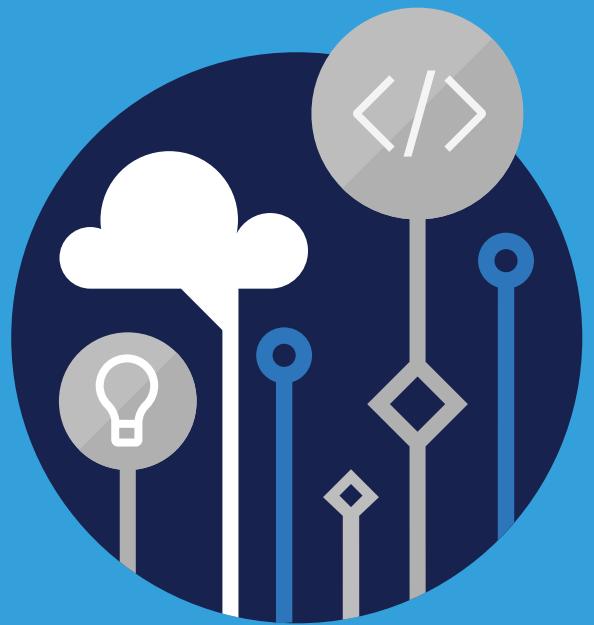


Microsoft
Official
Course



AZ-103T00

Microsoft Azure
Administrator

AZ-103T00
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> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

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.

- a) "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.
- b) "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.
- c) "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
- d) "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 a MPN Member, or (iii) a Microsoft full-time employee.
- e) "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
- f) "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.
- g) "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.
- h) "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.
- i) "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
- j) "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.
- k) "MPN Member" means an active Microsoft Partner Network program member in good standing.
- l) "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.

- m) "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.
- n) "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.
- o) "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.

a) **If you are a Microsoft IT Academy Program Member:**

- i) 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.
- ii) 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:

- iii) you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv) 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,
- v) 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,
- vi) 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,

- vii) 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,
- viii) you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
- ix) you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

b) **If you are a Microsoft Learning Competency Member:**

- i) 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.
- ii) 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:

- iii) you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv) you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
- v) 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,
- vi) 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,
- vii) 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,
- viii) you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
- ix) you will only provide access to the Trainer Content to MCTs.

c) **If you are a MPN Member:**

- i) 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.
- ii) 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:

- iii) you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
- iv) you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
- v) 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,
- vi) you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,
- vii) 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,
- viii) 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,
- ix) you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
- x) you will only provide access to the Trainer Content to Trainers.

d) **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.

e) **If you are a Trainer.**

- i) 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.
- ii) 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:
 - a) **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.
 - b) **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.

- c) **Pre-release Term.** If you are an 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.

- a) 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.
- b) 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 contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES.

Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 \$ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

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

Elle s'applique également, même si Microsoft connaît 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 Welcome	1
	Start Here	1
■	Module 1 Azure Administration	7
	Azure Portal and Cloud Shell	7
	Azure PowerShell and CLI	12
	Resource Manager	18
	ARM Templates	24
■	Module 2 Azure Virtual Machines	33
	Virtual Machine Planning	33
	Creating Virtual Machines	41
	Virtual Machine Availability	52
	Virtual Machine Extensions	58
	Lab and Review Questions	62
■	Module 3 Azure Storage	71
	Storage Accounts	71
	Blob Storage	81
	Azure Files	87
	Storage Security	95
	Lab and Review Questions	104
■	Module 4 Virtual Networking	115
	Virtual Networks	115
	IP Addressing and Endpoints	123
	Azure DNS	129
	Network Security Groups	137
	Lab and Review Questions	141
■	Module 5 Intersite Connectivity	153
	VNet Peering	153
	VNet-to-VNet Connections	159
	ExpressRoute Connections	168
	Lab and Review Questions	173
■	Module 6 Monitoring	183
	Azure Monitor	183

Azure Alerts	190
Log Analytics	197
Network Watcher	204
Lab and Review Questions	211
Module 7 Data Protection	219
Data Replication	219
File and Folder Backups	224
Virtual Machine Backups	232
Lab and Review Questions	241
Module 8 Network Traffic Management	247
Network Routing	247
Azure Load Balancer	252
Azure Traffic Manager	259
Lab and Review Questions	266
Module 9 Azure Active Directory	273
Azure Active Directory	273
Azure Active Directory Connect	278
Azure AD Join	284
Lab and Review Questions	287
Module 10 Securing Identities	293
Multi-Factor Authentication	293
Azure AD Identity Protection	301
Self-Service Password Reset	307
Lab and Review Questions	311
Module 11 Governance and Compliance	319
Subscriptions and Accounts	319
Role-based Access Control	327
Users and Groups	332
Azure Policy	339
Lab and Review Questions	344
Module 12 Data Services	353
Content Delivery Network	353
File Sync	358
Import and Export Service	363
Data Box	370
Lab and Review Questions	377

Module 0 Welcome

Start Here

About this Course

Course Description

This course teaches IT Professionals how to manage their Azure subscriptions, create and scale virtual machines, implement storage solutions, configure virtual networking, back up and share data, connect Azure and on-premises sites, manage network traffic, implement Azure Active Directory, secure identities, 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

