

You should use Traffic Manager. Traffic Manager lets you control the distribution of user traffic to your endpoints running in different datacenters around the world. Traffic Manager uses DNS and can route traffic to your two new download servers.

Review Question 9

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 external load balancer
- 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 Azure Storage

Storage Accounts

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 in the event of transient hardware failures. You can also opt to replicate data across datacenters or geographical regions for additional protection from local catastrophe or natural disaster. Data replicated in this way remains highly available in the event of 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 a variety of languages – .NET, Java, Node.js, Python, PHP, Ruby, Go, and others – as well as a mature 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 can use Azure storage on its own—for example as a file share—but it is often used by developers as a store for working data. Such stores can be used by websites, mobile apps, desktop applications, and many other types of custom solutions. 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.** This 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.** This includes Blobs and Data Lake Store. Blobs are highly scaleable, REST based cloud object store. Data Lake Store is Hadoop Distributed File System (HDFS) as a service.
- **Structured Data.** This includes Tables, Cosmos DB, and Azure SQL DB. Tables are a key/value, auto-scaling 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. They are best for applications that require bulk storage or where data is accessed infrequently.
 - **Premium** storage accounts are backed by solid state drives (SSD) and offer consistent low-latency performance. They can only be used with Azure virtual machine disks and are best for I/O-intensive applications, like databases.
- ✓ It is not possible to convert a Standard storage account to 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.

For more information, [Azure Storage](#)¹.

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

¹ <https://azure.microsoft.com/en-us/services/storage/>

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 authentication 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 generally used to store lists of messages to be processed asynchronously.

For example, say 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 his 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 parts of this processing 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. To learn more and try out the new premium experience, please check out Azure Cosmos DB Table API.

Storage Account Kinds

Azure Storage offers several types of storage accounts. Each type supports different features and has its own pricing model. Consider these differences before you create a storage account to determine the type of account that is best for your applications. The types of storage accounts are:

Storage account type	Supported services	Supported performance tiers	Replication options
BlobStorage	Blob (block blobs and append blobs only)	Standard	LRS, GRS, RA-GRS
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
General-purpose V2	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS, ZRS, ZGRS (preview), RA-ZGRS (preview)
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS, ZRS (limited regions)
FileStorage	Files only	Premium	LRS, ZRS (limited regions)

General-purpose v1 accounts (Storage). Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.

General-purpose v2 accounts (StorageV2). Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.

Block blob storage accounts (BlockBlobStorage). Blob-only storage accounts with premium performance characteristics. Recommended for scenarios with high transaction rates, using smaller objects, or requiring consistently low storage latency.

FileStorage storage accounts (FileStorage). Files-only storage accounts with premium performance characteristics. Recommended for enterprise or high performance scale applications.

Blob storage accounts (BlobStorage). Blob-only storage accounts. Use general-purpose v2 accounts instead when possible.

- ✓ All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest.

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
Node unavailability within a data center	Yes	Yes	Yes	Yes

	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
An entire data center (zonal or non-zonal) becomes unavailable	No	Yes	Yes	Yes
A region-wide outage	No	No	Yes	Yes
Read access to your data (in a remote, geo-replicated region) in the event of region-wide unavailability	No	No	Yes (with RA-GRS)	Yes (with RA-GZRS)
Available in storage account types	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:

- If your application stores data that can be easily reconstructed if data loss occurs.
- If your data is constantly changing, for example a live feed, and storing the data is really not required.
- If 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 extremely 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 in the case of unavailability.

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**. If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which 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 in the case of 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) if your applications need to be able to read data in the event of a disaster in the primary region.

Microsoft recommends using GZRS for applications requiring consistency, durability, high availability, excellent performance, and resilience for disaster recovery. For the additional security of read access to the secondary region in the event of a regional disaster, enable RA-GZRS for your storage account.

Accessing 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.

- ✓ 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. If you have an application with an SLA, by using the domain you can avoid the downtime by using a second option, 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

- ✓ A Blob storage account only exposes the Blob service endpoint. And, you can also configure a custom domain name to use with your storage account.

Securing 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.

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group
vnet01	1	subnet01	10.1.0.0/24 ✓ Enabled	Demo

- Firewalls and Virtual Networks allows for restricting access to the Storage Account from specific Subnets on Virtual Networks
- Subnets and Virtual Networks must exist in the same Azure Region or Region Pair as the Storage Account
- ✓ It is important to test and ensure the service endpoint is limiting access as expected.

Demonstration - Securing 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

Create a storage account using PowerShell (optional)

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.

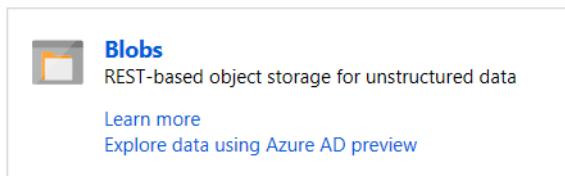
```
az group create --name storage-resource-group --location westus
az account list-locations --query "[].{Region:name}" --out table
az storage account create --name storagedemo --resource-group storage-resource-group --location
```

```
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.

Blob Storage

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:

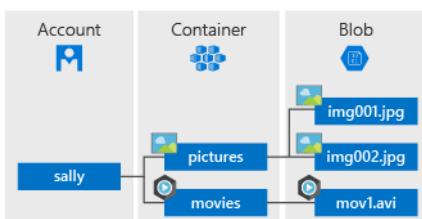
- Serving images or documents directly to a browser.
- Storing files for distributed access, such as installation.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

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.



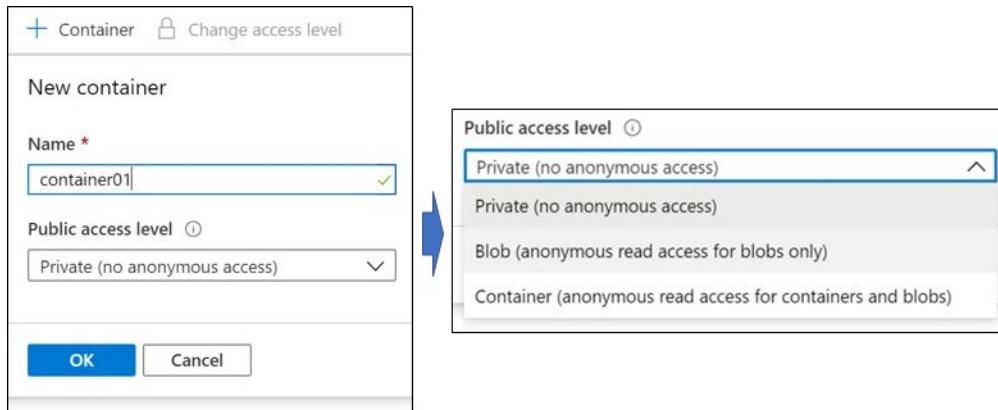
- ✓ Within the storage account, you can group as many blobs as needed in a container.

For more information, [Azure Blob Storage²](https://azure.microsoft.com/en-us/services/storage/blobs/).

² <https://azure.microsoft.com/en-us/services/storage/blobs/>

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.



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.
- ✓ You can also create the Blob container with PowerShell using the **New-AzStorageContainer** command.
- ✓ Have you thought about how you will organize your containers?

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 somewhat 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 somewhat 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.
- ✓ If there is a change in the usage pattern of your data, you can switch between these access tiers at any time.

Blob Lifecycle Management

Rule name *

Blobs

- Move blob to cool storage
 - Days after last modification: 30
- Move blob to archive storage
 - Days after last modification: 180
- Delete blob
 - Days after last modification: 365

Snapshots

- Delete snapshot
 - Days after blob is created: 30

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:

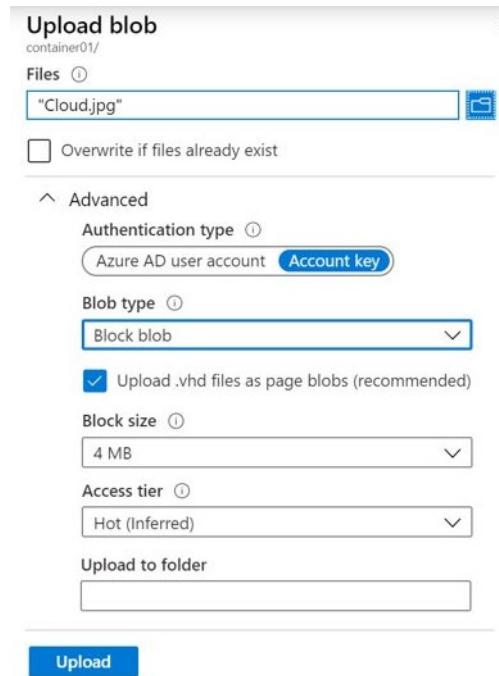
- Transition blobs to a cooler storage tier (hot to cool, hot to archive, or cool to archive) to optimize for performance and cost.
- Delete blobs at the end of their lifecycles.
- Define rules to be run once per day at the storage account level.
- Apply rules to containers or a subset of blobs (using prefixes as filters).

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.

Uploading 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.
- ✓ 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.
- ✓ Of course, you can always use Azure Storage Explorer.

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:** In addition to, the amount of data stored, the cost of storing data varies depending on the storage tier. The per-gigabyte cost decreases as the tier gets cooler.
- **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 that 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, 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** 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**.

Storage Security

Storage Security

Azure Storage provides a comprehensive set of security capabilities that together enable developers to build secure applications. In this lesson, we focus on Shared Access Signatures, but also cover storage encryption and some best practices. Here are the high-level security capabilities for Azure storage:

- **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.
 - 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.

Shared Access Signatures

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources (a specific blob in this case). You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature 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.

* Permissions [?](#)

Start and expiry date/time [?](#)

Start	Expiry
<input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="text" value="2019-02-27"/> 7:32:03 AM	<input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="text" value="2019-02-27"/> 3:32:03 PM
<input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="text" value="(UTC-08:00) --- Current Time Zone ---"/>	<input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="text" value="(UTC-08:00) --- Current Time Zone ---"/>

Allowed IP addresses [?](#)
for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols [?](#)

HTTPS HTTP

Signing key [?](#)

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.

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.
- ✓ 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.
- ✓ A stored access policy can provide an additional level of control over service-level SAS on the server side. You can group shared access signatures and provide additional restrictions for signatures that are bound by the policy.

For more information:

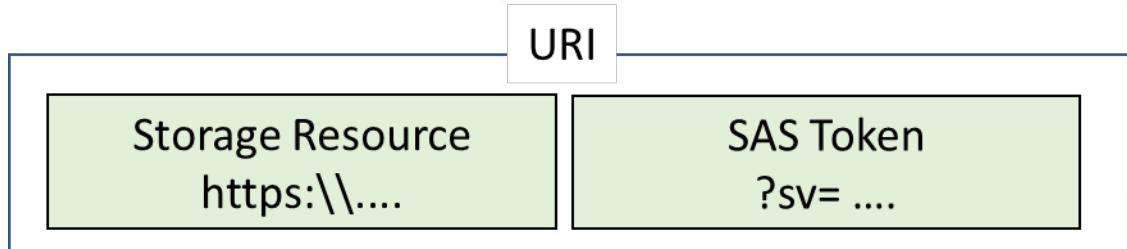
What is a shared access signature? - <https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1?toc=%2fazure%2fstorage%2fblobs%2ftoc.json#what-is-a-shared-access-signature>³

³ <https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

Define a stored access policy - <https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy>

URI and SAS Parameters

As you create your SAS a URI is created using parameters and tokens. The URI consists of your Storage Resource URI and the SAS token.



Here is an example URI. Each part is described in the table below.

```

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%6GRVAZ5Cdj2Pw4txxxxx
  
```

Name	SAS portion	Description
Resource 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%6GRVAZ5Cdj2Pw4txxxxx	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.

For more information, [Shared access signature parameters⁴](#).

Demonstration - SAS (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 that you learned about in the lesson.

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.

Storage Service Encryption

Azure **Storage Service Encryption** (SSE) for data at rest helps you protect your data to meet your organizational security and compliance commitments. With this feature, the Azure storage platform

⁴ <https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

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.

The handling of encryption, encryption at rest, decryption, and key management in Storage Service Encryption is 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

- ✓ 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.

Customer Managed keys

If you prefer, you can use the Azure Key Vault to manage your encryption keys. With the Key Vault 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.

Using custom keys give you more flexibility and control when creating, disabling, auditing, rotating, and defining access controls.

Encryption type

Microsoft Managed Keys
 Customer Managed Keys

Info 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](#)

- ✓ To use customer-managed keys with SSE, you can either create a new key vault and key or you can use an 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.

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 performing a man-in-the-middle attack is able to read the SAS and then use it just as the intended user could have, potentially compromising sensitive data or allowing 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 expiration on these very far in the future (or infinite) and make sure it's regularly updated to move it farther into the future.
- **Use near-term expiration times on an ad hoc SAS.** In this way, even if a SAS is compromised, it's valid only for a short time. This practice is especially important if you cannot 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, in order to allow time for retries if the service providing the SAS is unavailable. If your SAS is meant to be used for a small number of immediate, short-lived operations that are expected to be completed within the expiration period, then this may be unnecessary as the SAS is not expected to be renewed. However, if you have a client that is routinely making requests via SAS, then the possibility of expiration comes into play. The key consideration is to balance the need for the SAS to be short-lived (as previously stated) with the need to ensure that the client is requesting renewal early enough (to avoid disruption due to the SAS expiring prior to successful renewal).
- **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 200GB 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.

Azure Files and File Sync

Files vs Blobs

File storage⁵ offers shared storage for applications using the industry standard **SMB protocol**⁶. 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, just as 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.

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
Azure Files	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 which 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.

⁵ <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

⁶ <https://msdn.microsoft.com/library/windows/desktop/aa365233.aspx>

Feature	Description	When to use
Azure Blobs	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.

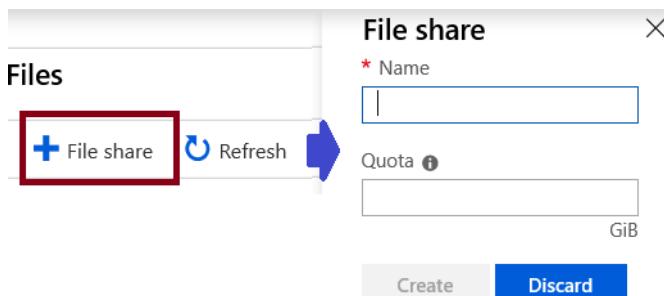
Other distinguishing features, when selecting Azure files.

- 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.
- ✓ 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.

For more information, [What is Azure Files?](#)⁷.

Managing File Shares

To access your files, you will need a storage account. Once that is in place, 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. All of this information is available by selecting **Connect** from your file share page.

⁷ <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

Windows [Linux](#) [macOS](#)

Drive letter

Z

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.

- ✓ Ensure port 445 is open. Azure Files uses SMB protocol. SMB communicates over TCP port 445 - 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.cred" ];
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. This can be done on-demand with a 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.

- ✓ Because Azure storage doesn't support HTTPS for custom domain names, this option is not applied using a custom domain name.

File Share Snapshots

Azure Files provides the capability to take share snapshots of file shares. Share snapshots capture the share state at that point in time. A share snapshot is 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. This 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. If 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. If 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 $resourceGroupName -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 "YourStorageAccountName" -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 $resourceGroupName -Name $storageAccountName
```

```
$fileShare = Get-AzStorageShare -Context $storageAccount.Context | Where-Object {
    $_.Name -eq $fileShareName -and $_.IsSnapshot -eq $false
}

if ($fileShare -eq $null) {
    throw [System.Exception]::new("Azure file share not found")
}

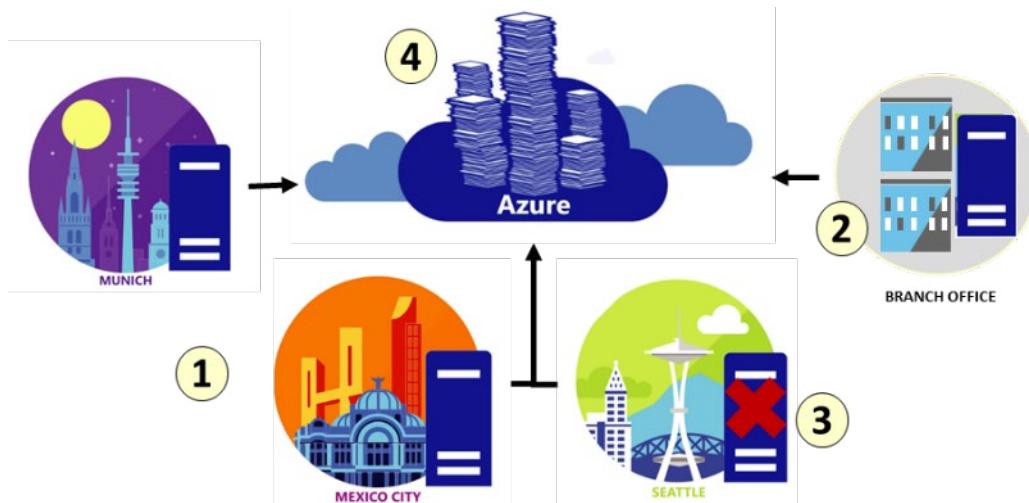
# The value given to the root parameter of the New-PSDrive cmdlet is the host address for the storage
# account,
# storage-account.file.core.windows.net for Azure Public Regions. $fileShare.StorageUri.PrimaryUri.Host is
# used because non-Public Azure regions, such as sovereign clouds or Azure Stack deployments, will
# have different
# hosts for Azure file shares (and other storage resources).
$password = ConvertTo-SecureString -String $storageAccountKeys[0].Value -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList "AZURE\$(($stor-
ageAccount.StorageAccountName)", $password
New-PSDrive -Name desired-drive-letter -PSProvider FileSystem -Root "\\$(($fileShare.StorageUri.Prima-
ryUri.Host)\$(($fileShare.Name))" -Credential $credential -Persist
```

When finished, you can dismount the file share by running the following command:

```
Remove-PSDrive -Name desired-drive-letter
```

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.



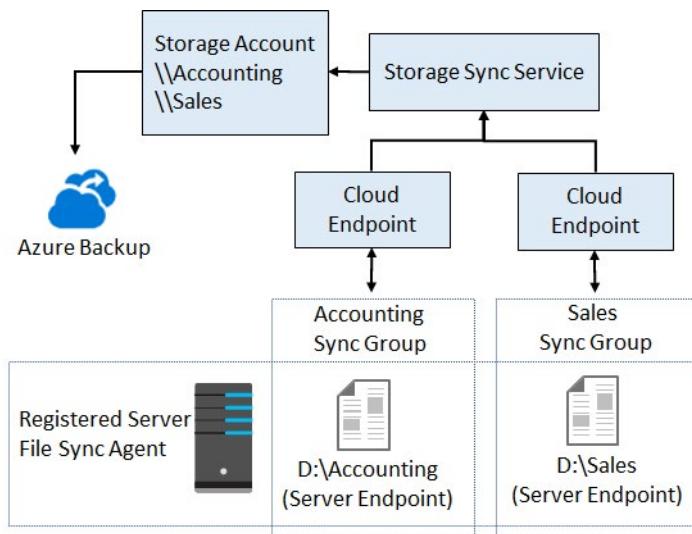
There are many uses and advantages to file sync.

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.
- ✓ 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.

For more information, [Planning for an Azure File Sync deployment⁸](#).

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.

⁸ <https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-planning>

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

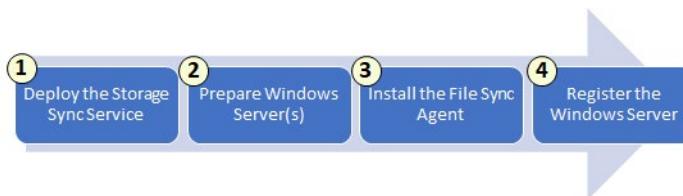
Server endpoint. A server endpoint represents a specific location on a registered server, such as a folder on a server volume. Multiple server endpoints can exist on the same volume if their namespaces do not overlap (for example, F:\sync1 and F:\sync2). You can configure cloud tiering policies individually 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.

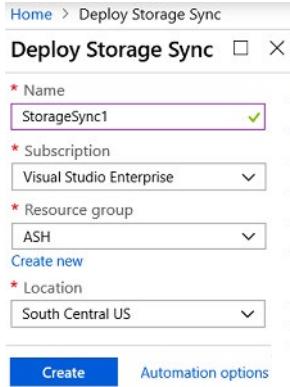
Cloud endpoint. A cloud endpoint is an Azure file share that is part of a sync group. The entire Azure file share syncs, and an Azure file share can be a member of only one cloud endpoint. Therefore, an Azure file share can be a member of only one sync group. If you add an Azure file share that has an 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.

File Sync Steps

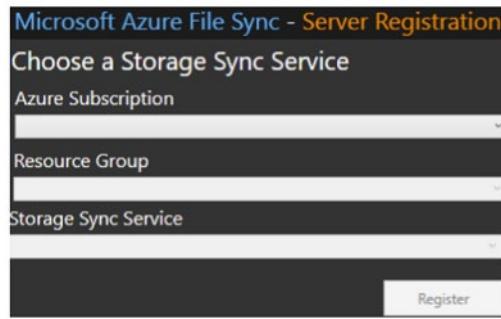
There are several high level steps for configuring File Sync.