- Administer Azure using the Azure portal, Cloud Shell, Azure PowerShell, CLI, and ARM templates.
- Plan for, create, and scale virtual machines.
- Implement Azure storage accounts, blob storage, Azure files, and shared access keys.
- Configure virtual networks including planning, IP addressing, Azure DNS, and network security groups.
- Configure data replication and backup files, folders, and virtual machines.
- Configure intersite connectivity solutions like VNet Peering, VNet-to-VNet connections, Site-to-Site connections, and ExpressRoute.
- Manage network traffic using service endpoints, network routing choices, Azure load balancer, Azure Traffic Manager, and Content Delivery Network.
- Manage subscriptions, accounts, users, groups, and billing. Implement Azure policies.
- Implement Azure Active Directory and Azure Active Directory Connect.
- Secure identities with MFA, Azure AD Identity Protection, AD Join, and Self-Service Password Reset.
- Share data using the Import and Export service, Data Box, and File Sync.
- Monitor 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 – Azure Administration

In this module, you'll learn about the tooling Azure Administrator uses to manage their infrastructure. This includes the Azure Portal, Cloud Shell, Azure PowerShell, CLI, Resource Manager, and Resource Manager Templates. The demonstrations in this module will ensure you are successful in the course labs. This module includes:

- Azure Portal and Cloud Shell
- Azure PowerShell and CLI
- Resource Manager
- ARM Templates

Module 02 – Azure Virtual Machines

In this module, you'll 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 - Deploy and Manage Virtual Machines
- Lab - Virtual Machines and Scale Sets

Module 03 – Azure Storage

In this module, you'll learn about basic storage features including storage accounts, blob storage, Azure files, and storage security. This module includes:

- Storage Accounts
- Blob storage
- Azure Files
- Storage Security
- Lab - Implement and Manage Storage

Module 04 – Virtual Networking

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

- Virtual Networks
- IP Addressing and Endpoints
- Azure DNS
- Network Security groups
- Lab - Configure Azure DNS

Module 05 – Intersite Connectivity

In this module, you'll learn about intersite connectivity features including VNet Peering, VNet-to-VNet connections, Site-to-Site Connections, and ExpressRoute. This module includes:

- VNet Peering
- VNet-to-VNet Connections
- ExpressRoute
- Lab - VNet Peering and Service Chaining

Module 06 – Monitoring

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

- Azure Monitor
- Azure Alerts
- Log Analytics
- Network Watcher
- Lab - Network Watcher

Module 07 – Data Protection

In this module, you'll learn about data replication strategies, backing up files and folders, and virtual machine backups. This module includes:

- Data Replication
- File and Folder Backups
- Virtual Machine Backups
- Lab - Azure Site Recovery Between Regions

Module 08 – Network Traffic Management

In this module, you'll learn about network traffic strategies including service endpoints, network routing, Azure Load Balancer, and Azure Traffic Manager. This module includes:

- Network Routing
- Azure Load Balancer
- Azure Traffic Manager
- Lab - Load Balancer and Traffic Manager

Module 09 – Azure Active Directory

In this module, you'll learn about Azure Active Directory (AD) including Azure AD Connect and Azure AD Join. This module includes:

- Azure Active Directory
- Azure AD Connect
- Azure AD Join
- Lab - Implement Directory Synchronization

Module 10 – Securing Identities

In this module, you'll learn how to secure identities including Multi-Factor Authentication, Azure AD Identity Protection, and Self-Service Password Reset. This module includes:

- Multi-Factor Authentication
- Azure AD Identity Protection
- Self-Service Password Reset
- Lab - Azure AD Identity Protection
- Lab - Self-Service Password Reset

Module 11 – Governance and Compliance

In this module, you'll learn about managing your subscriptions and accounts including role-based access control, users and groups, and Azure policy. This module includes:

- Subscriptions and Accounts
- Role-based Access Control (RBAC)
- Users and Groups
- Azure Policy
- Lab - Role-Based Access Control
- Lab - Governance and Compliance

Module 12 – Data Services

In this module, you'll learn how to effectively share data using Import and Export service, Data Box, Content Delivery Network, and File Sync. This module includes:

- Content Delivery Network
- File Sync
- Import and Export Service

- Data Box
- Lab - File Sync

AZ-103 Certification Exam

The AZ-103, **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-103 Study Areas	Weights
Manage Azure subscriptions and resources	15-20%
Implement and manage storage	15-20%
Deploy and manage virtual machines	15-20%
Configure and manage virtual networks	30-35%
Manage identities	15-20%

- ✓ Learn more about the **certification changes²** that took effect on May 1, 2019.

Resources

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

- **Azure forums³**. 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 Blog⁴**. Get the latest information about the certification tests and exam study groups.
- **Channel 9⁵**. Channel 9 provides a wealth of informational videos, shows, and events.
- **Azure Tuesdays with Corey⁶**. Corey Sanders answers your questions about Microsoft Azure - Virtual Machines, Web Sites, Mobile Services, Dev/Test etc.
- **Azure Fridays⁷**. 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 Blog⁸**. Keep current on what's happening in Azure, including what's now in preview, generally available, news & updates, and more.

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

² <https://www.microsoft.com/en-us/learning/community-blog-post.aspx?BlogId=8&Id=375217>

³ <https://social.msdn.microsoft.com/Forums/en-US/home?category=windowsazureplatform>

⁴ <https://www.microsoft.com/en-us/learning/community-blog.aspx>

⁵ <https://channel9.msdn.com/>

⁶ <https://channel9.msdn.com/Shows/Tuesdays-With-Corey/>

⁷ <https://channel9.msdn.com/Shows/Azure-Friday>

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

- **Azure Documentation⁹**. Stay informed on the latest products, tools, and features. Get information on pricing, partners, support, and solutions.

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

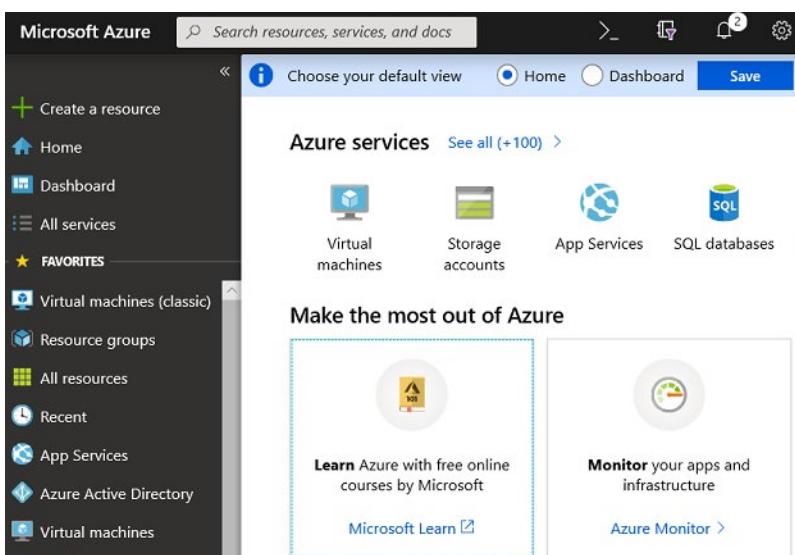
Module 1 Azure Administration

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.

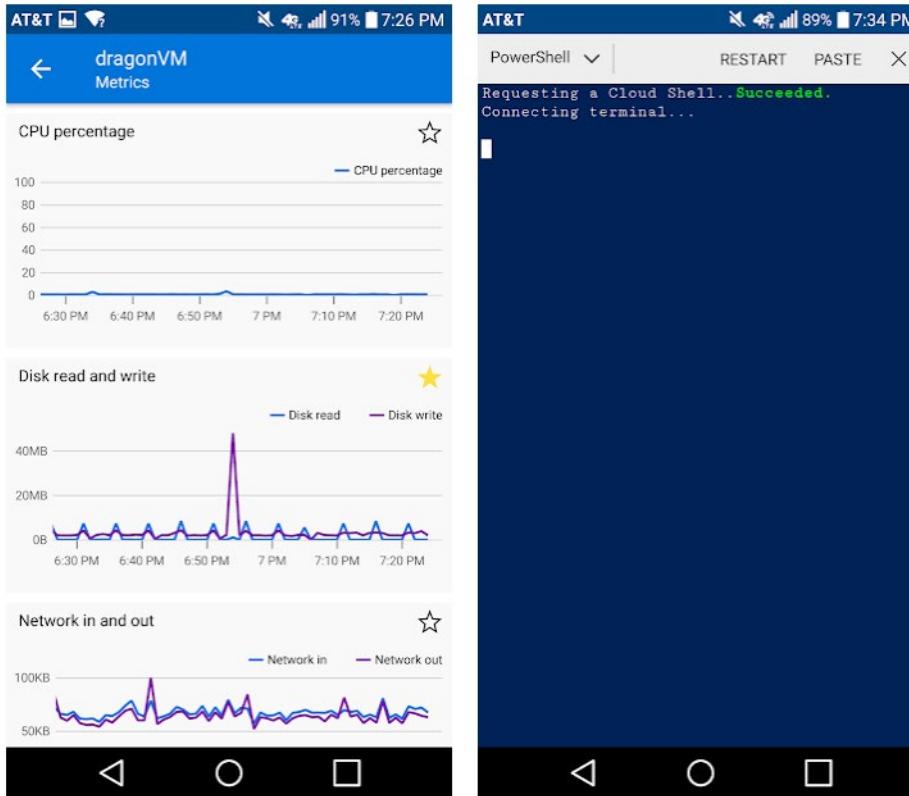
- Search resources, services, and docs.
- Manage resources.
- Create customized dashboards and favorites.
- Access the Cloud Shell.
- Receive notifications.
- Links to the Azure documentation.



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

Azure Mobile App

The **Microsoft Azure 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.

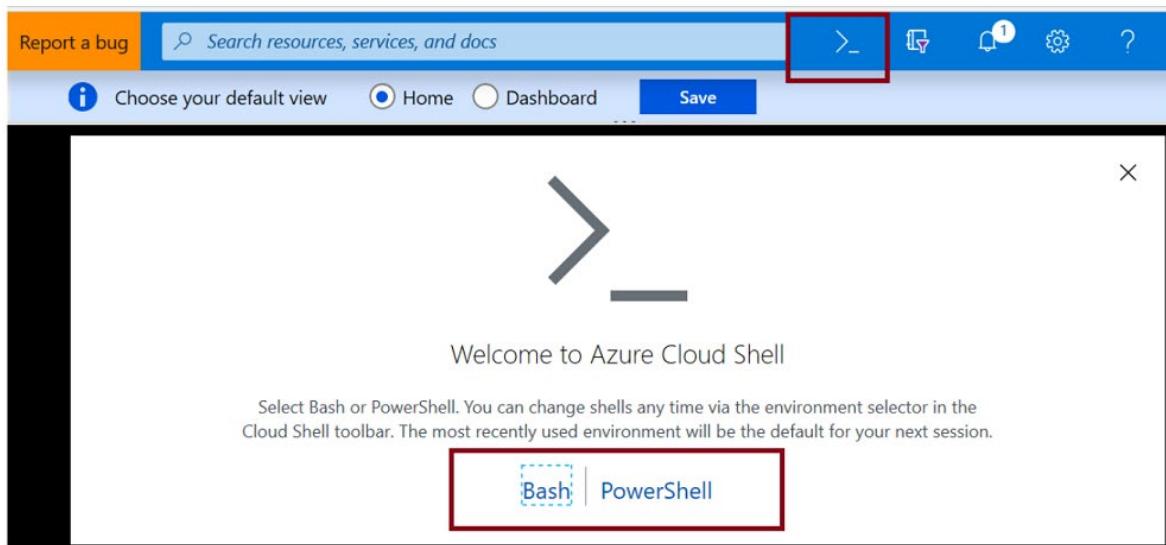
Customizing your experience

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.