1. **Deploy the Storage Sync Service.** The Storage Sync Service can be deployed from the Azure portal. 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 one). A server (or cluster) can be registered with only one Storage Sync Service at a time.

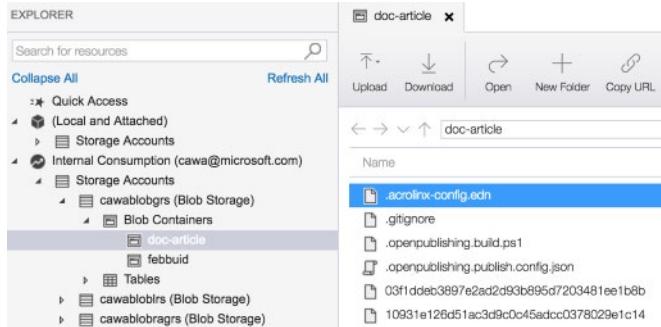


- ✓ Once File Sync is configured you will need to setup file synchronization.

Managing Storage

Azure Storage Explorer

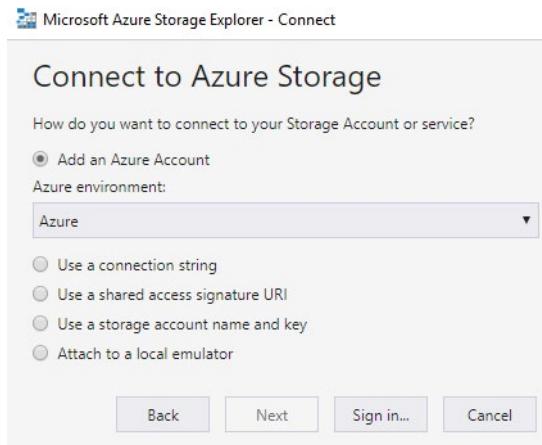
Azure Storage Explorer is a standalone app that makes it easy to work with Azure Storage data on Windows, macOS, and Linux. With Storage Explorer you can access multiple accounts and subscriptions and manage all your storage content.



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.



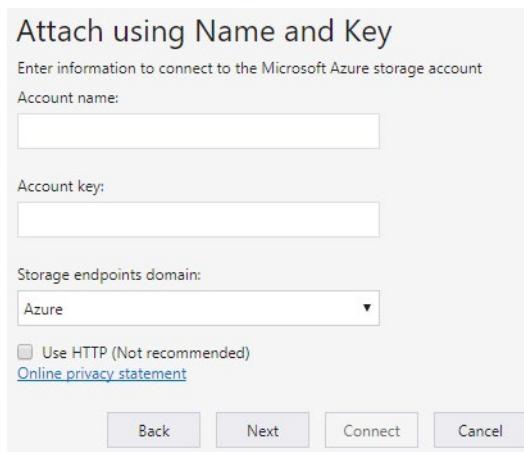
In addition, you can work with storage accounts in global and national Azure:

- **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.

✓ Access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. 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. We will cover access keys in more detail later.

✓ Notice this connection method provides access to the entire storage account.

For more information, [Get started with Storage Explorer⁹](#).

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

⁹ <https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows>

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.

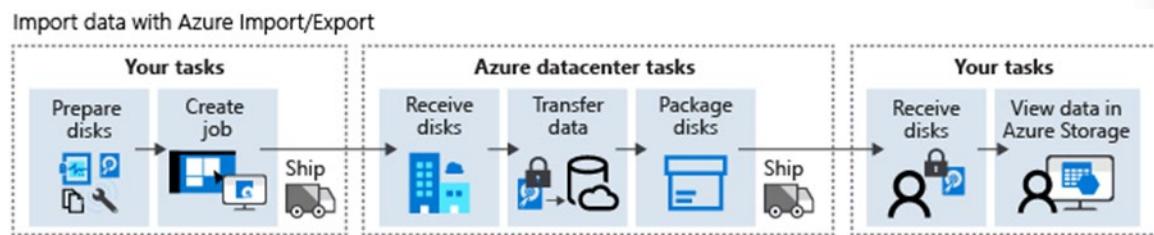
Usage Cases

Consider using Azure Import/Export service when uploading or downloading data over the network is too slow or getting additional 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.

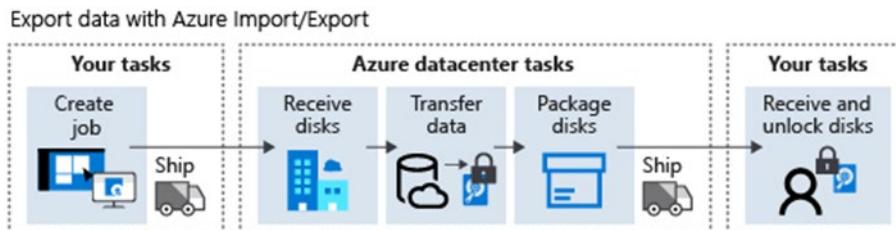


In order to perform an import, follow these steps:

- 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 WAImportExport tool.
- Run the WAImportExport 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.



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.

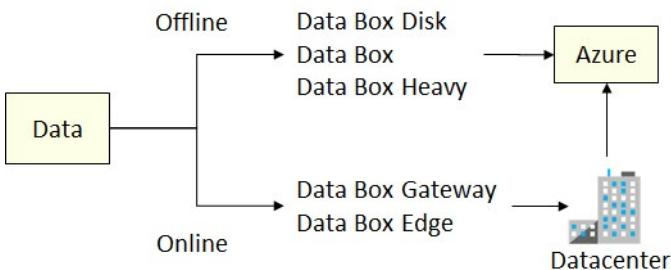
- ✓ You can create jobs directly from the Azure portal or you can accomplish this programmatically by using Azure Storage Import/Export REST API.

For more information, [Azure Import and Export Service¹⁰](https://azure.microsoft.com/en-us/documentation/articles/storage-import-export-service/).

¹⁰ <https://azure.microsoft.com/en-us/documentation/articles/storage-import-export-service/>

Data Box

Move stored or in-flight data to Azure quickly and cost-effectively. There are Data Box products for both offline and online scenarios.



Data Box for offline scenarios

Use Data Box offline data transfer products to move large amounts of data to Azure when you're limited by time, network availability, or costs. Scenarios for offline data box products include one-time migration, incremental transfers, and periodic updates. For example:

- Moving data from offline tapes to archival data in Azure cool storage.
- Moving a media library from offline tapes into Azure to create an online media library.
- Migrating your VM farm, SQL Server, and applications to Azure
- Moving historical data to Azure for in-depth analysis and reporting, using HDInsight.
- Moving backup data to Azure for offsite storage.

You can move your data to Azure using common copy tools such as Robocopy. All data is AES-encrypted, and the devices are wiped clean after upload in accordance with NIST Special Publication 800-88 revision 1 standards.

Product	Network Interfaces	Physical Security	Encryption
Data Box Disk	USB 3.0 connection	The disks are tamper-resistant and support secure update capability.	AES 128-bit
Data Box	1 Gbps or 10 Gbps network interfaces	Rugged device casing secured by tamper-resistant screws and tamper-evident stickers.	AES 256-bit
Data Box Heavy	High performance 40 Gbps network interfaces	Rugged device casing secured by tamper-resistant screws and tamper-evident stickers.	AES 256-bit

- ✓ Use the estimated speed to determine which box will transfer the data in the time frame you need. For data sizes < 40 TB, use Data Box Disk and for data sizes > 500 TB, sign up for Data Box Heavy.

Data Box for online scenarios

Data Box online data transfer products, Data Box Edge and Data Box Gateway, create a link between your site and Azure storage. This makes moving data to and from Azure as easy as working with a local network share. Their high-performance transfer capabilities take the hassle out of network data transport. Data Box Edge is also an artificial intelligence (AI)-enabled edge computing appliance.

Data Box Gateway

Data Box Gateway transfers data to and from Azure. It's a virtual appliance based on a virtual machine provisioned in your virtualized environment or hypervisor. The virtual device resides in your on-premises and you write data to it using the NFS and SMB protocols. The device then transfers your data to Azure block blob, page blob, or Azure Files. Use cases include:

- **Cloud archival.** Copy hundreds of TBs of data to Azure storage using Data Box Gateway in a secure and efficient manner. The data can be ingested one time or an ongoing basis for archival scenarios.
- **Data aggregation.** Aggregate data from multiple sources into a single location in Azure Storage for data processing and analytics.
- **Integration with on-premises workloads.** Integrate with on-premises workloads such as backup and restore that use cloud storage and need local access for commonly used files.

Data Box Edge

Data Box Edge is an on-premises physical network appliance transfers data to and from Azure. Analyze, process, and transform your on-premises data before uploading it to the cloud using AI-enabled edge compute capabilities. Azure Data Box Edge is an AI-enabled edge computing device with network data transfer capabilities. Use cases for Data Box Edge include:

- **Pre-process data.** Analyze data from on-premises or IoT devices to quickly get to results while staying close to where data is generated. Data Box Edge transfers the full data set to the cloud to perform more advanced processing or deeper analytics.
- **Inference Azure Machine Learning.** With Data Box Edge, you can run Machine Learning (ML) models to get quick results that can be acted on before the data is sent to the cloud. The full data set is transferred to continue to retrain and improve your ML models.
- **Transfer data over network to Azure.** Use Data Box Edge to easily and quickly transfer data to Azure to enable further compute and analytics or for archival purposes.

For more information, [Azure Data Box Products¹¹](#).

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.

¹¹ <https://azure.microsoft.com/en-us/services/storage/databox/>

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 as well as –include 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 /Source:<source> /Dest:<destination> [Options]
```

✓ AzCopy is available on Windows, Linux, and MacOS.

For more information, [Get started with AZCopy¹²](#).

Data Transfer Tool Selection

Dataset	Network Bandwidth	Solution to use
Large Dataset	Low-bandwidth network or direct connectivity to on-premises storage is limited by organization policies	Azure Import/Export for export; Data Box Disk or Data Box for import where supported; otherwise use Azure Import/Export

¹² <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy>

Dataset	Network Bandwidth	Solution to use
Large Dataset	High-bandwidth network: 1 gigabit per second (Gbps) - 100 Gbps	AZCopy for online transfers; or to import data, Azure Data Box Edge, or Azure Data Box Gateway
Large Dataset	Moderate-bandwidth network: 100 megabits per second (Mbps) - 1 Gbps	Azure Import/Export for export or Azure Data Box family for import where supported
Small dataset: a few GBs to a few TBs	Low to moderate-bandwidth network: up to 1 Gbps	If transferring only a few files, use Azure Storage Explorer, Azure portal, AZCopy, or AZ CLI

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 do a basic storage account connection.

In this demonstration, we will review several common Azure Storage Explorer tasks.

Download and install Storage Explorer

1. Download and install Azure Storage Explorer - <https://azure.microsoft.com/en-us/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, and 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 AZCopy¹³](#)
2. Install and launch the tool.

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.

¹³ <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>

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.

Module 07 Lab and Review

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

Module 07 Review Questions

Review Question 1

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. You need to reconfigure the storage to meet the following requirements:

- 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 shared access signature for the storage account and then set the allowed permissions to Read, set the allowed resource types to Object, and set the allowed services to Blob.
- Create a new access key for the storage account and then provide the connection string in the storage connectivity information to the public.

Review Question 2

Your company is planning to storage log data, crash dump files, and other diagnostic data for Azure VMs in Azure. The company has issued the following requirements for the storage:

- Administrators must be able to browse to the data in File Explorer.
- Access over SMB 3.0 must be supported.
- 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
- Queue storage

Review Question 3

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 Azure Table Storage.
- Deploy Azure Queues Storage.
- Deploy blob storage using block blobs.
- Deploy blob storage using append blobs.

Review Question 4

Your company is building an app in Azure. The app has the following storage requirements:

- Storage must be reachable programmatically through a REST API.
- Storage must be globally redundant.
- Storage must be accessible privately within the company's Azure environment.
- Storage must be optimal for unstructured data.

Which type of Azure storage should you use for the app? Select one.

- Azure Data Lake store
- Azure Table Storage
- Azure Blob Storage
- Azure File Storage

Review Question 5

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 in order 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.
- Use Azure Rights Management Services (RMS) to control access to each file.
- 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.

Review Question 6

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.
- Share the container entity tag (Etag) with the contingent staff member.
- Configure a Cross-Origin Resource Sharing (CORS) rule for the storage account.

Review Question 7

Your organization maintains historical images for large media companies. There are thousands of photos requiring over 600 TB of storage. Your datacenter has only limited bandwidth, and you need to quickly move the data to Azure blob storage. Additionally, security of the data including chain of custody logs and 256-bit encryption is required. Which of the following products would you recommend using? Select one.

- CDN
- Data Box
- Data Box Heavy
- Data Box Gateway
- Data Box Edge
- Import/Export

Review Question 8

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.
- The performance tier you select does not affect pricing.
- You can switch between hot and cool performance tiers at any time.

Review Question 9

You are planning a delegation model for your Azure storage. The company has issued the following requirements for Azure storage access:

- Apps in the non-production environment must have automated time-limited access

- Apps in the production environment must have unrestricted access to storage resources

You need to configure storage access to meet the requirements. What should you do? (Each answer presents part of the solution. Select two.)

- Use shared access signatures for the non-production apps.
- Use shared access signatures for the production apps.
- Use access keys for the non-production apps.
- Use access keys for the production apps.
- Use Stored Access Policies for the production apps.
- Use Cross Origin Resource Sharing for the non-production apps.

Review Question 10

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. The company has the following requirements:

- Microsoft Azure should maintain the exact same data as the shared folder on FS01.
- Files deleted on either side (on-premises or cloud) shall be subsequently and automatically deleted from the other side (on-premises or cloud).

You need to implement a solution to meet the requirements. What should you do? Select one.

- Deploy DFS Namespaces.
- Install and use AZCopy.
- Deploy Azure File Sync.
- Install and use Azure Storage Explorer.
- Deploy storage tiering.

Review Question 11

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
- Geo-redundant storage
- Read-access geo-redundant storage
- Zone-redundant storage

Review Question 12

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 File Server Resource Manager
- Use the Robocopy command-line tool
- Use the AzCopy command-line tool

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Create an Azure Storage account¹⁴**
- **Secure your Azure Storage¹⁵**
- **Optimize storage performance and costs using Blob storage tiers¹⁶**
- **Make your application storage highly available with read-access geo-redundant storage¹⁷**
- **Copy and move blobs from one container or storage account to another from the command line and in code¹⁸**
- **Move large amounts of data to the cloud by using Azure Data Box family¹⁹**
- **Monitor, diagnose, and troubleshoot your Azure storage²⁰**

¹⁴ <https://docs.microsoft.com/en-us/learn/modules/create-azure-storage-account/>

¹⁵ <https://docs.microsoft.com/en-us/learn/modules/secure-azure-storage-account/>

¹⁶ <https://docs.microsoft.com/en-us/learn/modules/optimize-archive-costs-blob-storage/>

¹⁷ <https://docs.microsoft.com/en-us/learn/modules/ha-application-storage-with-grs/>

¹⁸ <https://docs.microsoft.com/en-us/learn/modules/copy-blobs-from-command-line-and-code/>

¹⁹ <https://docs.microsoft.com/en-us/learn/modules/move-data-with-azure-data-box/>

²⁰ <https://docs.microsoft.com/en-us/learn/modules/monitor-diagnose-and-troubleshoot-azure-storage/>

Answers

Review Question 1

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. You need to reconfigure the storage to meet the following requirements:

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 shared access signature for the storage account and then set the allowed permissions to Read, set the allowed resource types to Object, and set the allowed services to Blob.
- Create a new access key for the storage account and then provide the connection string in the storage connectivity information to the public.

Explanation

In this scenario, you need to reconfigure 50 containers. While you can do that, it goes against the requirement to reduce the administrative overhead of future access changes. A shared access signature could work here, but not with the settings outlined in the answer choice. An access key is meant for use by your apps when communicating internally in Azure to the storage. In this scenario, 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).

Review Question 2

Your company is planning to storage log data, crash dump files, and other diagnostic data for Azure VMs in Azure. The company has issued the following requirements for the storage:

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
- Queue 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.

Review Question 3

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 Azure Table Storage.
- Deploy Azure Queues Storage.
- Deploy blob storage using block blobs.
- Deploy blob storage using append blobs.

Explanation

Append blobs optimize append operations (writes adding onto a log file, for example). In this scenario, the company needs to write data to log files, most often appending data (until a new log file is generated). Block blobs are cost efficient but not designed specifically for append operations, so performance isn't as high. Queue Storage is used for apps to communicate. Table Storage is a NoSQL database but not optimized for this scenario. Azure Files is geared for SMB storage, such as from Windows Servers but doesn't offer the optimized solution that append blobs do.

Review Question 4

Your company is building an app in Azure. The app has the following storage requirements:

Which type of Azure storage should you use for the app? Select one.

- Azure Data Lake store
- Azure Table Storage
- Azure Blob Storage
- Azure File Storage

Explanation

Azure Blob Storage is optimal for unstructured data and meets the requirements for the company's app. Azure Data Lake supports some of the requirements, such as unstructured data and REST API access. However, Azure Data Lake is geared for analytics workloads and is only available as locally-redundant (multiple copies of data in a single Azure region).

Review Question 5

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 in order 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.
- Use Azure Rights Management Services (RMS) to control access to each file.
- 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 achieves 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.

Review Question 6

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.
- Share the container entity tag (Etag) with the contingent staff member.
- 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.

Review Question 7

Your organization maintains historical images for large media companies. There are thousands of photos requiring over 600 TB of storage. Your datacenter has only limited bandwidth, and you need to quickly move the data to Azure blob storage. Additionally, security of the data including chain of custody logs and 256-bit encryption is required. Which of the following products would you recommend using? Select one.

- CDN
- Data Box
- Data Box Heavy
- Data Box Gateway
- Data Box Edge
- Import/Export

Explanation

Data Box Heavy. This product supports 1 PB total capacity per order and up to 800 TB usable capacity per order.

Review Question 8

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.
- The performance tier you select does not affect pricing.
- 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).

Review Question 9

You are planning a delegation model for your Azure storage. The company has issued the following requirements for Azure storage access:

You need to configure storage access to meet the requirements. What should you do? (Each answer presents part of the solution. Select two.)

- Use shared access signatures for the non-production apps.
- Use shared access signatures for the production apps.
- Use access keys for the non-production apps.
- Use access keys for the production apps.
- Use Stored Access Policies for the production apps.
- Use Cross Origin Resource Sharing for the non-production apps.

Explanation

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. Access keys provide unrestricted access to the storage resources, which is the requirement for production apps in this scenario.

Review Question 10

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. The company has the following requirements:

You need to implement a solution to meet the requirements. What should you do? Select one.

- Deploy DFS Namespaces.
- Install and use AZCopy.
- Deploy Azure File Sync.
- Install and use Azure Storage Explorer.
- 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.

Review Question 11

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
- Geo-redundant storage
- Read-access geo-redundant storage
- Zone-redundant storage

Explanation

Read-access geo-redundant storage (GRS) is the default replication option.

Review Question 12

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 File Server Resource Manager
- Use the Robocopy command-line tool
- Use the AzCopy command-line tool

Explanation

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.

Module 8 Azure Virtual Machines

Virtual Machine Planning

IaaS Cloud Services

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.

On-Premises (Private Cloud)	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Data & Access	Data & Access	Data & Access	Data & Access
Applications	Applications	Applications	Applications
Runtime	Runtime	Runtime	Runtime
Operating System	Operating System	Operating System	Operating System
Virtual Machine	Virtual Machine	Virtual Machine	Virtual Machine
Compute	Compute	Compute	Compute
Networking	Networking	Networking	Networking
Storage	Storage	Storage	Storage

You Manage
Cloud Provider Manages

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.
- ✓ Are you using virtual machines in Azure? What scenarios are of interest to you?

Planning Checklist

Provisioning VMs to Azure requires planning. Before you create a single VM be sure you have thought about the following:

- 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.

Location and Pricing

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. This lets you place your VMs as close as possible to your users to improve performance and to meet any legal, compliance, or tax requirements.

Two other things to think about regarding the location choice.

- **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 that will be incurred; even if the VM is stopped/deallocated and you aren't billed for the running VM, you will be 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 as well as start or stop at any time. Prefer 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. Prefer 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.

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:

VM Type	Family	Description
General Purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC	General-purpose VMs are designed to have a balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute Optimized	Fsv2	Compute optimized VMs are designed to have a high CPU-to-memory ratio. Suitable for medium traffic web servers, network appliances, batch processes, and application servers.

VM Type	Family	Description
Memory Optimized	Esv3, Ev3, Easv4, Eav4, Mv2, M, DSv2, Dv2	Memory optimized VMs are designed to have a high memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage Optimized	Lsv2	Storage optimized VMs are designed to have high disk throughput and IO. Ideal for VMs running databases.
GPU	NC, NCv2, NCv3, ND, NDv2, NV, NVv3, NVv4	GPU VMs are specialized virtual machines targeted for heavy graphics rendering and video editing. These VMs are ideal options for model training and inferencing with deep learning.
High Performance Compute	HB, HC, H	High performance compute is the fastest and most powerful CPU virtual machines with optional high-throughput network interfaces.

Resizing virtual machines

Azure allows you to change the VM size when the existing size no longer meets your needs. You can resize the VM - as long as your current hardware configuration is allowed in the new size. This provides a fully agile and elastic approach to VM management.

If you stop and deallocate the VM, you can then select any size available in your region since this removes your VM from the cluster it was running on.

- ✓ Be cautious when resizing production VMs - they may need to be rebooted which can cause a temporary outage and change some configuration settings such as the IP address.

For more information, [Sizes for Windows virtual machines in Azure¹](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json) and [Sizes for Linux virtual machines in Azure²](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes?toc=%2Fazure%2Fvirtual-machines%2Flinux%2Ftoc.json).

Virtual Machine Disks

Just like any other computer, virtual machines in Azure uses 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.

¹ <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json>

² <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes?toc=%2Fazure%2Fvirtual-machines%2Flinux%2Ftoc.json>

OS disk				
NAME	SIZE	STORAGE ACCOUNT...	ENCRYPTION	HOST CACHING
UbuntuServer_OsDisk_1_	30 GiB	Standard_LRS	Not enabled	Read/write
Data disks				
None				

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. This disk has a maximum capacity of 2,048 GiB. 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.
- 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.

Storage Operations

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 very 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.
- ✓ Managed disks are required for the single instance virtual machine SLA (99.95%).

Supported Operating Systems

Azure provides a variety of OS images that you can install into the VM, including several versions of Windows and flavors of Linux. As mentioned earlier, the choice of OS will influence your hourly compute pricing as Azure bundles the cost of the OS license into the price.

If you are looking for more than just base OS images, you can search the Azure Marketplace for more sophisticated install images that include the OS and popular software tools installed for specific scenarios. For example, if you needed a new WordPress site, the standard technology stack would consist of a Linux server, Apache web server, a MySQL database, and PHP. Instead of setting up and configuring each component, you can leverage a Marketplace image and install the entire stack all at once.

Finally, if you can't find a suitable OS image, you can create your disk image with what you need, upload it to Azure storage, and use it to create an Azure VM. Keep in mind that Azure only supports 64-bit operating systems.

Windows Server software

All Microsoft software that's installed in the Azure virtual machine environment must be licensed correctly. By default, Azure virtual machines include a license for many common products including Windows Server (selected roles and features), Microsoft Exchange, Microsoft SQL Server, and Microsoft SharePoint Server. Certain Azure virtual machine offerings may include additional Microsoft software on a per-hour or evaluation basis. Licenses for other software must be obtained separately.

- ✓ Microsoft does not support an upgrade of the Windows operating system of a Microsoft Azure virtual machine. Instead, you should create a new Azure virtual machine that is running the supported version of the operating system that is required and then migrate the workload.

Linux Server software

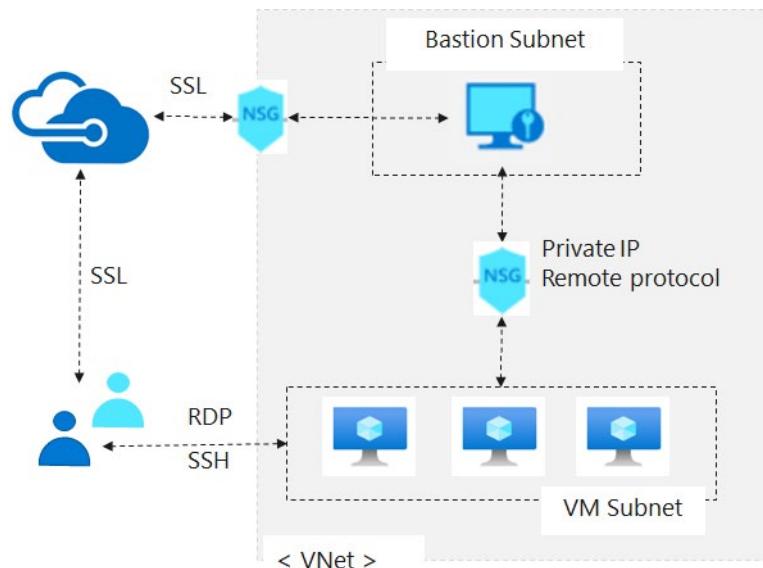
Azure supports many Linux distributions and versions including CentOS by OpenLogic, Core OS, Debian, Oracle Linux, Red Hat Enterprise Linux, and Ubuntu.

- ✓ Linux endorsed distributions supports an upgrade of the operating system of a Microsoft Azure virtual machine in case of full open source license. If licensed Linux distribution is used, then follow partner-specific rules to upgrade (BYOL or other).

For more information, [Microsoft server software support for Microsoft Azure virtual machines³](#) and [Linux on distributions endorsed by Azure⁴](#).

Virtual Machine Connections

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.

Note: How to connect using RDP and SSH will be covered in more detail in the next lesson.

³ <https://support.microsoft.com/en-us/help/2721672/microsoft-server-software-support-for-microsoft-azure-virtual-machines>

⁴ <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros>

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.

Creating Virtual Machines

Creating 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, Backup

Guest config - Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Windows Virtual Machines

Your use of the Windows Server images from Azure Marketplace Virtual Machine Gallery are provided to you for use with virtual machine instances under your Azure subscription which are governed by the Online Services Terms. These virtual machine instances are limited for use with Azure.

Latest Images

- Windows Server 2019 is the latest Long-Term Servicing Channel (LTSC) release with five years of mainstream support + five years of extended support. Choose the image that is right for your applica-

tion needs: 1) Server with Desktop Experience includes all roles including the graphical user interface (GUI), 2) Server Core omits the GUI for a smaller OS footprint, or 3) Containers option includes the Server with Desktop Experience, plus ready-made container images.

- Windows Server 2019 Datacenter - Server with Desktop Experience
- Windows Server 2019 Datacenter - with Containers
- Windows Server 2019 Datacenter - Server Core
- Windows Server 2019 Datacenter - Server Core with Containers

Windows Server Semi-Annual Channel releases deliver new operating system capabilities at a faster pace and are based on the Server Core installation option of the Datacenter edition. A new release comes out every six months and is supported for 18 months. Check the Lifecycle Support Page for support dates and always use the latest release if possible.

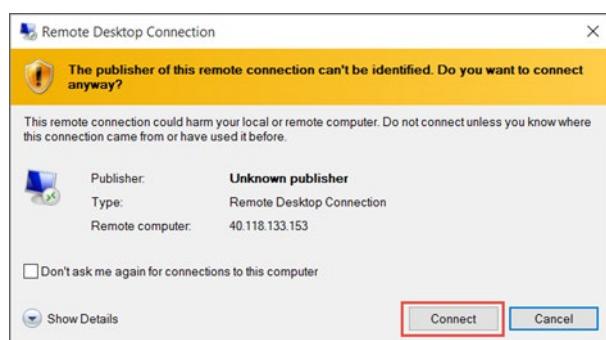
- ✓ There are also a large number of Windows Server 2016 and Windows Server 2012 images.

For more information, [Windows Virtual Machines Documentation⁵](#).

Windows VM Connections

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. This is 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.

⁵ <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/>

- 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.
- ✓ WinRM uses by TCP port 5986 by default, but you can change it to a custom value. In either case, you must ensure that no network security groups are blocking inbound traffic on the port that you choose.

Demonstration - Creating a VM in the Portal

In this demonstration, we will create and access a Windows virtual machine in the portal.

Create the virtual machine

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

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
```