Features of the Cloud Shell:

- 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.

Azure PowerShell and CLI

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	ExportedCom-
mands			
-----	-----	---	-----
Manifest	3.1.0.0	Microsoft.PowerShell.Management	{Add-Computer,
Add-Content, Checkpoint-Computer, Clear-Con...			
Manifest	3.1.0.0	Microsoft.PowerShell.Utility	{Add-Member,
Add-Type, Clear-Variable, Compare-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-PSRead-
LineKeyHandler, Get-PSReadLineOption, Remove-PS...			

Azure PowerShell

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

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

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

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

What is the Az module?

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

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

This module is an open source component [available on GitHub](#)¹.

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.

Demonstration - Working with PowerShell Locally

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

¹ <https://github.com/Azure/azure-powershell>

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. Login to Azure

```
Login-AzAccount
```

2. When prompted provide your credentials.

3. Verify your subscription information.

```
Get-AzSubscription
```

Create resources

Note: We will talk more about resource groups in an upcoming lesson.

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
```

Demonstration-Working with Azure CLI Locally

In this demonstration, you 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

You run Azure CLI by opening a Bash shell for Linux or macOS, or from the command prompt or PowerShell for Windows.

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

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
```

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>.

After a successful sign in, you'll be connected to your Azure subscription.

Note: We will talk more about resource groups in an upcoming lesson.

Create a resource group

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.

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

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

```
az group list
```

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

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

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

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

Note: You format the query using **JMESPath**, which is a standard query language for JSON requests. Learn more about this powerful filter language at <http://jmespath.org/>²

² <http://jmespath.org/>

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.

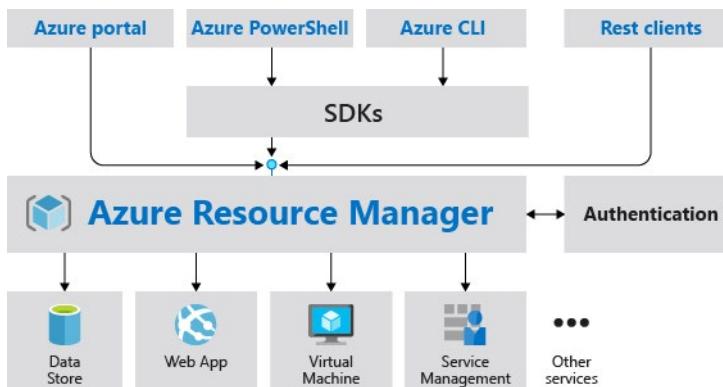
Azure Resource Manager enables you to work with the resources in your solution as a group. You can deploy, update, or delete all the resources for your solution in a single, coordinated operation. You use a template for deployment and that template can work for different environments such as testing,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

Resource Groups

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.

Guidance for creating resource groups

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

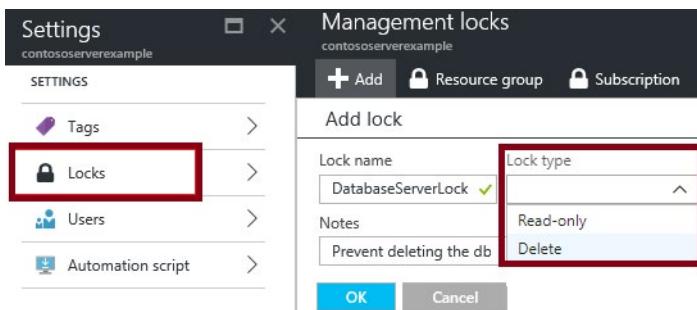
- All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.
- Each resource can only exist in one resource group.
- You 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.

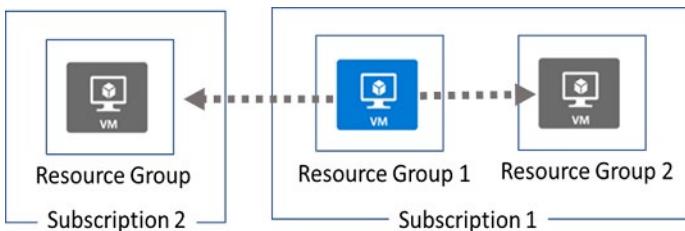


Locks come in two varieties.

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

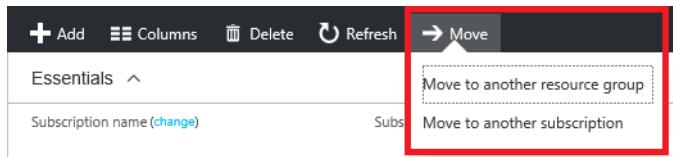
Before beginning this process:

- Review **services that can be moved**³.
- Review **services that cannot be moved**⁴.

³ <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-move-resources#services-that-can-be-moved>

⁴ <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-move-resources#services-that-cannot-be-moved>

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

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.