When done, close the RDP connection to the VM.

View the IIS welcome page

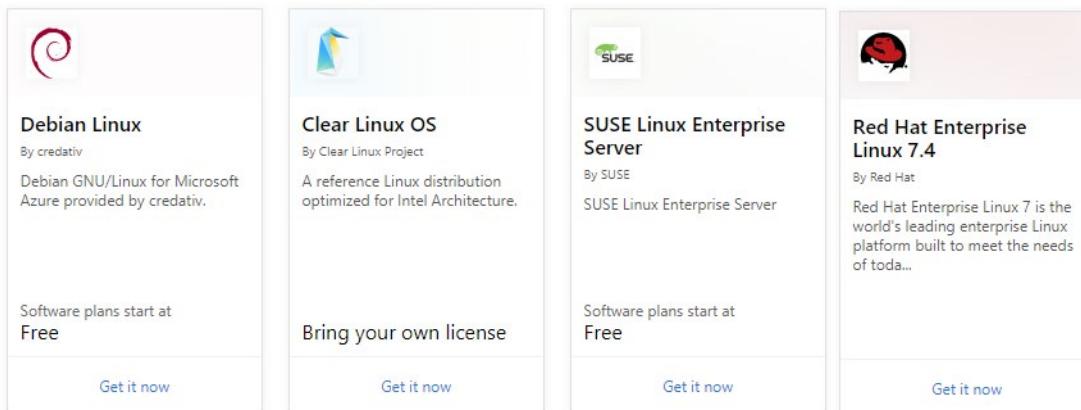
In the portal, select the VM and in the overview of the VM, use the **Click to copy** button to the right of the public IP address to copy it and paste it into a browser tab. The default IIS welcome page will open.

Clean up resources

- ✓ 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.

Linux Virtual Machines

Azure supports many Linux distributions and versions including CentOS by OpenLogic, Core OS, Debian, Oracle Linux, Red Hat Enterprise Linux, and Ubuntu.



Here are a few things to know about the Linux distributions.

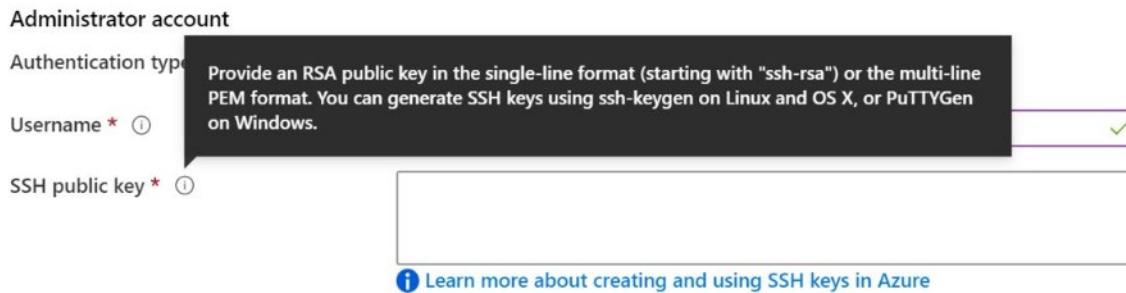
- There are hundreds of Linux images in the Azure Marketplace.
- Linux has the same deployment options as for Windows virtual machines: PowerShell (Resource Manager), Portal, and Command Line Interface.
- You can manage your Linux virtual machines with a host of popular open-source DevOps tools such as Puppet, and Chef.
- ✓ Take a few minutes to review the Marketplace Linux distributions. Are there any you are interested in?

For more information, [Linux virtual machines⁶](#).

Linux VM Connections

When you create a Linux VM, you can decide to authenticate with an **SSH public key** or **Password**.

⁶ <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/>



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.

- ✓ 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, locate and 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. Make a note of 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.

MCT USE ONLY. STUDENT USE PROHIBITED

Virtual Machine Availability

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.

Unplanned Hardware Maintenance

Unexpected Downtime

Planned Maintenance

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. This 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 at all times.

- ✓ What plans do you have in place to minimize the effect of downtime?

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, and your overall 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. When creating Availability sets keep these 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 can create availability sets through the Azure portal in the disaster recovery section. Also, you can build them using Resource Manager templates, or any of the scripting or API tools.

Instance details

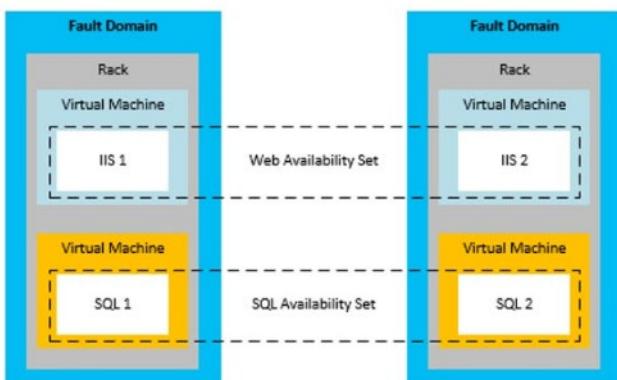
Name *	<input type="text" value="avset01"/>
Region *	<input type="text" value="(US) East US"/>
Fault domains	<input type="text" value="2"/>
Update domains	<input type="text" value="5"/>
Use managed disks	<input checked="" type="radio"/> Yes (Aligned)

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%.
- ✓ 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.

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 twenty update domains.

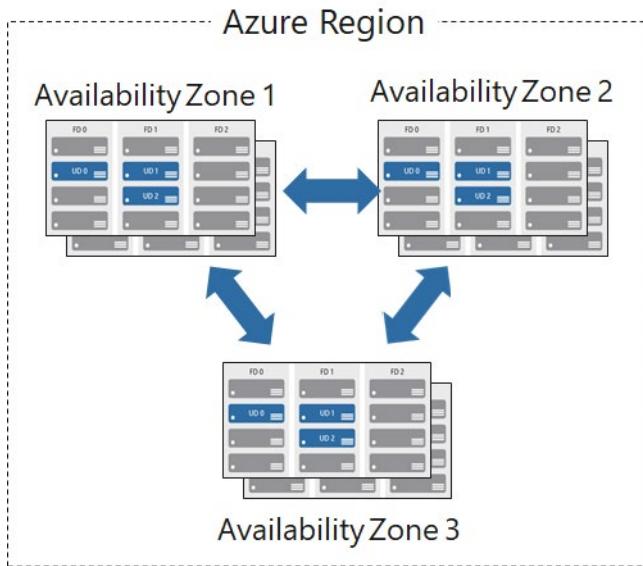
Fault domains

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. This mitigates against the effects of hardware failures, network outages, power interruptions, or software updates. Think of a fault domain as nodes belonging to the same physical rack.

- ✓ 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.

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 co-locating your compute, storage, networking, and data resources within a zone and replicating in other zones.

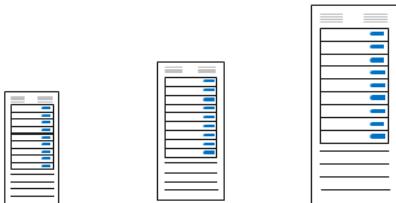
Azure services that support Availability Zones fall into two categories:

- **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).
- ✓ To achieve comprehensive business continuity on Azure, build your application architecture using the combination of Availability Zones with Azure region pairs.

Scaling Concepts

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 a increase (scale out) or decrease (scale in) in the number of virtual machine instances.

Considerations

- Vertical scaling generally has more limitations. It's 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 generally 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?

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, VM scale sets are designed to support true auto-scale – no pre-provisioning of VMs is required – and as such makes it easier to build large-scale services targeting big compute, big data, and containerized workloads. So, as demand goes up more virtual machine instances can be added, and 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 300 VM instances.

Implementing Scale Sets

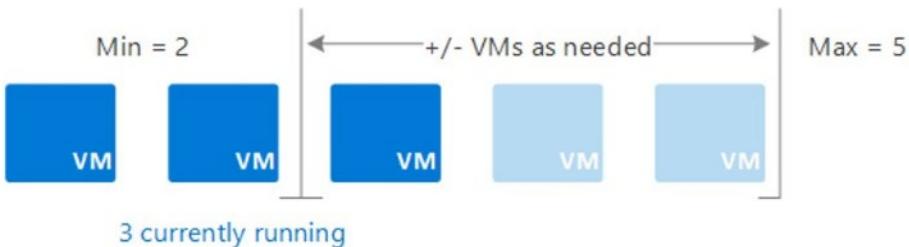
The screenshot shows the 'Instance' configuration page for a scale set. Key settings include:

- Initial instance count ***: 2
- Size ***: Standard D2s v3 (2 vcpus, 8 GiB memory (\$85.41/month))
- Azure Spot instance**: No
- Use managed disks**: Yes
- Allocation policy**: Enable scaling beyond 100 instances: Yes
- Spreading algorithm**: Max spreading

- **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, enabling several types of workloads to run for a significantly 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 1 placement group and can have 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, as this approach provides the best spreading in most cases.

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.
- ✓ 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.

Implementing 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 section for a scale set. It includes fields for initial instance count (2), scaling policy (Custom), and scale-out/in rules based on CPU usage thresholds and duration.

Setting	Value
Initial instance count *	2
Scaling policy	<input type="radio"/> Manual <input checked="" type="radio"/> Custom
Minimum number of VMs *	1
Maximum number of VMs *	10
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.

For more information, **Best Practices for Autoscale**⁷.

⁷ <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-autoscale-best-practices>

Virtual Machine Extensions

Virtual Machine Extensions

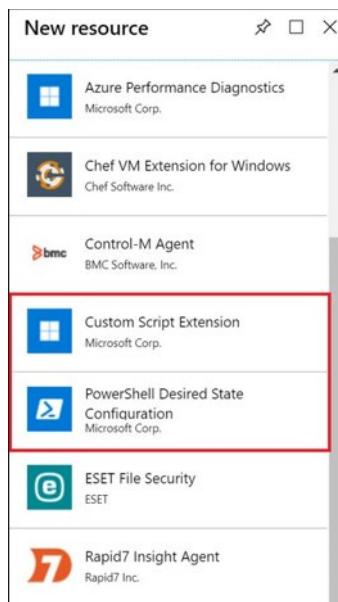
Creating and maintaining virtual machines can be a lot of work, and much of it is repetitive, requiring the same steps each time. Fortunately, there are several ways to automate the tasks of creating, maintaining, and removing virtual machines. One way is to use a virtual machine **extension**.

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.

There are different extensions for Windows and Linux machines and a large choice of first and third-party extensions.



- ✓ In this lesson we will focus on two extensions: Custom Script Extensions and Desired State Configuration. Both tools are based on PowerShell.

For more information, **Virtual machine extensions and features for Windows⁸** and **Virtual machine extensions and features for Linux⁹**.

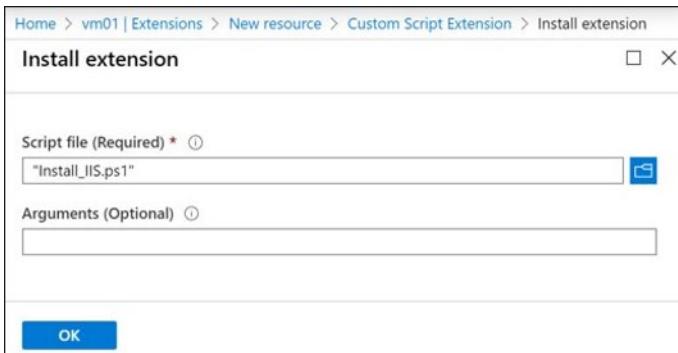
⁸ <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/features-windows?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json>

⁹ <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/features-linux>

Custom Script Extension

Custom Script Extension(CSE) can be used to automatically launch and execute virtual machine customization tasks post configuration. Your script extension may perform very 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. Once the file is uploaded it executes immediately.



You could also use the PowerShell **Set-AzVmCustomScriptExtension** command. You need to upload the script file to a blob container and provide the URI in the command like this:

```
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. And, of course, 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?
- ✓ Can you think of any custom script extensions that you might want to create?

Desired State Configuration

Desired State Configuration (DSC) is a management platform in Windows PowerShell that 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. It 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 will saved as a .ps1 file.

```
configuration IISInstall
{
    Node "localhost"
    {
        WindowsFeature IIS
        {
            Ensure = "Present"
            Name = "Web-Server"
        }
    }
}
```

Notice the DSC script consists of the following:

- The **Configuration** block. This is the outermost script block. You define it by using the **Configuration** keyword and providing a name. In this case, the name of the configuration is *IISInstall*.
 - One or more **Node** blocks. These define the nodes (computers or VMs) that you are configuring. In the above configuration, there is one Node block that targets a computer named "localhost".
 - One or more resource blocks. This is where the configuration sets the properties for the resources that it is configuring. In this case, 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.
- ✓ The Windows PowerShell DSC comes with a set of built-in configuration resources. For example, File Resource, Log Resource, and User Resource. Use the reference link to view the resources that are available to you. Are there any resources that you might be interested in?

Demonstration - Custom Script Extension

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

12. Return to your virtual machine RDP session.
13. 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.

Module 08 Lab and Review Questions

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: Deploy zone-resilient Azure virtual machine scale sets by using the Azure portal.
- Task 5: Configure Azure virtual machine scale sets by using virtual machine extensions.
- Task 6: Scale compute and storage for Azure virtual machine scale sets.
- ✓ Consult with your instructor for how to access the lab instructions and lab environment (if provided).

Module 08 Review Questions

Review Question 1

You host a service with two Azure virtual machines. You discover that occasional outages cause your service to fail. What two actions can you do to minimize the impact of the outages? Select two.

- Add a load balancer.
- Put the virtual machines in an availability set.
- Put the virtual machines in a scale set.
- Add a network gateway.
- Add a third instance of the virtual machine.

Review Question 2

You are researching Microsoft Azure for your company. The company is considering deploying Windows-based VMs in Azure. However, before moving forward, the management team has asked you to research the costs associated with Azure VMs. You need to document the configuration options that are likely to save the company money on their Azure VMs. Which options should you document? (Each answer presents part of the solution. Select four.)

- Use HDD instead of SSD for VM storage.
- Use unmanaged premium storage instead of managed standard storage.
- Bring your own Windows custom images.
- Use different Azure regions.
- Use the least powerful VMs that meet your requirements.
- Place all VMs in the same resource group.
- Bring your own Windows license for each VM.

Review Question 3

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
- Azure multi-factor authentication
- Access keys
- Shared access signature
- Security vault certificate

Review Question 4

Your company has Windows Server 2012 R2 VMs and Ubuntu Linux VMs in Microsoft Azure. The company has a new project to standardize the configuration of servers across the Azure environment. The company opts to use Desired State Configuration (DSC) across all VMs. You need to ensure that DSC can be used across all the VMs. What two things should you do? Select two.

- Replace the Ubuntu VMs with Red Hat Enterprise Linux VMs.
- Deploy the DSC extension for Windows Server VMs.
- Deploy the DSC extension for Linux VMs.
- Replace the Windows Server 2012 R2 VMs with Windows Server 2016 VMs.

Review Question 5

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.
- Deploy the scale set automation script.

Review Question 6

Your company is preparing to deploy an application to Microsoft 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. To get better performance, the team has the following requirements:

- If the CPU across the servers goes above 85%, a new VM should be deployed to provide additional resources.
- 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.
- Deploy the app and use PowerShell Desired State Configuration (DSC).

Review Question 7

Your company is deploying a critical business application to Microsoft Azure. The uptime of the application is of utmost importance. The application has the following components:

- 2 web servers
- 2 application servers
- 2 database servers

You need to design the layout of the VMs to meet the following requirements:

- Each VM in a tier must run on different hardware

- Uptime for the application must be maximized

You need to deploy the VMs to meet the requirements. 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.
- Deploy a load balancer for the web VMs and an availability set to hold the application and database VMs.

Review Question 8

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
- Work offline and then reimage the virtual machine.

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Build a scalable application with virtual machine scale sets¹⁰**
- **Deploy Azure virtual machines from VHD templates¹¹**
- **Choose the right disk storage for your virtual machine workload¹²**
- **Add and size disks in Azure virtual machines¹³**
- **Protect your virtual machine settings with Azure Automation State Configuration¹⁴**

¹⁰ <https://docs.microsoft.com/en-us/learn/modules/build-app-with-scale-sets/>

¹¹ <https://docs.microsoft.com/en-us/learn/modules/deploy-vms-from-vhd-templates/>

¹² <https://docs.microsoft.com/en-us/learn/modules/choose-the-right-disk-storage-for-vm-workload/>

¹³ <https://docs.microsoft.com/en-us/learn/modules/add-and-size-disks-in-azure-virtual-machines/>

¹⁴ <https://docs.microsoft.com/en-us/learn/modules/protect-vm-settings-with-dsc/>

Answers

Review Question 1

You host a service with two Azure virtual machines. You discover that occasional outages cause your service to fail. What two actions can you do to minimize the impact of the outages? Select two.

- Add a load balancer.
- Put the virtual machines in an availability set.
- Put the virtual machines in a scale set.
- Add a network gateway.
- Add a third instance of the virtual machine.

Explanation

To minimize the impact put the virtual machines in an availability set and add a load balancer.

Review Question 2

You are researching Microsoft Azure for your company. The company is considering deploying Windows-based VMs in Azure. However, before moving forward, the management team has asked you to research the costs associated with Azure VMs. You need to document the configuration options that are likely to save the company money on their Azure VMs. Which options should you document? (Each answer presents part of the solution. Select four.)

- Use HDD instead of SSD for VM storage.
- Use unmanaged premium storage instead of managed standard storage.
- Bring your own Windows custom images.
- Use different Azure regions.
- Use the least powerful VMs that meet your requirements.
- Place all VMs in the same resource group.
- Bring your own Windows license for each VM.

Explanation

In this scenario, you need to document which of the options presented are likely to save the company money for their Azure VMs. While this isn't an exhaustive list, the correct money-saving configuration options are: Use HDD instead of SSD, use different Azure regions, use the least powerful VMs that meet your requirements, and bring your own Windows license (instead of paying for a license with the VM). The other options usually increase cost.

Review Question 3

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
- Azure multi-factor authentication
- Access keys
- Shared access signature
- Security vault certificate

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.

Review Question 4

Your company has Windows Server 2012 R2 VMs and Ubuntu Linux VMs in Microsoft Azure. The company has a new project to standardize the configuration of servers across the Azure environment. The company opts to use Desired State Configuration (DSC) across all VMs. You need to ensure that DSC can be used across all the VMs. What two things should you do? Select two.

- Replace the Ubuntu VMs with Red Hat Enterprise Linux VMs.
- Deploy the DSC extension for Windows Server VMs.
- Deploy the DSC extension for Linux VMs.
- Replace the Windows Server 2012 R2 VMs with Windows Server 2016 VMs.

Explanation

Desired State Configuration (DSC) is available for Windows Server and Linux-based VMs. In this scenario, you just need to deploy the extensions to the existing VMs to start using DSC.

Review Question 5

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.
- Deploy the scale set automation script.

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.

Review Question 6

Your company is preparing to deploy an application to Microsoft 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. To get better performance, the team has the following requirements:

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.
- Deploy the app and use PowerShell Desired State Configuration (DSC).

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.

Review Question 7

Your company is deploying a critical business application to Microsoft Azure. The uptime of the application is of utmost importance. The application has the following components:

You need to design the layout of the VMs to meet the following requirements:

You need to deploy the VMs to meet the requirements. 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.
- Deploy a load balancer for the web VMs and an availability set to hold the application and database VMs.

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).

Review Question 8

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
- Work offline and then reimage the virtual machine.

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.

Module 9 Serverless Computing

Azure App Service Plans

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 resource in a different geographical region.

For more information, [Azure App Service plan overview](#)¹.

App Service Plan 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

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:

- **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.

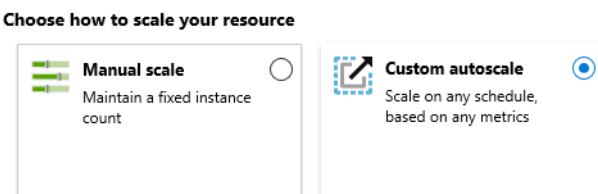
¹ <https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans>

- **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.

For more information, [App Service Plan Pricing²](#).

App Service Plan Scaling

There are two workflows 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.

² <https://azure.microsoft.com/en-us/pricing/details/app-service/windows/>

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.

App Service Plan Scale Out

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.

The screenshot shows the 'Default' autoscale profile in the Azure portal. It includes the following settings:

- Delete warning:** A note stating "The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale."
- Scale mode:** Set to "Scale based on a metric".
- Rules:** A note stating "No metric rules defined; click hyperlink [Add a rule](#) to scale out and scale in your instances based on rules. For example: 'Add a rule that increases instance count by 1 when CPU percentage is above 70%'." Below this is a link "+ Add a rule".
- Instance limits:** Set to Minimum 1, Maximum 2, Default 1.
- Schedule:** Set to "This scale condition is executed when none of the other scale condition(s) match".

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](#)³.
2. Search for and select **App Service Plans**.
3. Click **+ Add** to create a new App Service plan.

Setting	Value
Subscription	Choose your subscription
Resource Group	myRGAppServices (create new)
Name	AppServicePlan1
Operating System	Windows
Region	East US

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**.

³ <http://portal.azure.com/>

Note: This rule will add an instance when the CPU percentages is greater than 80% for 10 minutes.

Setting	Value
Time aggregation	Average
Metric name	CPU percentage
Operator	Greater than
Threshold	80
Duration	10 minutes
Operation	Increase count by
Instance count	1
Cool down	5 minutes

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?

Azure App Services

App Service Overview

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.

Learn how to deploy your first application to the cloud using App Service:



Learn how to deploy your code:



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.

- ✓ For the Azure Administrator certification focus on implementation tasks.

For more information: [Azure App Service Overview⁴](#)

Creating 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 *	webappces1	.azurewebsites.net
Publish *	Code	Docker Container
Runtime stack *	Select a runtime stack.	
Operating System *	Linux	Windows
Region *	Central US	<small>Not finding your App Service Plan? Try a different region.</small>

- **Name.** The name must be unique and will 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.

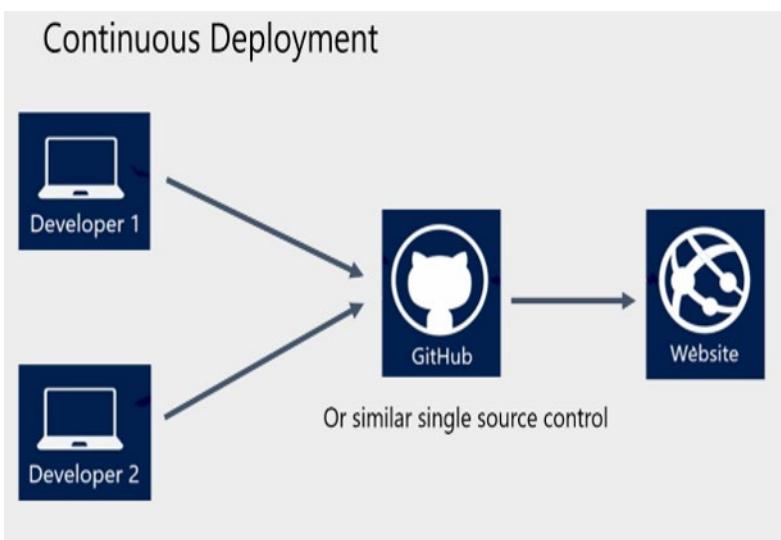
- **Always On.** Keep the app loaded even when there's no traffic. It's required for continuous WebJobs or for WebJobs that are triggered using a CRON expression.
- **ARR affinity.** In a multi-instance deployment, ensure that the client is routed to the same instance for the life of the session. You can set this option to Off for stateless application,

⁴ <https://docs.microsoft.com/en-us/azure/app-service/overview>

- **Connection strings.** Connection strings are encrypted at rest and transmitted over an encrypted channel.

Continuous Deployment

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.

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	Running	ASP-webapprg-a247	100
webappces-Staging	Running	ASP-webapprg-a247	0

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.

- ✓ Each App Service plan mode supports a different number of deployment slots.

For more information, [Set up staging environments⁵](#)

Creating 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 *
- Virtual network integration *
- 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

⁵ <https://docs.microsoft.com/en-us/azure/app-service/web-sites-staged-publishing?toc=%2Fazure%2Fapp-service%2Ftoc.json>

- IP restrictions
- Always On
- Diagnostic log settings
- Cross-origin resource sharing (CORS)

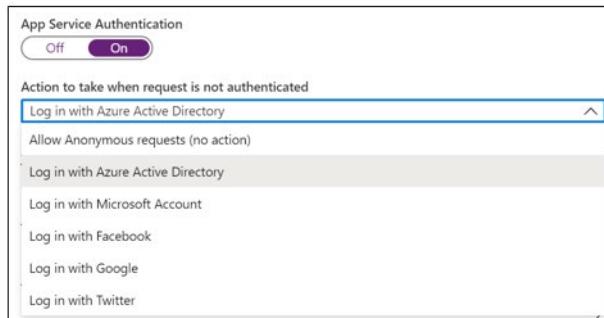
Secure an App Service

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.

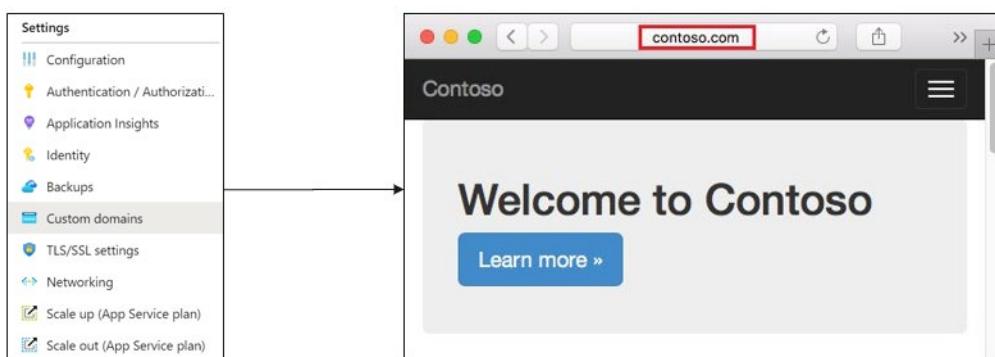
Caution: Restricting access in this way applies to all calls to your app, which may not be desirable for apps wanting a publicly available home page, as in many single-page applications.

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`.

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.



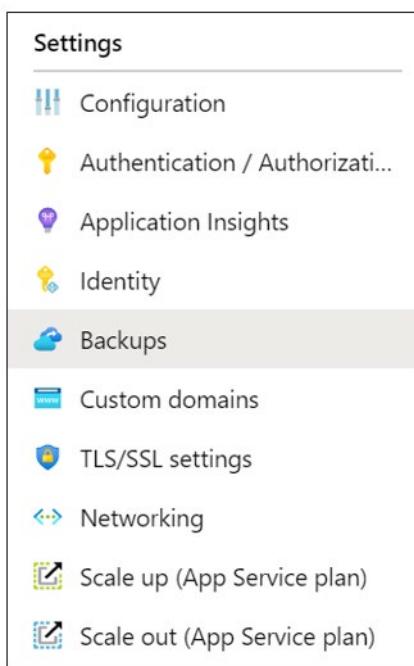
Configuration steps

- 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, their site will walk you through the process.
- 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.
- ✓ 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).

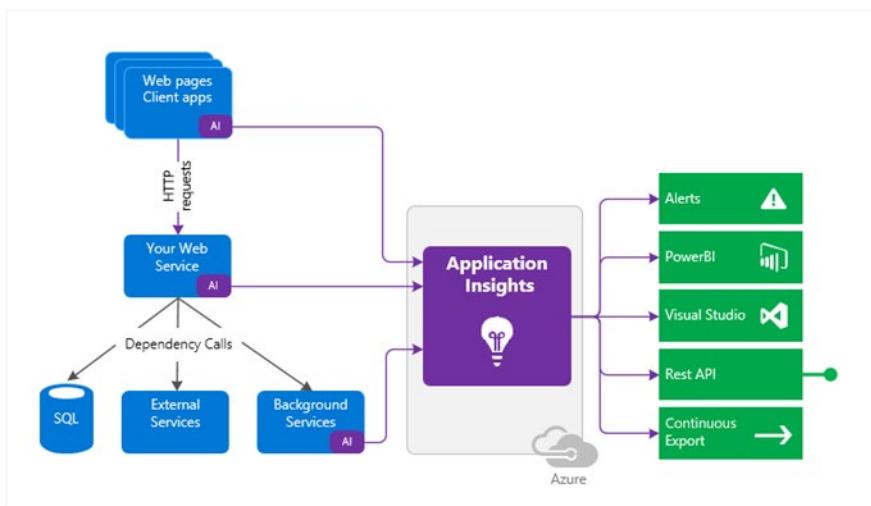
Considerations

- 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 blacklisted directories, or any blacklisted file, is left as is. You restore partial backups of your site the same way you would restore a regular backup. The restore process does the right thing.
- 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.

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. It works for apps on a wide variety of 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 telemetry 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.

For more information, [Application Insights⁶](#)

Demonstration - Create an 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 actually 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 commonly 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 portal⁷](#).
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	Choose your subscription
Resource Group	myRGWebApp1 (create new)
Name	myLinuxWebAppxxxx (unique)

⁶ <https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview>

⁷ <http://portal.azure.com/>

Setting	Value
Publish	Docker Container
Operating System	Linux
Region	East US (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	Single container
Image Source	Quickstart
Sample	Python Hello World

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 note 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	DEVELOPMENT
Clone Settings From	myLinuxWebAppXXXX

4. Click **Add**.
5. If the **Add a slot** blade remains open, click **Close**.
6. From the **Deployment Slots** blade, make a note of 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	webappxxxxstorage (unique)
Account kind	Storage (general purpose v1)
Performance	Standard
Replication	Locally-redundant storage (LRS)
Location	(US) East US

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	1 Hours
Start backup schedule from	Configure custom start time
Retention (Days)	30
Keep at least one backup	Yes

12. Click **Save**.

Container Services

Containers vs 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.

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 server.
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

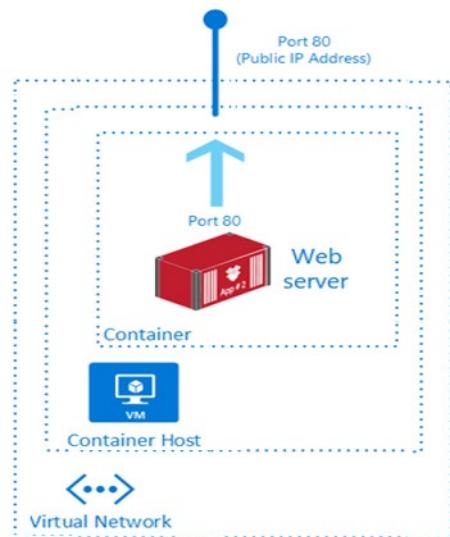
Containers offer several advantages over physical and virtual machines, including:

- 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.

For more information, **Containers vs Virtual Machines**⁸

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.

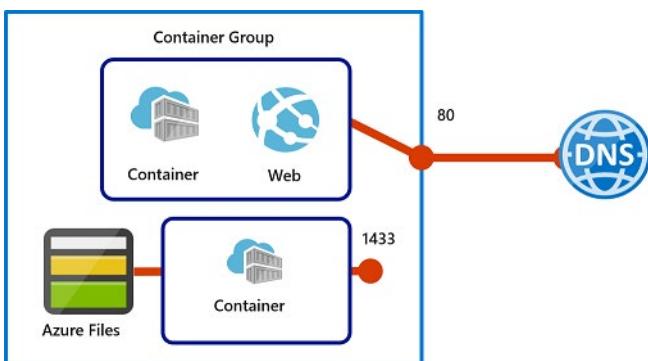


Feature	Description
Fast Startup Times	Containers can start in seconds without the need to provision and manage virtual machines.
Public IP Connectivity and DNS Names	Containers can be directly exposed to the internet with an IP address and a FQDN.
Hypervisor-level Security	Container applications are 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.
Co-scheduled 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.

⁸ <https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/containers-vs-vm>

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 5000.
- 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 1 CPU, then the container group is allocated 2 CPUs.

Networking

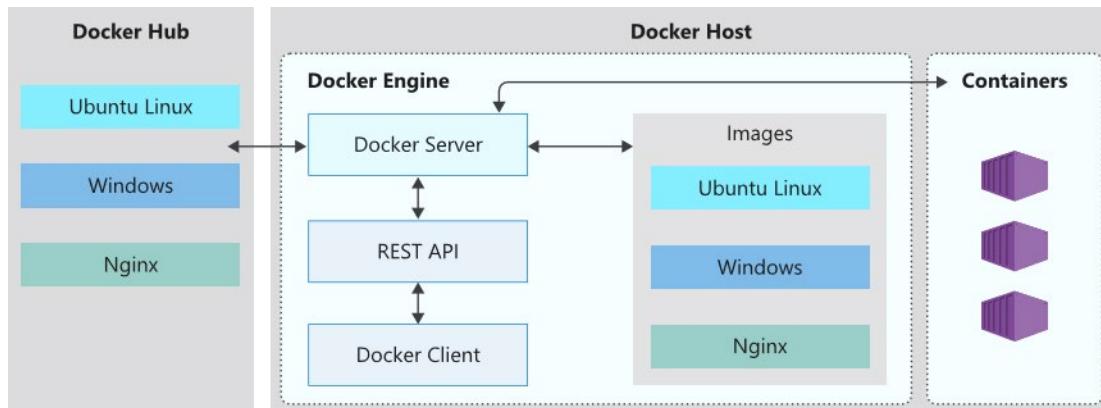