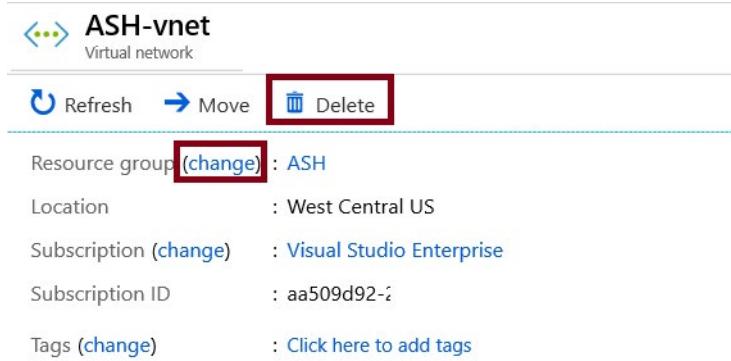
Using PowerShell to delete resource groups

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"
```

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.



Using PowerShell to delete a resource

To remove an individual resource use, **Remove-AzResource**. You will need the ResourceId. In this example, we are removing a website. You could also use the resource name.

```
Remove-AzResource -ResourceId <resourceId>
```

Demonstration - Resource Groups

In this demonstration, we will create and delete resource locks.

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

Manage resource groups in the portal

1. Access the Azure portal.
2. Create a resource group. Remember the name of this resource group.
3. In the **Settings** blade for the resource group, select **Locks**.
4. To add a lock, select **Add**. If you want to create a lock at a parent level, select the parent. The currently selected resource inherits the lock from the parent. For example, you could lock the resource group to apply a lock to all its resources.
5. Give the lock a **name** and **lock type**. Optionally, you can add notes that describe the lock.
6. To delete the lock, select the ellipsis and **Delete** from the available options.

Manage resource groups with PowerShell

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

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

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

```
Get-AzResourceLock
```

4. Delete the resource lock and confirm your action.

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

5. Verify the resource lock has been removed.

```
Get-AzResourceLock
```

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

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.

Here are some other template benefits to consider:

- **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

Azure Resource Manager 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/2015-01-01/
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 Templates - [https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-authoring-templates#template-limits⁵](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-authoring-templates#template-limits)

Template Parameters

Parameters

This template section is where you specify which values are configurable when the template runs. For example, you might allow users of your template to specify a username, password, or domain name.

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."  
        }  
    }  
}
```

Template Variables

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"  
}
```

⁵ <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-authoring-templates>

QuickStart Templates

Azure Quickstart templates⁶ are Resource Manager templates provided by the Azure community.

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.

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

Demonstration - QuickStart Templates

In this demonstration, you will explore QuickStart templates.

Explore the gallery

1. You could start by browsing to the **Azure Quickstart Templates gallery⁷**. 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 VM⁸** template.

[Templates](#) / Deploy a simple Windows VM

Deploy a simple Windows VM

[Deploy to Azure](#)

[Browse on GitHub](#)

This template allows you to deploy a simple Windows VM using a few different options for the Windows version, using the latest patched version. This will deploy a A2 size VM in the resource group location and return the FQDN of the VM.

⁶ <https://azure.microsoft.com/en-us/resources/templates/>

⁷ <https://azure.microsoft.com/resources/templates?azure-portal=true>

⁸ <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
```

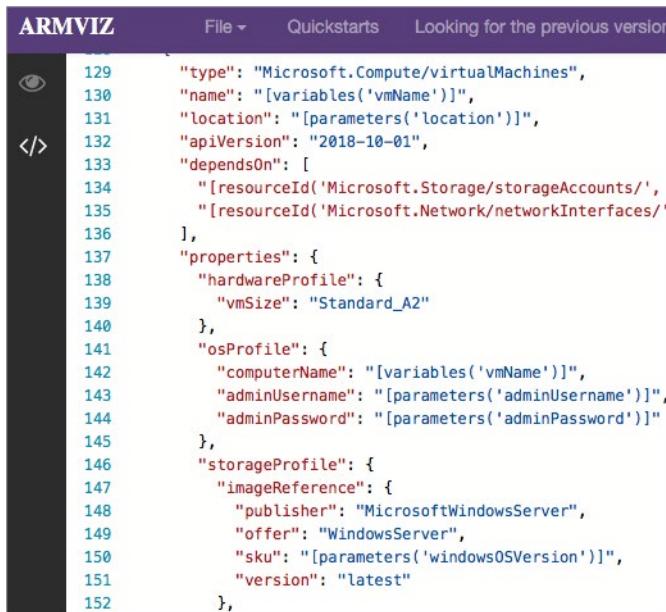
2. Click **Browse on GitHub** to navigate to the template's source code on GitHub.

The screenshot shows a GitHub repository page titled "Very simple deployment of a Windows VM". It features two prominent buttons: "Deploy to Azure" and "Visualize". Below these buttons is a brief description of the template's purpose: "This template allows you to deploy a simple Windows VM using a few different options. It will use the latest patched version. This will deploy a A2 size VM in the resource group location specified in the parameters section. You can change the name of the VM." The "Deploy to Azure" button has a blue background and white text, while the "Visualize" button has a light blue background and white text.

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**.

The screenshot shows the ARMVIZ interface, which displays three resources: "SimpleWinVM" (Virtual Machine), "myVMNic" (Network Interface), and "MyVNET" (Virtual Network). The "SimpleWinVM" resource is highlighted with a larger preview window showing its configuration details. The interface has a dark header bar with the title "ARMVIZ" and navigation links for "File", "Quickstarts", and "Looking for the previous version?". On the left, there is a vertical toolbar with icons for "View" and "Search".