Container groups can share an external-facing IP address, one or more ports on that IP address, and a DNS label with a fully qualified domain name (FQDN). To enable external clients to reach a container within the group, you must expose the port on the IP address and from the container. Because containers 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.

Docker



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. This means it includes things like:

- 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 a Docker provides is the guarantee that the containerized software will always run the same, regardless of whether it is being run locally on Windows, Linux or in the cloud on Azure. This means, for instance, that software can be developed locally within a Docker container, shared with QA (Quality Assurance) resources for testing and then deployed to production in the Azure Cloud. Once deployed to the Azure Cloud, the application can easily be scaled up and down using the Azure Container Service (AKS).

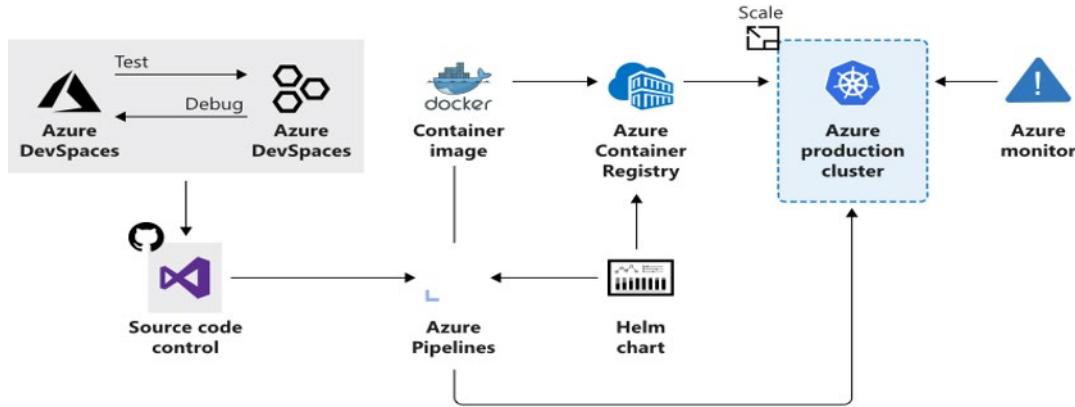
Docker terminology

You should be familiar with the following key terms before using Docker and Container Instances to create, build, and test containers:

- **Container.** This 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.** This 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.** This refers to the action of building a container image based on the information and context provided by its Dockerfile, plus additional files in the folder where the image is built. You can build images by using the Docker docker build command.
- **Pull.** This refers to the process of downloading a container image from a container registry.
- **Push.** This refers to the process of uploading a container image to a container registry.
- **Dockerfile.** This refers to a text file that contains instructions on how to build a Docker image. It's like a batch script; the first line states the base image, followed by instructions to install required programs, copy files, and so on until you get the working environment you need.

Azure Kubernetes Service

Azure Kubernetes Service



Azure Kubernetes Service (AKS)

Kubernetes is a rapidly evolving platform that manages container-based applications and their associated networking and storage components. The focus is on the application workloads, not the underlying infrastructure components. Kubernetes provides a declarative approach to deployments, backed by a robust set of APIs for management operations.

You can build and run modern, portable, microservices-based applications that benefit from Kubernetes orchestrating and managing the availability of those application components. Kubernetes supports both stateless and stateful applications as teams progress through the adoption of microservices-based applications.

As an open platform, Kubernetes allows you to build your applications with your preferred programming language, OS, libraries, or messaging bus. Existing continuous integration and continuous delivery (CI/CD) tools can integrate with Kubernetes to schedule and deploy releases.

Azure Kubernetes Service (AKS) provides a managed Kubernetes service that reduces the complexity for deployment and core management tasks, including coordinating upgrades. The AKS cluster masters are managed by the Azure platform, and you only pay for the AKS nodes that run your applications. AKS is built on top of the open-source Azure Container Service Engine (acs-engine).

Azure Kubernetes Service (AKS) makes it simple to deploy a managed Kubernetes cluster in Azure. AKS reduces the complexity and operational overhead of managing Kubernetes by offloading much of that responsibility to Azure. As a hosted Kubernetes service, Azure handles critical tasks like health monitoring and maintenance for you. In addition, the service is free, you only pay for the agent nodes within your clusters, not for the masters.

Features

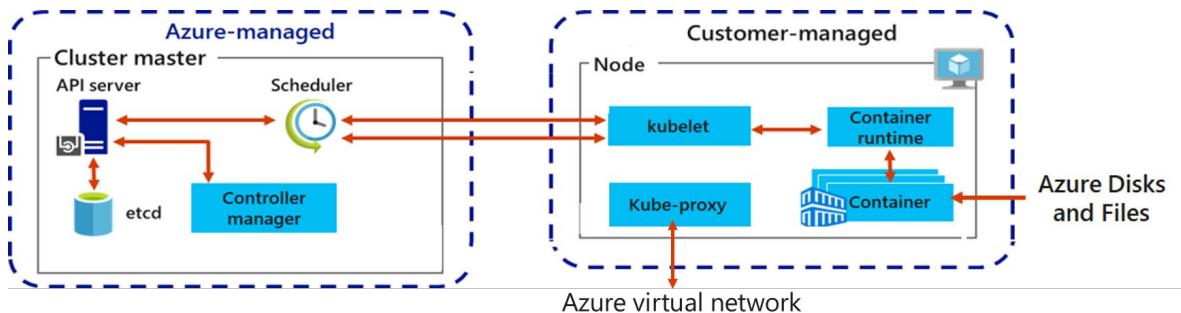
Feature	Description
Flexible deployment options	Azure Kubernetes Service offers portal, command line, and template driven deployment options (Resource Manager templates and Terraform). When deploying an AKS cluster, the Kubernetes master and all nodes are deployed and configured for you. Additional features such as advanced networking, Azure Active Directory integration, and monitoring can also be configured during the deployment process.
Identity and security management	AKS clusters support Role-Based Access Control (RBAC). An AKS cluster can also be configured to integrate with Azure Active Directory. In this configuration, Kubernetes access can be configured based on Azure Active Directory identity and group membership.
Integrated logging and monitoring	Container health gives you performance visibility by collecting memory and processor metrics from containers, nodes, and controllers. Container logs are also collected. This data is stored in your Log Analytics workspace, and is available through the Azure portal, Azure CLI, or a REST endpoint.
Cluster node scaling	As demand for resources increases, the nodes of an AKS cluster can be scaled out to match. If resource demand drops, nodes can be removed by scaling in the cluster. AKS scale operations can be completed using the Azure portal or the Azure CLI.
Cluster node upgrades	Azure Kubernetes Service offers multiple Kubernetes versions. As new versions become available in AKS, your cluster can be upgraded using the Azure portal or Azure CLI. During the upgrade process, nodes are carefully cordoned and drained to minimize disruption to running applications.
HTTP application routing	The HTTP Application Routing solution makes it easy to access applications deployed to your AKS cluster. When enabled, the HTTP application routing solution configures an ingress controller in your AKS cluster. As applications are deployed, publically accessible DNS names are auto configured.
GPU enabled nodes	AKS supports the creation of GPU enabled node pools. Azure currently provides single or multiple GPU enabled VMs. GPU enabled VMs are designed for compute-intensive, graphics-intensive, and visualization workloads.

Feature	Description
Development tooling integration	Kubernetes has a rich ecosystem of development and management tools such as Helm, Draft, and the Kubernetes extension for Visual Studio Code. These tools work seamlessly with Azure Kubernetes Service. Additionally, Azure Dev Spaces provides a rapid, iterative Kubernetes development experience for teams. With minimal configuration, you can run and debug containers directly in Azure Kubernetes Service (AKS).
Virtual network integration	An AKS cluster can be deployed into an existing VNet. In this configuration, every pod in the cluster is assigned an IP address in the VNet, and can directly communicate with other pods in the cluster, and other nodes in the VNet. Pods can connect also to other services in a peered VNet, and to on-premises networks over ExpressRoute and site-to-site (S2S) VPN connections.
Private container registry	Integrate with Azure Container Registry (ACR) for private storage of your Docker images.

AKS Clusters and Nodes

A Kubernetes cluster is divided into two components:

- **Cluster master nodes**, which provide the core Kubernetes services and orchestration of application workloads.
- **Nodes** that run your application workloads.



Cluster master

When you create an AKS cluster, a cluster master is automatically created and configured. This cluster master is provided as a managed Azure resource abstracted from the user. There is no cost for the cluster master, only the nodes that are part of the AKS cluster.

Nodes and node pools

To run your applications and supporting services, you need a Kubernetes node. An *AKS cluster*, which is an Azure virtual machine (VM) that runs the Kubernetes node components and container runtime, contains one or more nodes:

- The *kubelet* is the Kubernetes agent that processes the orchestration requests from the cluster master, 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. In AKS, Docker is used as the 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.

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.

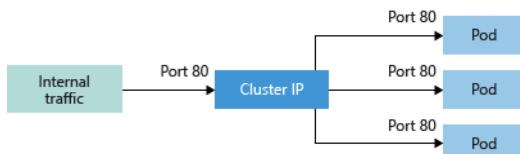
In Kubernetes, Services logically group pods to allow for direct access via an IP address or DNS name and on a specific port. You can also distribute traffic using a load balancer. More complex routing of application traffic can also be achieved with Ingress Controllers. Security and filtering of the 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.

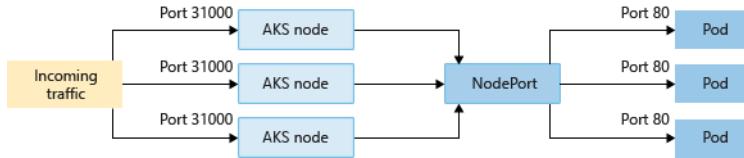
Services

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:

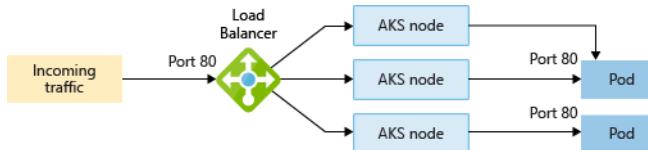
- **Cluster IP** - Creates an internal IP address for use within the AKS cluster. Good for internal-only applications that support other workloads within the cluster.



- **NodePort** - Creates a port mapping on the underlying node that allows the application to be accessed directly with the node IP address and port.



- **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 customer 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.

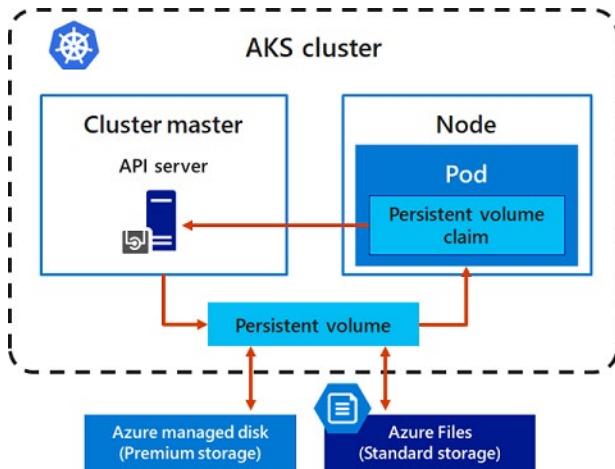
When you create a pod, you can define resource limits to request a certain amount of CPU or memory resources. The Kubernetes Scheduler attempts to schedule the pods to run on a node with available resources to meet the request. You can also specify maximum resource limits that prevent a given pod from 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.

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. Currently, Files can only use Azure Standard storage backed by regular HDDs.

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, two initial StorageClasses are created:

- *default* - Uses Azure Standard storage to create a Managed Disk. The reclaim policy indicates that the underlying Azure Disk is deleted when the pod that used it is deleted.
- *managed-premium* - Uses Azure Premium storage to create Managed Disk. The reclaim policy again indicates that the underlying Azure Disk is deleted when the pod 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`. The following example uses Premium Managed Disks and specifies that the underlying Azure Disk should be retained when the pod is deleted:

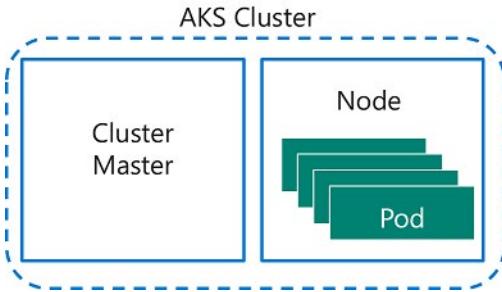
Persistent volume claims

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.

AKS Service Security

To protect your customer data as you run application workloads in Azure Kubernetes Service (AKS), the security of your cluster is a key consideration. Kubernetes includes security components such as network policies and Secrets. Azure then adds in components such as network security groups and orchestrated cluster upgrades. These security components are combined to keep your AKS cluster running the latest OS security updates and Kubernetes releases, and with secure pod traffic and access to sensitive credentials.



This section introduces the core concepts that secure your applications in AKS:

- Master components security
- Node security
- Cluster upgrades
- Network security
- Kubernetes Secrets

Master security

In AKS, the Kubernetes master components are part of the managed service provided by Microsoft. Each AKS cluster has their own single-tenanted, dedicated Kubernetes master to provide the API Server, Scheduler, etc. This master is managed and maintained by Microsoft

By default, the Kubernetes API server uses a public IP address and with fully qualified domain name (FQDN). You can control access to the API server using Kubernetes role-based access controls and Azure Active Directory.

Node security

AKS nodes are Azure virtual machines that you manage and maintain. The nodes run an optimized Ubuntu Linux distribution with the Docker container runtime. When an AKS cluster is created or scaled up, the nodes are automatically deployed with the latest OS security updates and configurations.

The Azure platform automatically applies OS security patches to the nodes on a nightly basis. If an OS security update requires a host reboot, that reboot is not automatically performed. You can manually reboot the nodes, or a common approach is to use **Kured**⁹, an open-source reboot daemon for Kubernetes. Kured runs as a [DaemonSet][aks-daemonset] and monitors each node for the presence of a file indicating that a reboot is required. Reboots are managed across the cluster using the same cordon and drain process as a cluster upgrade.

Nodes are deployed into a private virtual network subnet, with no public IP addresses assigned. For troubleshooting and management purposes, SSH is enabled by default. This SSH access is only available using the internal IP address. Azure network security group rules can be used to further restrict IP range access to the AKS nodes. Deleting the default network security group SSH rule and disabling the SSH service on the nodes prevents the Azure platform from performing maintenance tasks.

To provide storage, the nodes use Azure Managed Disks. For most VM node sizes, these are Premium disks backed by high-performance SSDs. The data stored on managed disks is automatically encrypted at

⁹ <https://github.com/weaveworks/kured>

rest within the Azure platform. To improve redundancy, these disks are also securely replicated within the Azure datacenter.

Cluster upgrades

For security and compliance, or to use the latest features, Azure provides tools to orchestrate the upgrade of an AKS cluster and components. This upgrade orchestration includes both the Kubernetes master and agent components. You can view a list of available Kubernetes versions for your AKS cluster. To start the upgrade process, you specify one of these available versions. Azure then safely cordons and drains each AKS node and performs the upgrade.

Cordon and drain

During the upgrade process, AKS nodes are individually cordoned from the cluster so new pods are not scheduled on them. The nodes are then drained and upgraded as follows:

- Existing pods are gracefully terminated and scheduled on remaining nodes.
- The node is rebooted, the upgrade process completed, and then joins back into the AKS cluster.
- Pods are scheduled to run on them again.
- The next node in the cluster is cordoned and drained using the same process until all nodes are successfully upgraded.

Network security

For connectivity and security with on-premises networks, you can deploy your AKS cluster into existing Azure virtual network subnets. These virtual networks may have an Azure Site-to-Site VPN or Express Route connection back to your on-premises network. Kubernetes ingress controllers can be defined with private, internal IP addresses so services are only accessible over this internal network connection.

Azure network security groups

To filter the flow of traffic in virtual networks, Azure uses network security group rules. These rules define the source and destination IP ranges, ports, and protocols that are allowed or denied access to resources. Default rules are created to allow TLS traffic to the Kubernetes API server and for SSH access to the nodes. As you create services with load balancers, port mappings, or ingress routes, AKS automatically modifies the network security group for traffic to flow appropriately.

Kubernetes Secrets

A Kubernetes *Secret* is used to inject sensitive data into pods, such as access credentials or keys. You first create a Secret using the Kubernetes API. When you define your pod or deployment, a specific Secret can be requested. Secrets are only provided to nodes that have a scheduled pod that requires it, and the Secret is stored in *tmpfs*, not written to disk. When the last pod on a node that requires a Secret is deleted, the Secret is deleted from the node's *tmpfs*. Secrets are stored within a given namespace and can only be accessed by pods within the same namespace.

The use of Secrets reduces the sensitive information that is defined in the pod or service YAML manifest. Instead, you request the Secret stored in Kubernetes API Server as part of your YAML manifest. This approach only provides the specific pod access to the Secret.

AKS and Azure Active Directory

There are different ways to authenticate with and secure Kubernetes clusters. Using role-based access controls (RBAC), you can grant users or groups access to only the resources they need. With Azure Kubernetes Service (AKS), you can further enhance the security and permissions structure by using Azure Active Directory. These approaches help you secure your application workloads and customer data.

This section introduces the core concepts that help you authenticate and assign permissions in AKS:

- Kubernetes service accounts
- Azure Active Directory integration
- Role-based access controls (RBAC)
- Roles and ClusterRoles
- RoleBindings and ClusterRoleBindings

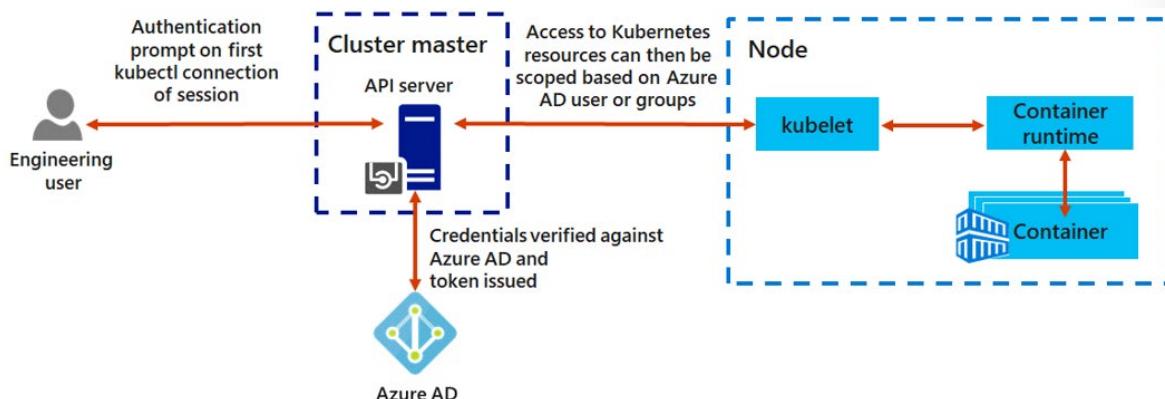
Kubernetes service accounts

One of the primary user types in Kubernetes is a service account. A service account exists in, and is managed by, the Kubernetes API. The credentials for service accounts are stored as Kubernetes secrets, which allows them to be used by authorized pods to communicate with the API Server. Most API requests provide an authentication token for a service account or a normal user account.

Normal user accounts allow more traditional access for human administrators or developers, not just services and processes. Kubernetes itself does not provide an identity management solution where regular user accounts and passwords are stored. Instead, external identity solutions can be integrated into Kubernetes. For AKS clusters, this integrated identity solution is Azure Active Directory.

Azure Active Directory integration

The security of AKS clusters can be enhanced with the integration of Azure Active Directory (AD). Built on decades of enterprise identity management, Azure AD is a multi-tenant, cloud-based directory, and identity management service that combines core directory services, application access management, and identity protection. With Azure AD, you can integrate on-premises identities into AKS clusters to provide a single source for account management and security.



With Azure AD-integrated AKS clusters, you can grant users or groups access to Kubernetes resources within a namespace or across the cluster. To obtain a `kubectl` configuration context, a user can run the `az aks get-credentials` command. When a user then interacts with the AKS cluster with `kubectl`,

they are prompted to sign in with their Azure AD credentials. This approach provides a single source for user account management and password credentials. The user can only access the resources as defined by the cluster administrator.

Role-based access controls (RBAC)