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 and out.
7. Click on the VM resource labeled **SimpleWinVM**.



```

129     "type": "Microsoft.Compute/virtualMachines",
130     "name": "[variables('vmName')]",
131     "location": "[parameters('location')]",
132     "apiVersion": "2018-10-01",
133     "dependsOn": [
134       "[resourceId('Microsoft.Storage/storageAccounts/',",
135       "[resourceId('Microsoft.Network/networkInterfaces/'"
136     ],
137     "properties": {
138       "hardwareProfile": {
139         "vmSize": "Standard_A2"
140       },
141       "osProfile": {
142         "computerName": "[variables('vmName')]",
143         "adminUsername": "[parameters('adminUsername')]",
144         "adminPassword": "[parameters('adminPassword')]"
145       },
146       "storageProfile": {
147         "imageReference": {
148           "publisher": "MicrosoftWindowsServer",
149           "offer": "WindowsServer",
150           "sku": "[parameters('windowsOSVersion')]",
151           "version": "latest"
152         },

```

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

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
```

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

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.

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.

First, 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

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

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.

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.ps1⁹** 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

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

```
Get-AzVM
```

Note the VM name, then run the following command to obtain additional VM details:

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

⁹ <https://github.com/Microsoft/PartsUnlimited/blob/master/build.ps1?azure-portal=true>

Note the extension value listed.

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 >
```

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.

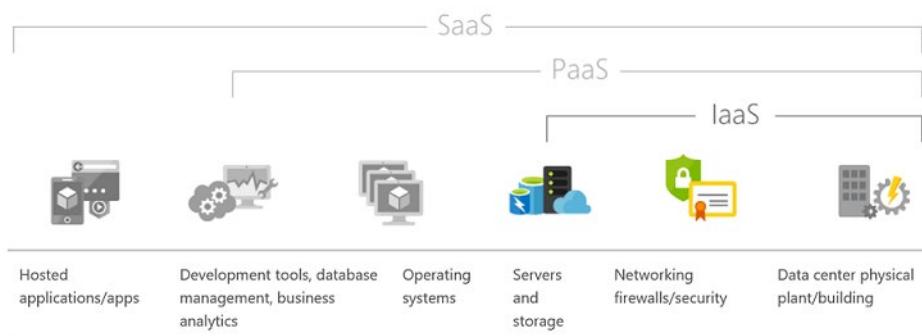
Module 2 Azure Virtual Machines

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.



There are lots of business scenarios for IaaS.

- **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.

- **Web apps.** IaaS provides all the infrastructure to support web apps, including storage, web and application servers, and networking resources. Organizations can quickly deploy web apps on IaaS and easily scale infrastructure up and down when demand for the apps is unpredictable.
 - **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

Azure Virtual Machine creation 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

Determine the size of the VM

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, 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, Fs, F	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.
Memory Optimized	Esv3, Ev3, M, GS, G, 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.

VM Type	Family	Description
Storage Optimized	Lsv2, Ls	Storage optimized VMs are designed to have high disk throughput and IO. Ideal for VMs running databases.
GPU	NV, NVv2, NC, NCv2, NCv3, ND, NDv2	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	H	High performance compute is the fastest and most powerful CPU virtual machines with optional high-throughput network interfaces.

What if my size needs change?

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 will be rebooted automatically 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 Azure - <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json#size-tables>¹

Sizes for Linux virtual machines in Azure - <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.

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

¹ <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json#size-tables>

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 Options

Azure Premium Storage delivers high-performance, low-latency disk support for virtual machines (VMs) with input/output (I/O)-intensive workloads. VM disks that use Premium Storage store data on solid-state drives (SSDs). To take advantage of the speed and performance of premium storage disks, you can migrate existing VM disks to Premium Storage.

In Azure, you can attach several premium storage disks to a VM. Using multiple disks gives your applications up to 256 TB of storage per VM. With Premium Storage, your applications can achieve 80,000 I/O operations per second (IOPS) per VM, and a disk throughput of up to 2,000 megabytes per second (MB/s) per VM. Read operations give you 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) (Preview), Premium SSD, Standard SSD, and Standard Hard Disk Drives (HDD).

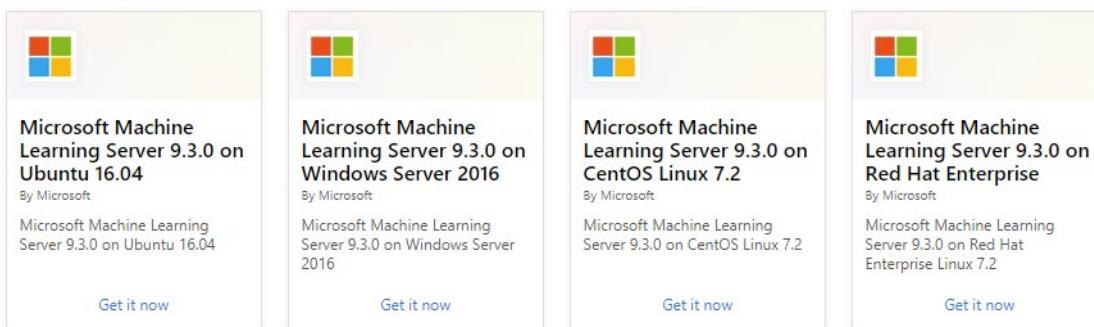
- ✓ For the best performance for your application, we recommend that you migrate any VM disk that requires high IOPS to Premium Storage. If your disk does not require high IOPS, you can help limit costs by keeping it in standard Azure Storage. In standard storage, VM disk data is stored on hard disk 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.



What Windows Server Software is Supported?

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.

What Linux Software is supported?

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 machines - <https://support.microsoft.com/en-us/help/2721672/microsoft-server-software-support-for-microsoft-azure-virtual-machines>

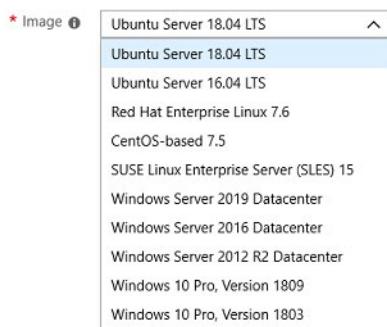
Linux on distributions endorsed by Azure - <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros#supported-distributions–versions>.²

² <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/endorsed-distros>

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](#) [Guest config](#) [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

Terms of Use

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 application 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.