To provide granular filtering of the actions that users can perform, Kubernetes uses role-based access controls (RBAC). This control mechanism lets you assign users, or groups of users, permission to do things like create or modify resources, or view logs from running application workloads. These permissions can be scoped to a single namespace, or granted across the entire AKS cluster. With Kubernetes RBAC, you create roles to define permissions, and then assign those *roles* to users with *role bindings*.

Azure role-based access controls (RBAC)

One additional mechanism for controlling access to resources is Azure role-based access controls (RBAC). Kubernetes RBAC is designed to work on resources within your AKS cluster, and Azure RBAC is designed to work on resources within your Azure subscription. With Azure RBAC, you create a *role definition* that outlines the permissions to be applied. A user or group is then assigned this role definition for a particular *scope*, which could be an individual resource, a resource group, or across the subscription.

Roles and ClusterRoles

Before you assign permissions to users with Kubernetes RBAC, you first define those permissions as a *Role*. Kubernetes roles grant permissions. There is no concept of a *deny* permission.

Roles are used to grant permissions within a namespace. If you need to grant permissions across the entire cluster, or to cluster resources outside a given namespace, you can instead use *ClusterRoles*.

A ClusterRole works in the same way to grant permissions to resources, but can be applied to resources across the entire cluster, not a specific namespace.

RoleBindings and ClusterRoleBindings

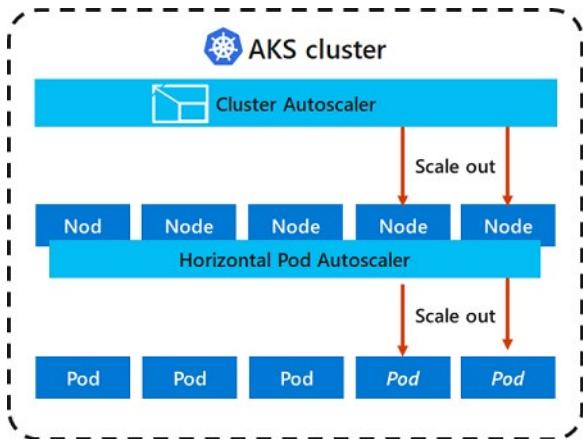
Once roles are defined to grant permissions to resources, you assign those Kubernetes RBAC permissions with a *RoleBinding*. If your AKS cluster integrates with Azure Active Directory, bindings are how those Azure AD users are granted permissions to perform actions within the cluster.

Role bindings are used to assign roles for a given namespace. This approach lets you logically segregate a single AKS cluster, with users only able to access the application resources in their assigned namespace. If you need to bind roles across the entire cluster, or to cluster resources outside a given namespace, you can instead use *ClusterRoleBindings*.

A ClusterRoleBinding works in the same way to bind roles to users, but can be applied to resources across the entire cluster, not a specific namespace. This approach lets you grant administrators or support engineers access to all resources in the AKS cluster.

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 additional 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.

Cooldown 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 autoscale 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 additional 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 additional 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 additional 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.

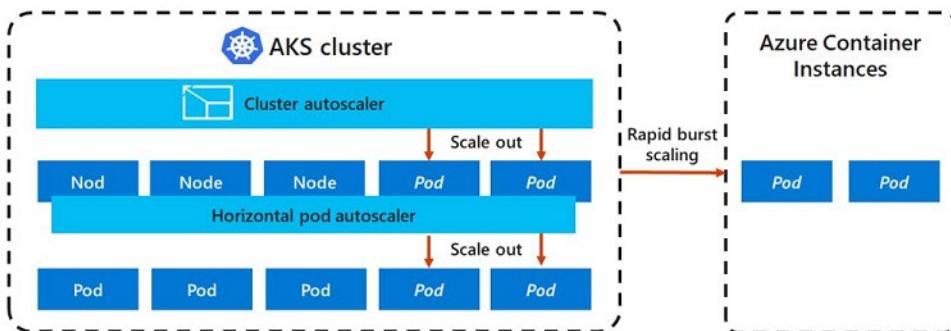
Scale down events

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.

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, but it may take a few minutes for those nodes to successfully provision and allow the Kubernetes scheduler to run pods on them.

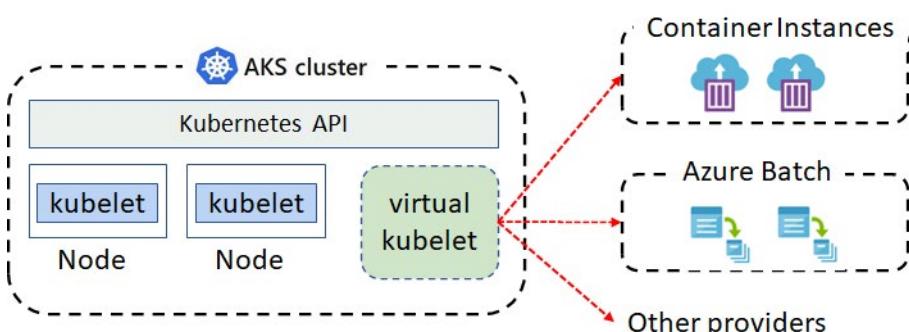
ACI lets you quickly deploy container instances without additional infrastructure overhead. When you connect with AKS, ACI becomes a secured, logical extension of your AKS cluster. The Virtual Kubelet component is installed in your AKS cluster that presents ACI as a virtual Kubernetes node. Kubernetes 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 and with no delay as cluster autoscaler deploys new nodes in your AKS cluster.

Virtual nodes are deployed to an additional 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.

Virtual Kubelet

Virtual Kubelet is an open-source Kubernetes kubelet implementation that masquerades as a kubelet.



In this example of a Kubernetes cluster, virtual kubelet is used to allow us to back our Kubernetes cluster with services such as Container Instances and Azure Batch. These services then host our individual nodes on behalf of the cluster.

The virtual kubelet registers itself as a node and allows developers to deploy pods and containers with their own APIs. This lets the virtual kubelet provide a shim layer with a pseudo-kubelet implementation enabling you to use other services for your individual instances.

Provider list

- Azure Batch
- Container Instances
- Alibaba Cloud Elastic Container Instance (ECI)
- AWS Fargate
- Kubernetes Container Runtime Interface (CRI)
- Huawei Cloud Container Instance (CCI)
- HashiCorp Nomad
- OpenStack Zun
- Custom provider

Demonstration - Deploy Azure Kubernetes Service

In this demonstration, we will deploy an Azure Kubernetes Service.

Create a Kubernetes service

1. Sign-in to the **Azure portal**¹⁰.
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**.
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.

¹⁰ <http://portal.azure.com/>

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](<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough-portal#run-the-application>).

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.

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.

Module 09 Lab and Review

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

Module 09 Review Questions

Review Question 1

You have multiple apps running in a single App Service plan. True or False: Each app in the service plan can have different scaling rules.

- True
- False

Review Question 2

Which of the following settings are not swapped when you swap an app? Select three.

- Handler mappings
- Publishing endpoints
- General settings, such as framework version, 32/64-bit, web sockets
- Always On
- Custom domain names

Review Question 3

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.

- Free
- Shared
- Basic
- Standard
- Premium

Review Question 4

You are backing up your App Service. Which of the following is included in the backup? Select two.

- App configuration
- Azure database for MySQL
- Files and database content totalling 15GB
- Firewall enabled-storage account
- SSL enabled Azure Database for MySQL

Review Question 5

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.

- Master node
- Pods
- Node virtual machines
- Tables

Review Question 6

Which of the following is not true about container groups? Select one.

- Is scheduled on a multiple host machines.
- Is assigned a DNS name label.
- Exposes a single public IP address, with one exposed port.
- Consists of two containers.
- Includes two Azure file shares as volume mounts.

Review Question 7

Which of the following is the Kubernetes agent that processes the orchestration requests from the cluster master, and schedules running the requested containers? Select one.

- controller master
- container runtime
- kube-proxy
- kubelet

Review Question 8

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
- Load Balancer
- NodePort

Review Question 9

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
- synchronization of accounts across providers

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Host a web application with Azure App service¹¹**
- **Stage a web app deployment for testing and rollback by using App Service deployment slots¹²**
- **Scale an App Service web app to efficiently meet demand with App Service scale up and scale out¹³**
- **Dynamically meet changing web app performance requirements with autoscale rules¹⁴**
- **Capture and view page load times in your Azure web app with Application Insights¹⁵**
- **Introduction to Docker containers¹⁶**

¹¹ <https://docs.microsoft.com/en-us/learn/modules/host-a-web-app-with-azure-app-service/>

¹² <https://docs.microsoft.com/en-us/learn/modules/stage-deploy-app-service-deployment-slots/>

¹³ <https://docs.microsoft.com/en-us/learn/modules/app-service-scale-up-scale-out/>

¹⁴ <https://docs.microsoft.com/en-us/learn/modules/app-service-autoscale-rules/>

¹⁵ <https://docs.microsoft.com/en-us/learn/modules/capture-page-load-times-application-insights/>

¹⁶ <https://docs.microsoft.com/en-us/learn/modules/intro-to-docker-containers/>

- Run Docker containers with Azure Container Instances¹⁷
- Introduction to the Azure Kubernetes Service¹⁸

¹⁷ <https://docs.microsoft.com/en-us/learn/modules/run-docker-with-azure-container-instances/>

¹⁸ <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-kubernetes-service/>

Answers

Review Question 1

You have multiple apps running in a single App Service plan. True or False: Each app in the service plan can have different scaling rules.

- True
- False

Explanation

False. 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.

Review Question 2

Which of the following settings are not swapped when you swap an app? Select three.

- Handler mappings
- Publishing endpoints
- General settings, such as framework version, 32/64-bit, web sockets
- Always On
- Custom domain names

Explanation

Publishing endpoints, Always on, and Custom domain names. 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).

Review Question 3

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.

- Free
- Shared
- Basic
- Standard
- Premium

Explanation

Standard. The Standard App Service Plan meets the requirements at the least cost.

Review Question 4

You are backing up your App Service. Which of the following is included in the backup? Select two.

- App configuration
- Azure database for MySQL
- Files and database content totalling 15GB
- Firewall enabled-storage account
- SSL enabled Azure Database for MySQL

Explanation

App configuration and Azure database for MySQL. App Service can back up: app configuration, file content, and a database connected to your app (SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, MySQL in-app). 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. SSL enabled Azure Database for MySQL does not get backed up.

Review Question 5

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.

- Master node
- Pods
- Node virtual machines
- Tables

Explanation

Node virtual machines. You only pay for the virtual machines instances, storage, and networking resources consumed by your Kubernetes cluster.

Review Question 6

Which of the following is not true about container groups? Select one.

- Is scheduled on a multiple host machines.
- Is assigned a DNS name label.
- Exposes a single public IP address, with one exposed port.
- Consists of two containers.
- Includes two Azure file shares as volume mounts.

Explanation

Is scheduled on a multiple host machines. A container group is scheduled on a single host machine.

Review Question 7

Which of the following is the Kubernetes agent that processes the orchestration requests from the cluster master, and schedules running the requested containers? Select one.

- controller master
- container runtime
- kube-proxy
- kubelet

Explanation

kubelet. The kubelet process the orchestration requests from the cluster master, and schedules the running the requested containers.

Review Question 8

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
- Load Balancer
- NodePort

Explanation

NodePort. NodePort maps incoming direct traffic to the pods.

Review Question 9

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
- synchronization of accounts across providers

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

Module 10 Data Protection

File and Folder Backups

Azure Backup

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.

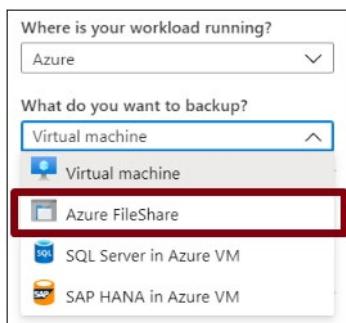
✓ What are some of the reasons your organization might choose Azure Backup? Is your organization using Azure Backup?

For more information, [What is Azure Backup?](#)¹

Recovery Service Vault Backup Options

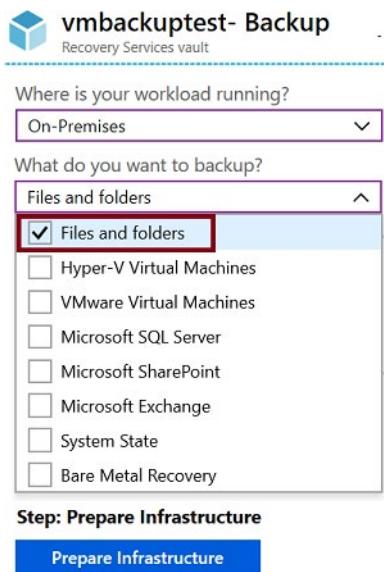
The **Recovery Services vault** is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services such as 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 file shares.



- The Recovery Services vault can also be used to backup on-premises files and folders.

¹ <https://docs.microsoft.com/en-us/azure/backup/backup-overview#why-use-azure-backup>



- ✓ Within an Azure subscription, you can create up to 25 Recovery Services vaults per region.
- ✓ Notice your backup choices for virtual machines. This will be covered in the next lesson.

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**.

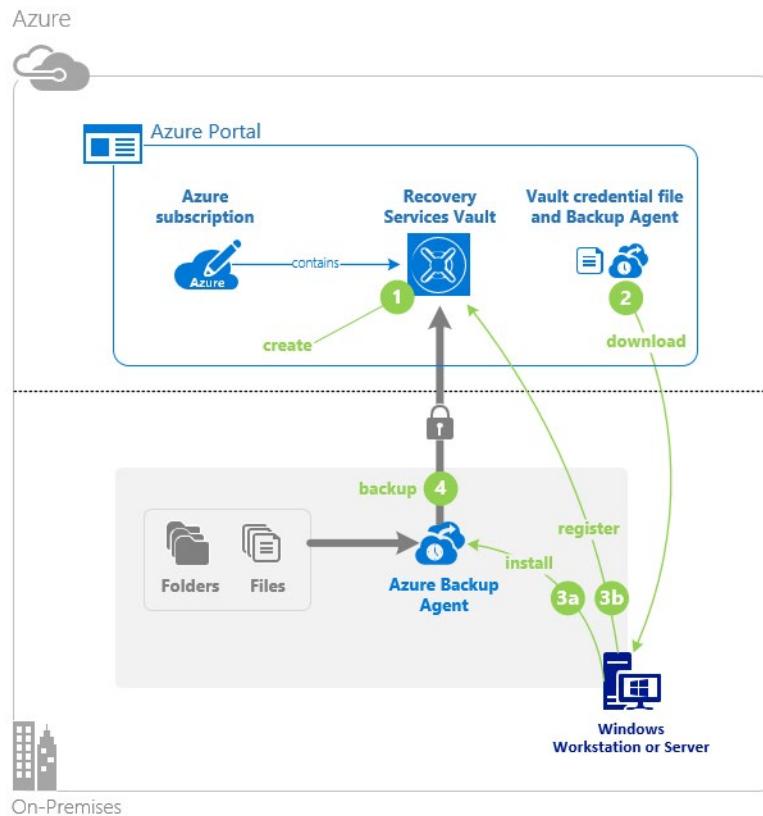
Verify the file share backup

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.

Implementing 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.



- Create the recovery services vault.** Within your Azure subscription you will need to create a recovery services vault for the backups.
- Download the agent and credential file.** The recovery services vault provides a link to download the Azure Backup Agent. The Backup Agent will be installed on the local machine. There is also a credentials file that is required during the installation of the agent. You must have the latest version of the agent. Versions of the agent below 2.0.9083.0 must be upgraded by uninstalling and reinstalling the agent.
- Install and register agent.** The installer provides a wizard to configure the installation location, proxy server, and passphrase information. The downloaded credential file will be used to register the agent.
- Configure the backup.** Use the agent to create a backup policy including when to backup, what to backup, how long to retain items, and settings like network throttling.

Microsoft 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" and "Microsoft Azure Backup supports scheduled backups of files and folders to an cloud storage account". A warning message indicates that backups have not been configured for this server, with a link to "Schedule Backup" in the Actions pane. Below this, there's a section titled "Jobs (Activity in the past 7 days, double click on the message to see details)" with tabs for "Jobs" and "Alerts". The "Jobs" tab is selected, showing a table with 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 main content is a vertical "Actions" menu with the following items:

- Backup (selected)
- Register Server
- Schedule Backup
- Recover Data
- Change Properties
- Open Portal
- Privacy & Cookies
- View
- Help

This is a full featured agent that has many features.

- Backup 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.
- Backup and restore content.
- No support for Linux.

Demonstration - Backup File 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. Note 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.

Virtual Machine Backups

Virtual Machine Data Protection

You can protect your data by taking backups at regular intervals. There are several backup options available for VMs, depending on your use-case.

Snapshots

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. The topics in this lesson will focus on Azure Backup.

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.
- ✓ Have you tried any of these backup methods? Do you have a backup plan?

Workload Protection Needs

There are several methods for backing up virtual machines.

1. Enable backup for individual Azure VMs. When you enable backup, Azure Backup installs an extension to the Azure VM agent that's running on the VM. The agent backs up the entire VM.
2. Run the MARS agent on an Azure VM. This is useful if you want to back up individual files and folders on the VM.
3. Back up an Azure VM to a System Center Data Protection Manager (DPM) server or Microsoft Azure Backup Server (MABS) running in Azure. Then back up the DPM server/MABS to a vault using Azure Backup.

Often those that are new to deploying workloads in a public cloud do not consider how they will protect the workload once it is hosted there. This is, of course, a critical requirement for business continuity.

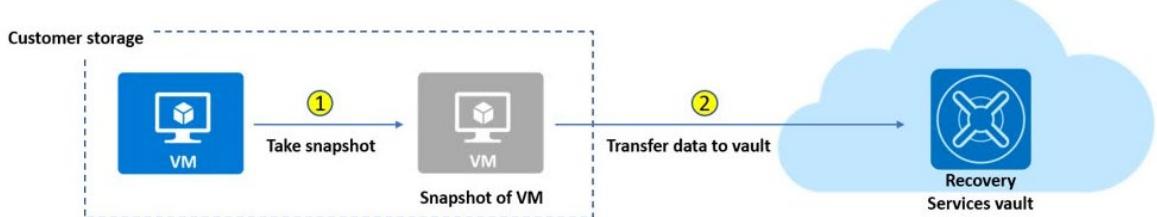
Document how the workload is being protected today, including how often the workload is backed up, what types of backups are accomplished, and whether disaster recovery protection is in place for the workload. Options for workload protection include:

- Extending on-premises data protection solutions into Azure. In many cases, an organization can extend their backup strategy into Azure by choosing from many of the backup solutions available today in the Azure Marketplace.
- Using native features in Azure to enable data protection, such as Azure Backup. Azure Backup is a native data protection service in Azure that allows for the protection of on-premises and Azure workloads.

The screenshot shows the Microsoft Azure Marketplace search results for the term "backup". The search bar at the top contains "backup". The results page displays 23 products under the "Product results" section. The products are categorized into four rows:

- Row 1:** Four instances of "Acronis Backup" by Acronis, Inc. Each card includes a large letter "A", a brief description ("The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available"), and a "Get it now" button.
- Row 2:** Four instances of "Seagate Backup Services" by Seagate, "Managed Backup Portal" by Veeam, "OFFICE 365 CLOUD BACKUP" by UpSafe, and "Quickbooks Online Backup" by Intuit, Inc. Each card includes a logo, a brief description, and a "Get it now" button.
- Row 3:** Three instances of "Acronis Backup" by Acronis, Inc. Each card includes a large letter "A", a brief description ("The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available"), and a "Get it now" button.
- Row 4:** Three instances of "Acronis Backup" by Acronis, Inc. Each card includes a large letter "A", a brief description ("The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available"), and a "Get it now" button.

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 this upgrade, a recovery point is created as soon as the snapshot is finished and this recovery point of snapshot type can be used to perform a restore using the same restore flow. You can identify this recovery point in the Azure portal by using "snapshot" as the recovery point type, and after the snapshot is transferred to the vault, the recovery point type changes to "snapshot and vault".

Capabilities and considerations

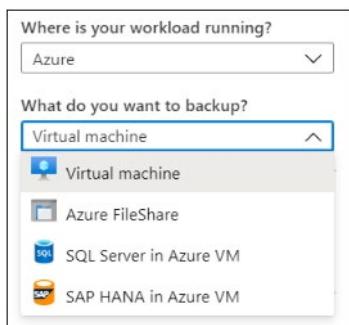
- Ability to use snapshots taken as part of a backup job that is available for recovery without waiting for data transfer to the vault to finish.
- Reduces backup and restore times by retaining snapshots locally, for two days by default. This default snapshot retention value is configurable to any value 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.
- ✓ By default, snapshots are retained for two days. This feature allows restore operation from these snapshots there by cutting down the restore times. It reduces the time that is required to transform and copy data back from the vault.

For more information, [Get improved backup and restore performance with Azure Backup Instant Restore capability²](#)

Recovery Services Vault VM Backup Options

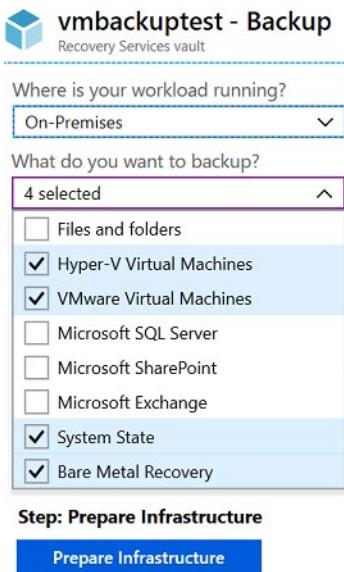
Recovery Services vault is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services such as IaaS VMs (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.



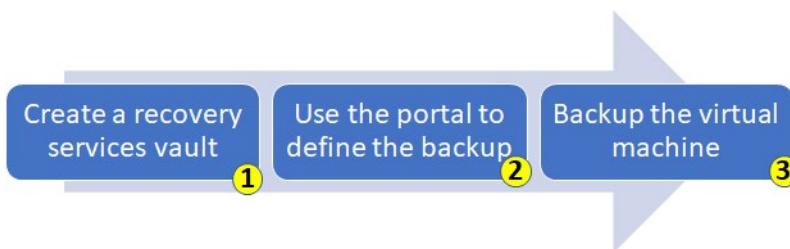
² <https://docs.microsoft.com/en-us/azure/backup/backup-instant-restore-capability>

- The Recovery Services vault can be used to backup on-premises virtual machines including: Hyper-V, VmWare, System State, and Bare Metal Recovery.



Implementing VM Backups

Backing up Azure virtual machines using Azure Backup is easy and follows a simple process.



- 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.
- 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.
- 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.

For more information, [Plan your VM backup infrastructure in Azure³](#).

Implementing VM Restore

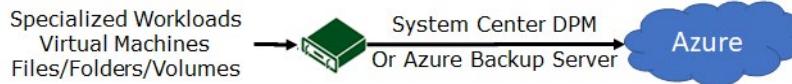
Once your virtual machine snapshots are safely in the recovery services vault it is easy to recover them.

The screenshot shows the Azure Backup service interface for a backup item named "ContosoWebFE1". The top navigation bar includes links for "Backup now", "Restore VM", "File Recovery", "Stop backup", and "Resume backup". Below this, there are sections for "Alerts and Jobs" and "Backup status". Under "Alerts and Jobs", there are links to "View all Alerts (last 24 hours)" and "View all Jobs (last 24 hours)". Under "Backup status", it shows "Backup Pre-Check" as "Passed" and "Last backup status" as "Success 3/12/2020, 12:20:38 AM". A section titled "Restore points (30)" displays three categories: "CRASH CONSISTENT" (30), "APPLICATION CONSISTENT" (0), and "FILE-SYSTEM CONSISTENT" (0). It includes a sorting option for "Time" and "Consistency". Two restore points are listed: "3/12/2020, 12:20:42 AM" and "3/11/2020, 12:20:59 AM", both labeled as "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.

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 such as SQL Server, Exchange, and SharePoint, in addition to file/folder/volume backups, and machine state backups (bare-metal, 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.

³ <https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction>

- You can manage backups for multiple machines that you gather into protection groups in a single console. This is particularly useful when apps are tiered over multiple machines and you want to back them up together.

Backup steps

1. Install the DPM or MABS protection agent on machines you want to protect. You then add the machines to a DPM protection group.
2. To protect on-premises machines, the DPM or MABS server must be located on-premises.
3. To protect Azure VMs, the MABS server must be located in Azure, running as an Azure VM.
4. 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.
5. 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.
6. The disk of the protected workload is backed up to the local MABS/DPM disks, according to the schedule you specified.
7. The DPM/MABS disks are backed up to the vault by the MARS agent that's running on the DPM/MABS server.

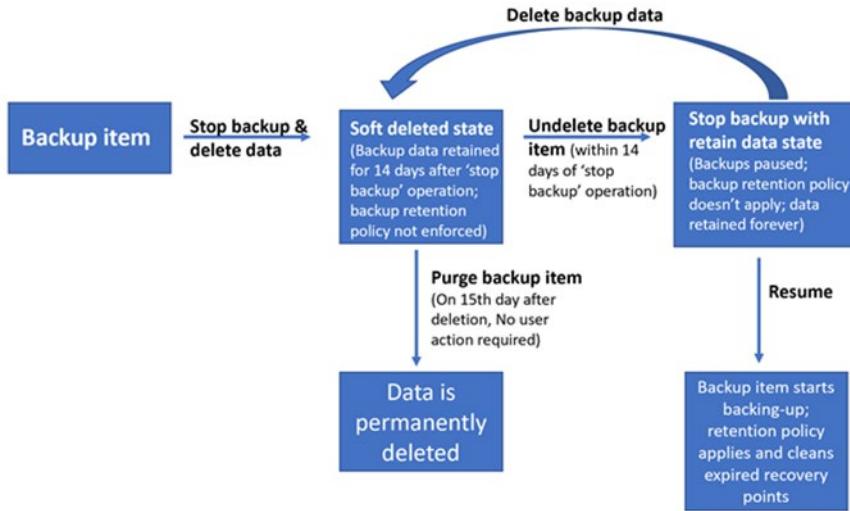
Backup Component Comparison

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
Azure Backup Server	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

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.



How soft delete works

When enabled, soft delete enables you to save and recover your data when blobs or blob snapshots are deleted. This protection extends to blob data that is erased as the result of an overwrite.

When data is deleted, it transitions to a soft deleted state instead of being permanently erased. When soft delete is on and you overwrite data, a soft deleted snapshot is generated to save the state of the overwritten data. Soft deleted objects are invisible unless explicitly listed. You can configure the amount of time soft deleted data is recoverable before it is permanently expired.

Configuration settings

When you create a new account, soft delete is off by default. Soft delete is also off by default for existing storage accounts. You can toggle the feature on and off at any time during the life of a storage account.

You will still be able to access and recover soft deleted data when the feature is turned off, assuming that soft deleted data was saved when the feature was previously turned on. When you turn on soft delete, you also need to configure the retention period.

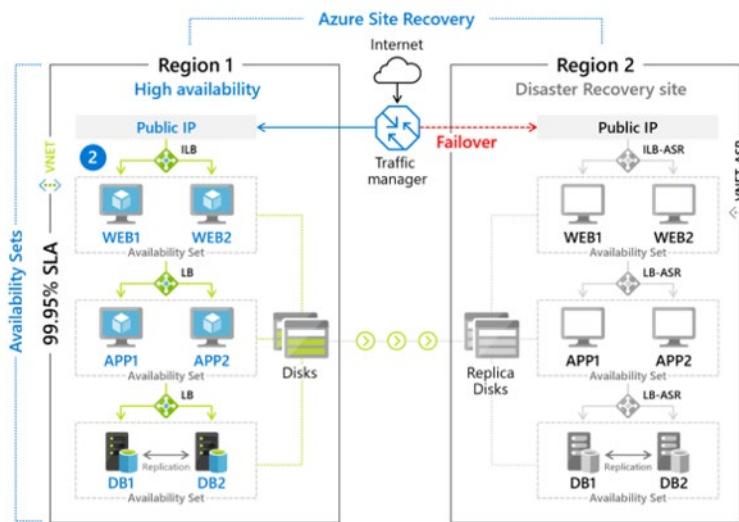
The retention period indicates the amount of time that soft deleted data is stored and available for recovery. For blobs and blob snapshots that are explicitly deleted, the retention period clock starts when the data is deleted. For soft deleted snapshots generated by the soft delete feature when data is overwritten, the clock starts when the snapshot is generated. Currently you can retain soft deleted data for between 1 and 365 days.

You can change the soft delete retention period at any time. An updated retention period will only apply to newly deleted data. Previously deleted data will expire based on the retention period that was configured when that data was deleted. Attempting to delete a soft deleted object will not affect its expiry time.

- ✓ Soft delete is backwards compatible, so you don't have to make any changes to your applications to take advantage of the protections this feature affords.

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.

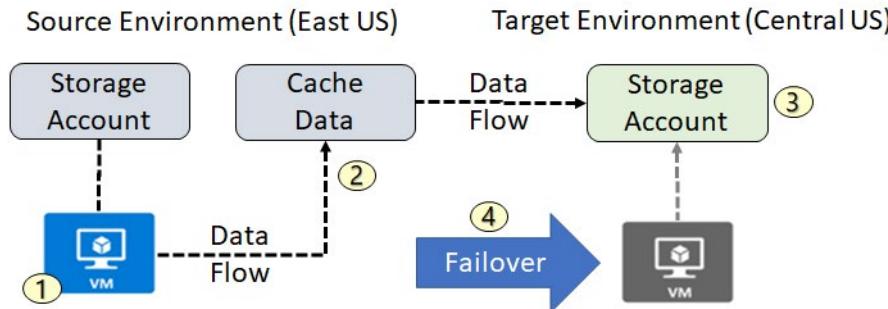
Features

- 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.
- ✓ Are you considering using Azure Site Recovery and are you interested in any of these specific features? Which one is most important to you?

For more information, [Azure Site Recovery documentation⁴](#).

Azure to Azure Architecture



When you enable replication for an Azure VM, the following happens:

1. The Site Recovery Mobility service extension is automatically installed on the VM. The extension registers the VM with Site Recovery. Continuous replication begins for the VM. Disk writes are immediately transferred to the cache storage account in the source location.
2. Site Recovery processes the data in the cache, and sends it to the target storage account, or to the replica managed disks.
3. After the data is processed, crash-consistent recovery points are generated every five minutes. App-consistent recovery points are generated according to the setting specified in the replication policy.
4. When you initiate a failover, the VMs are created in the target resource group, target virtual network, target subnet, and in the target availability set. During a failover, you can use any recovery point.

⁴ <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview>

Module 10 Lab and Review Questions

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

Module 10 Review Questions

Review Question 1

You need to backup files and folders to Azure. Which three steps must you perform?

- Download, install and register the backup agent.
- Synchronize configuration.
- Back up files and folders.
- Create a backup services vault.
- Create a recovery services vault.

Review Question 2

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 Site Recovery
- Azure Backup Server

Review Question 3

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.
- Azure Migrate.

Review Question 4

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.

- Define recovery points.
- Create a Recovery Services vault.
- Create a Backup policy.
- Install the Azure VM Agent.

Review Question 5

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 a database used for development on a data disk? Select one.

- Virtual machine backup
- Azure Site Recovery
- Disk image backup
- Disk snapshot

Review Question 6

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
- Azure Site Recovery
- Disk image backup
- Disk snapshot

Review Question 7

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 (MARS) agent
- Azure Backup Server
- Enable disk snapshots
- Enable backup for individual Azure VMs

Review Question 8

You plan to use virtual machine soft delete. Which of the following statements are true? Select two.

- Soft delete provides 20 days extended retention of data.
- If you delete a backup, soft delete still provides recovery of data.
- Soft delete is built-in protection at no additional cost.
- Soft delete items are stored in archive storage.
- A recovery service vault can be deleted if it only has soft-deleted backup items.

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Protect your virtual machines by using Azure Backup⁵**
- **Back up and restore your Azure SQL database⁶**
- **Protect your Azure infrastructure with Azure Site Recovery⁷**
- **Protect your on-premises infrastructure from disasters with Azure Site Recovery⁸**

⁵ <https://docs.microsoft.com/en-us/learn/modules/protect-virtual-machines-with-azure-backup/>

⁶ <https://docs.microsoft.com/en-us/learn/modules/backup-restore-azure-sql/>

⁷ <https://docs.microsoft.com/en-us/learn/modules/protect-infrastructure-with-site-recovery/>

⁸ <https://docs.microsoft.com/en-us/learn/modules/protect-on-premises-infrastructure-with-azure-site-recovery/>

Answers

Review Question 1

You need to backup files and folders to Azure. Which three steps must you perform?

- Download, install and register the backup agent.
- Synchronize configuration.
- Back up files and folders.
- Create a backup services vault.
- Create a recovery services vault.

Explanation

Review Question 2

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 Site Recovery
- Azure Backup Server

Explanation

Azure Backup Server provides a bare metal backup capability.

Review Question 3

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.
- Azure Migrate.

Explanation

For backing up Azure virtual machines running production workloads, use Azure Backup. Azure Backup supports application-consistent backups for both Windows and Linux virtual machines. Azure Site Recovery coordinates virtual-machine and physical-server replication, failover, and fallback, but Azure Backup will protect and restore data at a more granular level. Managed snapshots provide a read-only full copy of a managed disk, and is an ideal solution in development and test environments, but Azure Backup is the better option for your production workloads.

Review Question 4

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.

- Define recovery points.
- Create a Recovery Services vault.
- Create a Backup policy.
- Install the Azure VM Agent.

Explanation

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.

Review Question 5

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 a database used for development on a data disk? Select one.

- Virtual machine backup
- Azure Site Recovery
- Disk image backup
- Disk snapshot

Explanation

You can use snapshots to quickly restore the database data disks.

Review Question 6

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
- Azure Site Recovery
- 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.

Review Question 7

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 (MARS) agent
- 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.

Review Question 8

You plan to use virtual machine soft delete. Which of the following statements are true? Select two.

- Soft delete provides 20 days extended retention of data.
- If you delete a backup, soft delete still provides recovery of data.
- Soft delete is built-in protection at no additional cost.
- Soft delete items are stored in archive storage.
- A recovery service vault can be deleted if it only has soft-deleted backup items.

Explanation

If you delete a backup, soft delete still provides recovery of data. Soft delete is built-in protection at no additional cost.

Module 11 Monitoring

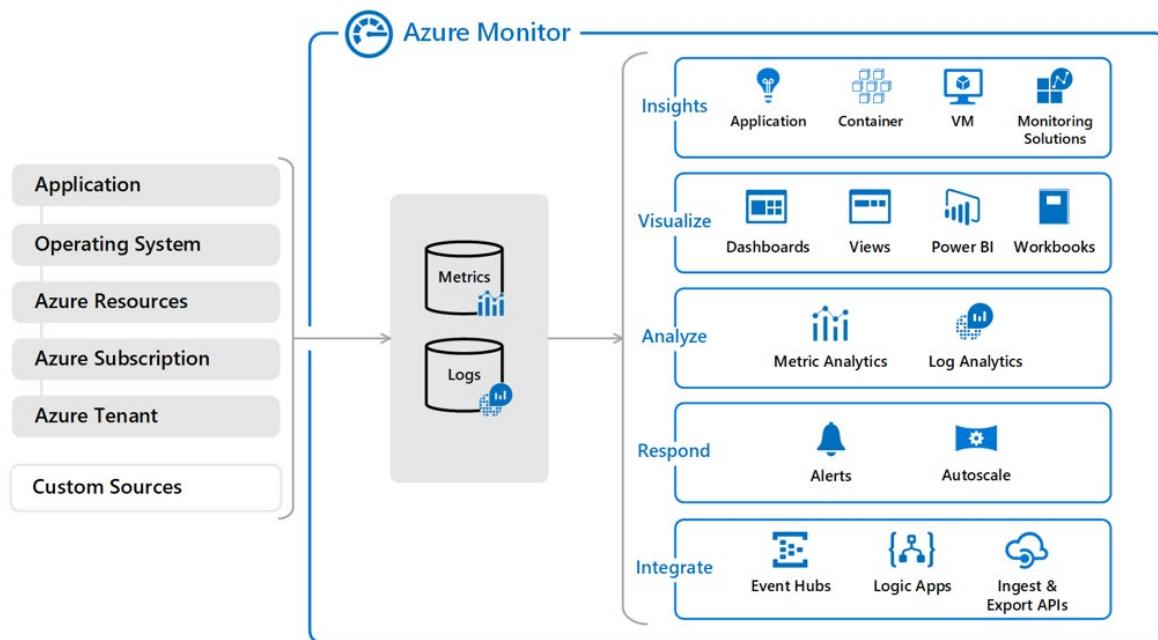
Azure Monitor

Azure Monitor Service

Monitoring is the act of collecting and analyzing data 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. It also helps you increase your uptime by proactively notifying you of critical issues so that you can resolve them before they become problems.

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 telemetry from your application and the Azure resources that support them. They can 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, which are the two fundamental types of data use by Azure Monitor. On the left are the sources of monitoring data that populate these data stores. On the right are the different functions that Azure Monitor performs with this collected data such as analysis, alerting, and streaming to external systems.



For more information, [Azure Monitor Documentation¹](#)

Key Capabilities

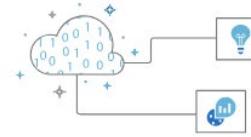
- **Monitor and visualize metrics.** Metrics are numerical values available from Azure resources helping you understand the health, operation and performance of your system.
- **Query and analyze logs.** Logs are activity logs, diagnostic logs, and telemetry from monitoring solutions; analytics queries 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.



Monitor & Visualize Metrics

Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

[Explore Metrics](#)



Query & Analyze Logs

Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

[Search Logs](#)



Setup Alert & Actions

Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

[Create Alert](#)

¹ <https://docs.microsoft.com/en-us/azure/azure-monitor/>

Monitoring Data Platform

All data collected by Azure Monitor fits into one of two fundamental types, **metrics and logs²**.

- **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. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis.

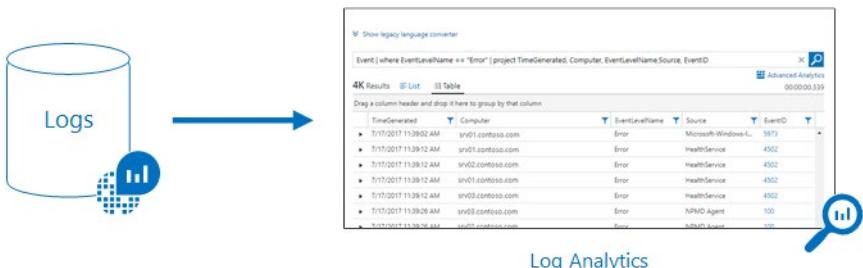
For many Azure resources, the data collected by Azure Monitor is displayed on the Overview page in the Azure portal. For example, virtual machines have several charts displaying performance metrics. Click on any of the graphs to open the data in Metric explorer in the Azure portal, which allows you to 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.



Log Data

Log data collected by Azure Monitor is stored in Log Analytics which includes a **rich query language³** to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using the Log Analytics page in the Azure portal and then either directly analyze the data using these tools or save queries for use with visualizations or alert rules.

Azure Monitor uses a version of the **Data Explorer⁴** 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.



² <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-collection>
³ <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview>
⁴ [https://docs.microsoft.com/en-us/azure/kusto/query/](https://docs.microsoft.com/en-us/azure/kusto/query)

Data Types

Azure Monitor can collect data from a variety of 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. This 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.

As soon as you create an Azure subscription and start adding resources such as virtual machines and web apps, Azure Monitor starts collecting data. Activity Logs record when resources are created or modified. Metrics tell you how the resource is performing and the resources that it's consuming.

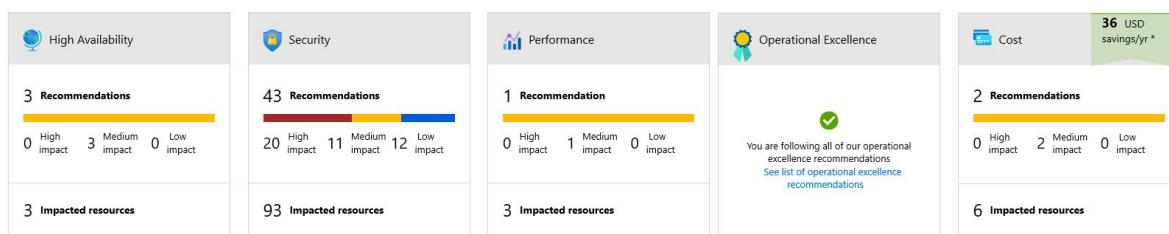
Extend the data you're collecting into the actual operation of the resources by enabling diagnostics and adding an agent to compute resources. This will collect telemetry for the internal operation of the resource and allow you to configure different data sources to collect logs and metrics from Windows and Linux guest operating systems.

- ✓ Azure Monitor can collect log data from any REST client using the Data Collector API. This allows you to create custom monitoring scenarios and extend monitoring to resources that don't expose telemetry through other sources.

Azure Advisor

Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.

The Advisor cost recommendations page helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources.



Select the recommended action for a recommendation to implement the recommendation. A simple interface will open that enables you to implement the recommendation or refer you to documentation that assists you with implementation.

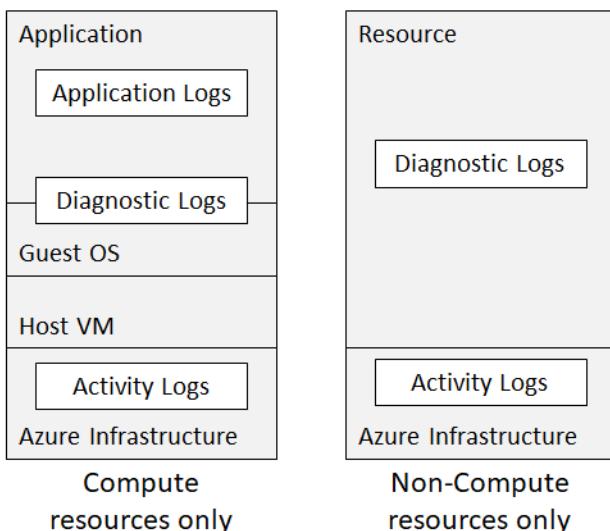
- ✓ Advisor provides recommendations for virtual machines, availability sets, application gateways, App Services, SQL servers, and Redis Cache.

Activity Log

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.



- ✓ 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

Activity log

In the Azure portal, you can filter your Activity Log by these fields:

- **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.

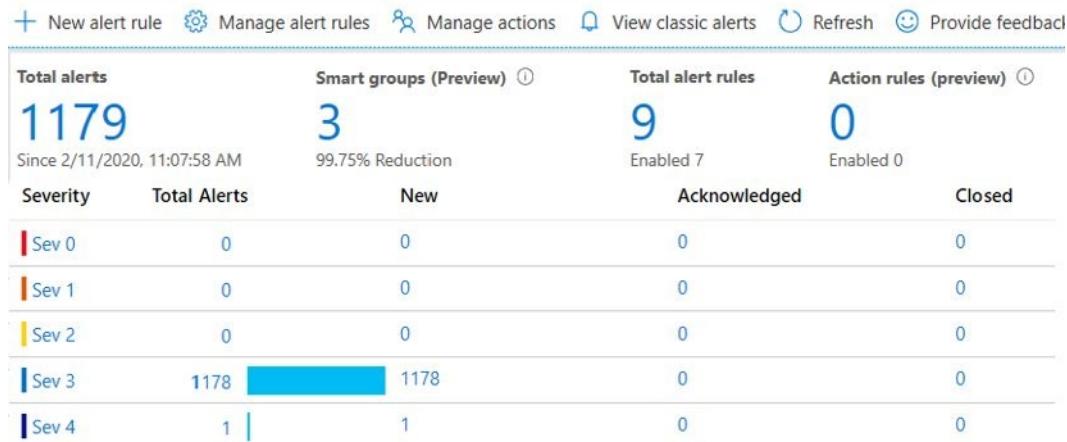
Event categories

- **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 Security Center. 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.
- ✓ 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.

Azure Alerts

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
New	The issue has just been detected and has not yet been reviewed.
Acknowledged	An administrator has reviewed the alert and started working on it.
Closed	The issue has been resolved. After an alert has been closed, you can reopen it by changing it to another state.

✓ 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.

For more information, [The new alerts experience in Azure Monitor⁵](#)

Creating 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 consists of alert rules, action groups, and monitor conditions.

Create rule
Rules management

*** RESOURCE**
Select the target(s) that you wish to monitor

*** CONDITION**
No condition defined, click on 'Add condition' to select a signal and define its logic

ACTION GROUPS
Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. Learn more [here](#)

ACTION GROUP NAME	ACTION GROUP TYPE
No action group selected	
<input type="button" value="Select existing"/>	<input type="button" value="Create New"/>

⁵ <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-unified-alerts>

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. Tje Action Groups topic is coming up.

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.

When an action is configured to notify a person by email or SMS the person will receive a confirmation indicating they have been added to the action group.

Action group name * ⓘ
Sample action group

Short name * ⓘ
SampleAG

Subscription * ⓘ
Visual Studio Enterprise

Resource group * ⓘ
Default-ActivityLogAlerts (to be created)

Actions

Action name *	Action Type *
Unique name for the action	Select an action type ^
	<ul style="list-style-type: none"> Automation Runbook Azure Function Email Azure Resource Manager Role Email/SMS/Push/Voice ITSM LogicApp 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.
 - **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/Push/Voice** - Specify any email, SMS, push, or voice actions.
 - **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 HTTP endpoint that allows external applications to communicate with your system.
- ✓ Always check the documentation for the number of actions you can create.

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.

Log Analytics

Log Analytics

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 helps you to fully leverage the value of 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 fully leverage 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.

The screenshot shows the Azure Monitor - Logs interface. On the left, there's a navigation sidebar with links for Overview, Activity log, Alerts, Metrics, and Logs (which is highlighted with a red box). Below that are sections for Insights (Applications, Virtual Machines (preview), Containers, Network) and More. The main area is titled 'New Query 1' and shows a tree view of log sources under 'Active'. One node, 'contosoretail-IT', is expanded, showing its children: 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.

Connected Sources

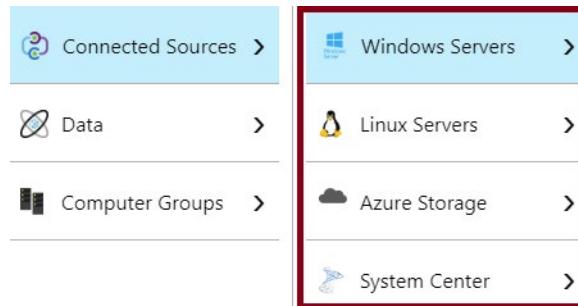
Connected Sources are the computers and other resources that generate data collected by Log Analytics. This can include agents installed on **Windows⁶** and **Linux⁷** computers that connect directly or agents in connected **System Center Operations Manager management group⁸**. Log Analytics can also collect data from **Azure storage⁹**.

⁶ <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents>

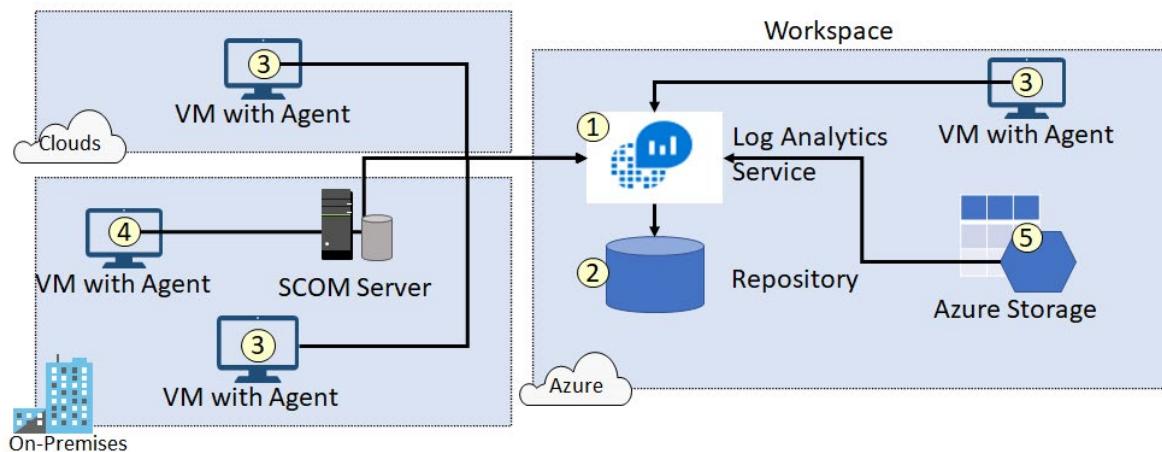
⁷ <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-linux-agents>

⁸ <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-om-agents>

⁹ <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-storage>



The following diagram shows how Connected Sources flow data to the Log Analytics service.

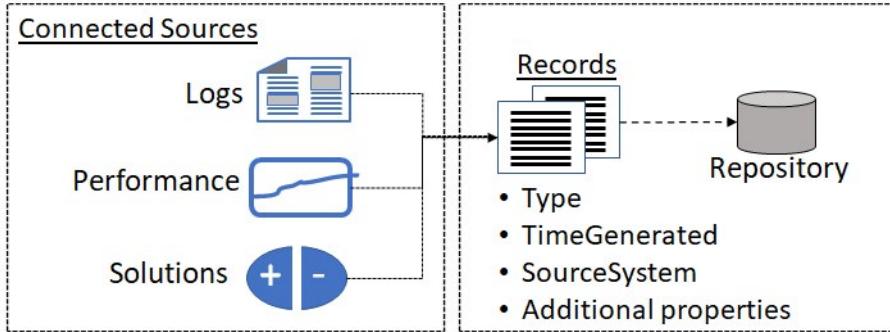


Ensure you can locate each of the following.

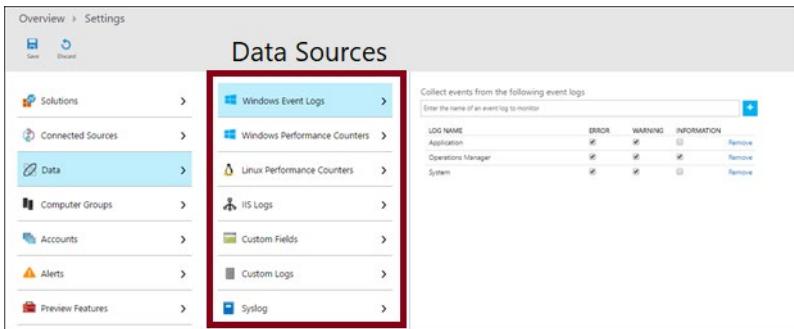
- The Log Analytics service (1) collects data and stores it in the repository (2). The repository is hosted in Azure. Connected Sources provide information to the Log Analytics service.
- Computer agents (3) generate data to the Log Analytics service. These agents can run on Windows or Linux computers, 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 which 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.

Data Sources

Data sources are the different kinds of data collected from each connected source. These can include events and performance data from Windows and Linux agents, in addition to sources such as IIS logs and custom text logs. You configure each data source that you want to collect, and the configuration is automatically delivered to each connected source.



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.



Log Analytics Querying

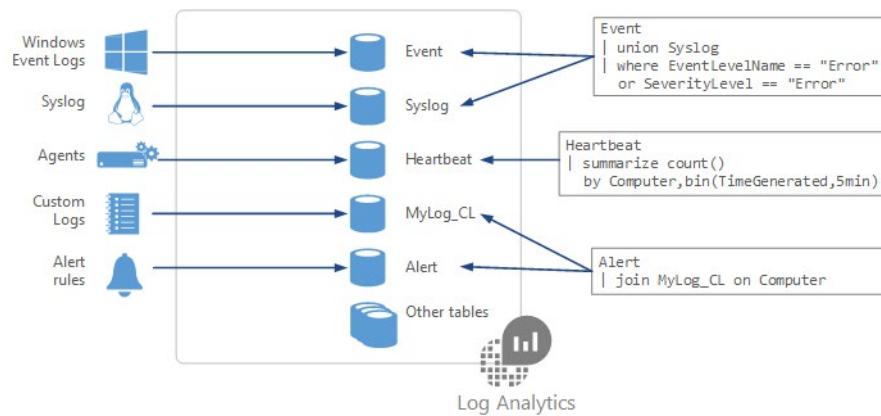
Log Analytics provides a query syntax to quickly retrieve and consolidate data in the repository. You can create and save Log Searches to directly analyze data in the portal or have log searches run automatically to create an alert if the results of the query indicate an important condition.



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 leverage the Log Search API to build custom solutions that leverage Log Analytics data or to integrate with other systems.

Query Language Syntax

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 ErrorCount = count() by Computer
| top 10 by ErrorCount 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 queries¹⁰](#)

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 Demonstration¹¹](#) 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**.

¹⁰ <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/query-language>

¹¹ <https://portal.loganalytics.io/demo>

- ✓ Is there a particular query you are interested in?

Network Watcher

Network Watcher

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 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.

Connection monitor

Connection monitor is a feature of Network Watcher that can monitor communication between a virtual machine and an endpoint. The connection monitor capability monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint.

For example, you might have a web server VM that communicates with a database server VM. Someone in your organization may, unknown to you, apply a custom route or network security rule to the web server or database server VM or subnet.

If an endpoint becomes unreachable, connection troubleshoot informs you of the reason. Potential reasons might be DNS name resolution problem, the CPU, memory, or firewall within the operating system of a VM, or the hop type of a custom route, or security rule for the VM or subnet of the outbound connection. Connection monitor also provides the minimum, average, and maximum latency observed over time.

Network performance monitor

Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute. Network performance monitor detects network issues like traffic blackholing, routing errors, and issues that conventional network monitoring methods aren't able to detect. The solution generates alerts and notifies you when a threshold is breached for a network link. It also ensures timely detection of network performance issues and localizes the source of the problem to a particular network segment or device.

- ✓ To use Network Watcher capabilities, the account you log into Azure with, must be assigned to the Owner, Contributor, or Network contributor built-in roles, or assigned to a custom role. A custom role can be given permissions to read, write, and delete the Network Watcher.

For more information, **Network Watcher**¹²

¹² <https://azure.microsoft.com/en-us/services/network-watcher/>

Network Watcher Diagnostics

Network Watcher	
Monitoring	Network diagnostic tools
Topology	IP flow verify
Connection monitor	Next hop
Network Performance Monitor	Effective security rules
Logs	VPN troubleshoot
NSG flow logs	Packet capture
Diagnostic logs	Connection troubleshoot
Traffic Analytics	

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.

Diagnostics - IP Flow Verify

Verify IP Flow Purpose: 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.

Example

When you deploy a VM, Azure applies several default security rules to the VM that 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 tells you which security rule allowed or denied the communication, so that you can resolve the problem.

- ✓ 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.

Diagnostics - Next Hop

Next Hop Purpose: 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.

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 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.

Diagnostics - Effective Security Rules

If you have several NSGs and are not sure which security rules are being applied, you can examine the Effective security rules.

nsg01												
Inbound rules												
Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access ↑↓
RDP_Inbound		100		13.23.34.45/32	0-65535		0.0.0.0/0	3389-3389		TCP		Allow
AllowVnetInBound		65000		Virtual network (1 prefixes)	0-65535		Virtual network (1 prefixes)	0-65535		All		Allow
AllowAzureLoadBalancerInBound		65001		Azure load balancer (2 prefixes)	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		Allow
DenyAllInBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		Deny
Outbound rules												
Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access ↑↓
AllowVnetOutBound		65000		Virtual network (1 prefixes)	0-65535		Virtual network (1 prefixes)	0-65535		All		Allow
AllowInternetOutBound		65001		0.0.0.0/0,0.0.0.0/0	0-65535		Internet (216 prefixes)	0-65535		All		Allow
DenyAllOutBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		Deny

- **Priority.** A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

- **Source.** Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group. Specifying a range, a service tag, or application security group, enables you to create fewer security rules.
- **Protocol.** TCP, UDP, ICMP or Any.
- **Action.** Allow or deny.

Diagnostics - VPN Troubleshoot

VPN Troubleshoot Purpose: Troubleshoot gateways and connections.

Example

Virtual Network Gateways provide connectivity between on-premises resources and other virtual networks within Azure. Monitoring gateways and their connections are critical to ensuring communication is working as expected. VPN diagnostics can troubleshoot the health of the gateway, or connection, and provide detailed logging. The request is a long running transaction and results are returned once the diagnosis is complete.

Name	Troubleshooting s...	Resource status	Resource Group	Location
vng01	Running	Succeeded	Demo	East US
cn01	-	Succeeded	Demo	East US

VPN Troubleshoot 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.

- ✓ You can select multiple gateways or connections to troubleshoot simultaneously or you can focus on an individual component.

Diagnostics - Packet Capture

Add packet capture

Subscription *

MSDN Platforms Subscription

Resource group *

Demo

Target virtual machine *

vm01

Packet capture name *

capture01

Capture configuration

The packet capture output file (.cap) can be stored in a storage account and/or on the target VM.

Storage account File Both

Storage accounts *

samcteusvmdiagnostic

Maximum bytes per packet ⓘ

default: 0 (entire packet)

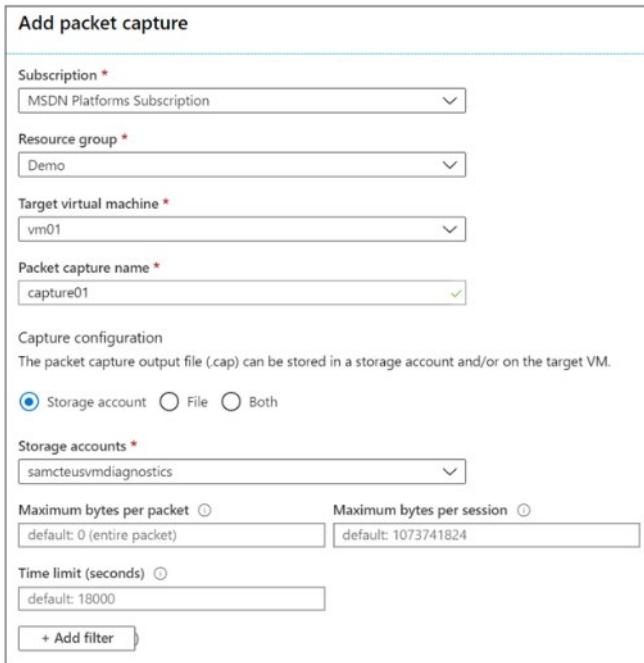
Maximum bytes per session ⓘ

default: 1073741824

Time limit (seconds) ⓘ

default: 18000

+ Add filter



Network Watcher packet capture allows you to create capture sessions to track traffic to and from a virtual machine. Filters are provided for the capture session to ensure you capture only the traffic you want. Packet capture helps to diagnose network anomalies, both reactively, and proactively. Other uses include gathering network statistics, gaining information on network intrusions, to debug client-server communication, and much more. Being able to remotely trigger packet captures, eases the burden of running a packet capture manually on a desired virtual machine, which saves valuable time.

Diagnostics - Connection Troubleshoot

The connection troubleshoot feature of Network Watcher provides the capability to check a direct TCP connection from a virtual machine to a virtual machine (VM), fully qualified domain name (FQDN), URI, or IPv4 address. Network scenarios are complex, they are implemented using network security groups, firewalls, user-defined routes, and resources provided by Azure. Complex configurations make troubleshooting connectivity issues challenging. Network Watcher helps reduce the amount of time to find and detect connectivity issues. The results returned can provide insights into whether a connectivity issue is due to a platform or a user configuration issue.

The screenshot shows the 'Create probe' dialog in the Network Watcher portal. The 'Source' section includes 'Subscription' (MSDN Platforms Subscription), 'Resource group' (Demo), 'Source type' (Virtual machine), and 'Destination' (URI: FQDN or IPv4: 13.24.35.46). The 'Probe Settings' section includes 'Protocol' (TCP selected), 'Destination port' (3389), and 'Source port' (3389). A 'Check' button is at the bottom.

Further examples of different supported network troubleshooting scenarios include:

- Checking the connectivity and latency to a remote endpoint, such as for websites and storage endpoints.
- Connectivity between an Azure VM and an Azure resource like Azure SQL server, where all Azure traffic is tunneled through an on-premises network.
- Connectivity between VMs in different VNets connected using VNet peering.

Logs - NSG Flow Logs

NSG flow logs allows you to view information about ingress and egress IP traffic through an NSG. Flow logs are written in JSON format and show outbound and inbound flows on a per rule basis. The JSON format can be visually displayed in Power BI or third-party tools like Kibana.

Metrics	Name	Resource type	Resource group	Status	Location
Usage + quotas	nsg01	Network security gro...	Demo	Enabled	East US
Logs	nsg02	Network security gro...	Demo	Enabled	East US
NSG flow logs	nsg03	Network security gro...	Demo	Enabled	East US
Diagnostic logs					

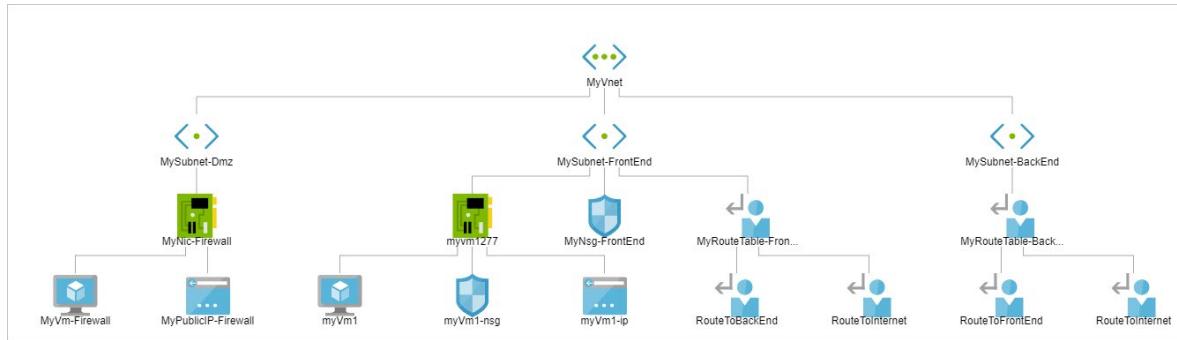
- ✓ This feature now supports (January 2020) firewalled storage accounts and service endpoints for storage.

Monitoring - 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 infrastruc-

ture. 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.

- ✓ To generate the topology, you need a Network Watcher instance in the same region as the virtual network.

Module 11 Lab and Review Questions

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

Module 11 Review Questions

Review Question 1

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
- MyLog_CL
- Alert

Review Question 2

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
- Signal Type
- Action Group

Review Question 3

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.

- Event
- SysLog
- Heartbeat
- MyLog_CL
- Alert

Review Question 4

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 Auditing
- Network Watcher Connection Troubleshoot
- Network Watcher Flows
- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology

Review Question 5

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.

- Configure IIS logging and review the connection errors.
- Turn on virtual machine diagnostic logging and use Log Analytics.
- Use Network Watcher's VPN Diagnostics feature.
- Use Network Watcher's IP Flow Verify feature.
- Configure Windows performance counters and use Performance Monitor.

Review Question 6

You are interested in finding a single tool to help identify high VM CPU utilization, DNS resolution failures, firewall rules that are blocking traffic, and misconfigured routes. Which tool can you use? Select one.

- Network Watcher Auditing
- Network Watcher Connection Troubleshoot
- Network Watcher Flows
- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology

Review Question 7

You are reviewing the Alerts page and notice an alert has been Acknowledged. What does this mean? Select one.

- The issue has just been detected and has not yet been reviewed.
- An administrator has reviewed the alert and started working on it.
- The issue has been resolved.
- The issue has been closed.

Review Question 8

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
- Alert
- Recommendation
- Policy

Additional Study

Microsoft Learn provides self paced skills training on a variety of topics. These Learn modules cover the content you have just learned. You can search for additional modules by product, role, or level.

- **Analyze your Azure infrastructure by using Azure Monitor logs¹³**
- **Improve incident response with alerting on Azure¹⁴**
- **Monitor the health of your Azure virtual machine by collecting and analyzing diagnostic data¹⁵**
- **Monitor, diagnose, and troubleshoot your Azure storage¹⁶**

¹³ <https://docs.microsoft.com/en-us/learn/modules/analyze-infrastructure-with-azure-monitor-logs/>

¹⁴ <https://docs.microsoft.com/en-us/learn/modules/incident-response-with-alerting-on-azure/>

¹⁵ <https://docs.microsoft.com/en-us/learn/modules/monitor-azure-vm-using-diagnostic-data/>

¹⁶ <https://docs.microsoft.com/en-us/learn/modules/monitor-diagnose-and-troubleshoot-azure-storage/>

Answers

Review Question 1

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
- MyLog_CL
- Alert

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.

Review Question 2

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
- Signal Type
- Action Group

Explanation

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.

Review Question 3

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.

- Event
- SysLog
- Heartbeat
- MyLog_CL
- Alert

Explanation

Syslog is an event logging protocol that is common to Linux. Syslog includes information such as error messages.

Review Question 4

You are analyzing the company virtual network and think it would helpful to get a visual representation of the networking elements. Which feature can you use? Select one.

- Network Watcher Auditing
- Network Watcher Connection Troubleshoot
- Network Watcher Flows
- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology

Explanation

Network Watcher's Topology feature provides a visual representation of your networking elements.

Review Question 5

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.

- Configure IIS logging and review the connection errors.
- Turn on virtual machine diagnostic logging and use Log Analytics.
- Use Network Watcher's VPN Diagnostics feature.
- Use Network Watcher's IP Flow Verify feature.
- Configure Windows performance counters and use Performance Monitor.

Explanation

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.

Review Question 6

You are interested in finding a single tool to help identify high VM CPU utilization, DNS resolution failures, firewall rules that are blocking traffic, and misconfigured routes. Which tool can you use? Select one.

- Network Watcher Auditing
- Network Watcher Connection Troubleshoot
- Network Watcher Flows
- Network Watcher Next Hop
- Network Watcher Views
- Network Watcher Topology

Explanation

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.

Review Question 7

You are reviewing the Alerts page and notice an alert has been Acknowledged. What does this mean? Select one.

- The issue has just been detected and has not yet been reviewed.
- An administrator has reviewed the alert and started working on it.
- The issue has been resolved.
- The issue has been closed.

Explanation

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.

Review Question 8

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
- Alert
- Recommendation
- 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.