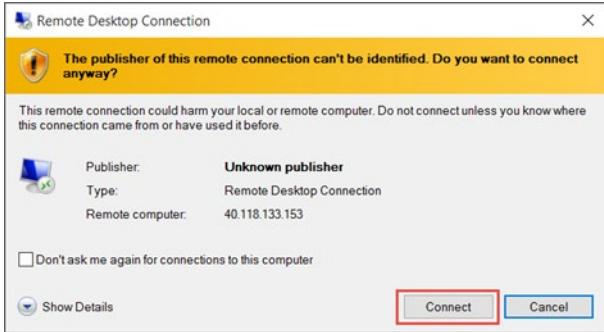
For more information:

Windows Virtual Machines Documentation - <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/>

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.
 - 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.

For more information:

Setting up WinRM access for Virtual Machines in Azure Resource Manager: <https://aka.ms/ljezi1>

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.

Home > New > Create a virtual machine

Create a virtual machine

Basics **Disks** **Networking** **Management** **Guest config** **Tags** **Review + create**

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

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

PROJECT DETAILS

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

* Subscription [?](#) Pay-As-You-Go

* Resource group [?](#) (New) myResourceGroup [Create new](#)

- Under **Instance details**, type *myVM* for the **Virtual machine name** and choose *East US* for your **Location**. Leave the other defaults.

INSTANCE DETAILS

* Virtual machine name [?](#) myVM

* Region [?](#) East US

Availability options None

* Image [?](#) Windows Server 2016 Datacenter [Browse all images and disks](#)

* Size [?](#) Standard DS1 v2
1 vcpu, 3.5 GB memory [Change size](#)

- 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.

ADMINISTRATOR ACCOUNT

* Username [?](#) azureuser

* Password [?](#) [Change password](#)

* Confirm password [?](#) [Change password](#) Password and confirm password must match

- Under **Inbound port rules**, choose **Allow selected ports** and then select **RDP (3389)** and **HTTP** from the drop-down.

INBOUND PORT RULES

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports None Allow selected ports

*

! These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

- Move to the **Management** tab, and under **Monitoring** turn **Off** Boot Diagnostics. This will eliminate validation errors.
- Leave the remaining defaults and then select the **Review + create** button at the bottom of the page. Wait for the validation, then click **Create**.

SAVE MONEY

Save up to 49% with a license you already own using Azure Hybrid Benefit for Windows Server. [Learn more](#)

* Already have a Windows license? Yes No

Review + create Previous Next : Disks >

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.

- Select the **Connect** button on the virtual machine properties page.
- In the **Connect to virtual machine** page, keep the default options to connect by DNS name over port 3389 and click **Download RDP file**.
- Open the downloaded RDP file and select **Connect** when prompted.
- 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**.
- You may receive a certificate warning during the sign-in process. Select **Yes** or **Continue** to create the connection.

Install web server

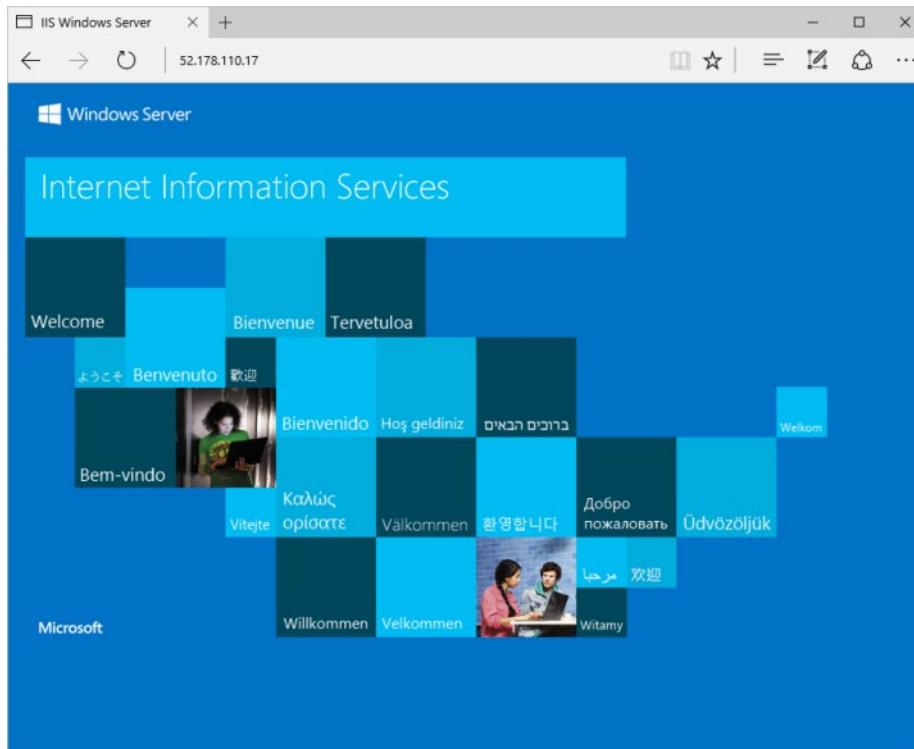
To observe your VM in action, install the IIS web server. Open a PowerShell prompt on the VM and run the following command:

```
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.

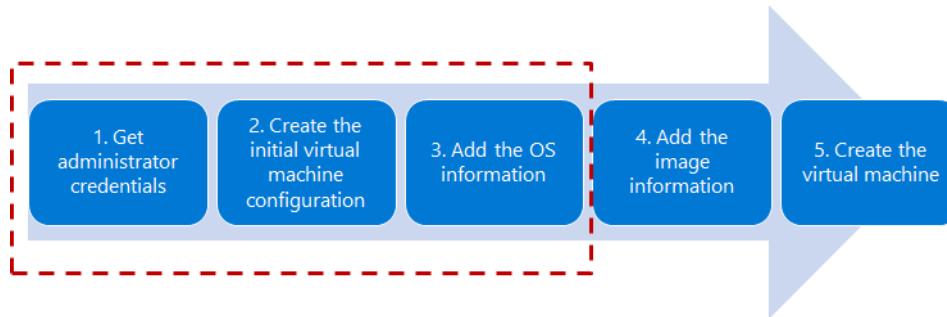


Clean up resources

- ✓ 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.

PowerShell - Example (Part 1)

You can also create a virtual machine using PowerShell. In this example, a virtual machine is created with a name of *myVM* running the latest version of Windows Server 2016 Datacenter.



1. Get the username and password needed for the administrator account on the virtual machine with **Get-Credential**:

```
$cred = Get-Credential
```

2. Create the initial configuration for the virtual machine with **New-AzVMConfig**:

```
$vm = New-AzVMConfig -VMName myVM -VMSize Standard_D1
```

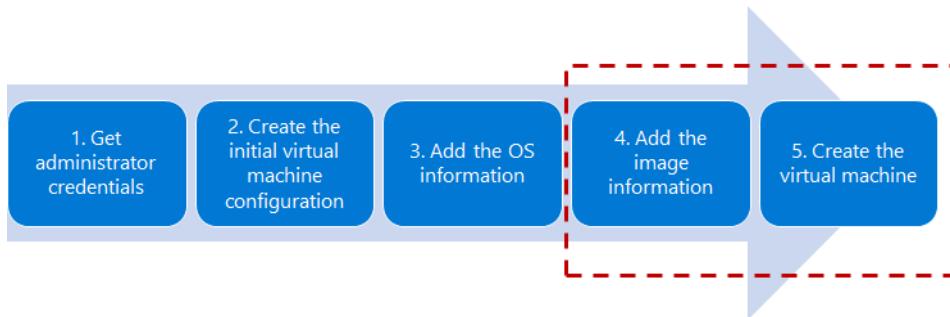
3. Add the operating system information to the virtual machine configuration with **Set-AzVMOperatingSystem**:

```
$vm = Set-AzVMOperatingSystem ` 
-VM $vm ` 
-Windows ` 
-ComputerName myVM ` 
-Credential $cred ` 
-ProvisionVMAgent -EnableAutoUpdate
```

✓ Continues in the next topic.

PowerShell - Example (Part 2)

This continues the example on the previous page.



4. Add the image information to the virtual machine configuration with **Set-AzVMSourceImage**:

```
$vm = Set-AzVMSourceImage ` 
-VM $vm ` 
-PublisherName MicrosoftWindowsServer ` 
-Offer WindowsServer ` 
-Skus 2016-Datacenter ` 
-Version latest
```

5. Create the virtual machine with **New-AzVM**.

```
New-AzVm ` 
-ResourceGroupName "myResourceGroup" ` 
-Name "myVM" ` 
-Location "East US" ` 
-VirtualNetworkName "myVnet" ` 
-SubnetName "mySubnet" ` 
-SecurityGroupName "myNetworkSecurityGroup" ` 
-PublicIpAddressName "myPublicIpAddress" ` 
-OpenPorts 80,3389
```

Demonstration - Creating a Virtual Machine with PowerShell

In this demonstration, we will create a virtual machine using PowerShell.

Create the virtual machine

Note: You can use the Cloud Shell or a local version of PowerShell.

Note: There are many ways to create a virtual machine with PowerShell. This example is different from the one explained in the topic slides.

1. Launch the Cloud Shell.

2. Run this code:

```
# create a resource group
New-AzResourceGroup -Name myResourceGroup -Location EastUS

# create the virtual machine
# when prompted, provide a username and password to be used as the logon
credentials for the VM
New-AzVm `

    -ResourceGroupName "myResourceGroup" `

    -Name "myVM" `

    -Location "East US" `

    -VirtualNetworkName "myVnet" `

    -SubnetName "mySubnet" `

    -SecurityGroupName "myNetworkSecurityGroup" `

    -PublicIpAddressName "myPublicIpAddress" `

    -OpenPorts 80,3389
```

Verify the machine creation in the portal

1. Access the portal and view your virtual machines.
2. Verify **myVM** was created.
3. Review the VM settings.
4. Notice this is a Windows machine in a new VNet and subnet.
5. Notice the command started the machine.
6. At this point you could use either the portal or PowerShell to make changes.

Connect to the virtual machine

1. Retrieve the public IP address of the machine.

```
Get-AzPublicIpAddress -ResourceGroupName "myResourceGroup" | Select "IpAddress"
```

2. Create an RDP session from your local machine. Replace the IP address with the public IP address of your VM. This command runs from a cmd window.

```
mstsc /v:publicIpAddress
```

3. When prompted, provide your login credentials for the machine. Be sure to **Use a different account**. Type the username as localhost\username, enter password you created for the virtual machine, and then select **OK**. You may receive a certificate warning during the sign-in process. Select **Yes** or **Continue** to create the connection
4. When done, close the RDP connection to the VM.
5. Clean up your resources. This will take a few minutes and remove the resource group and virtual machine.

```
Remove-AzResourceGroup -Name myResourceGroup
```

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.

 Debian Linux By credativ Debian GNU/Linux for Microsoft Azure provided by credativ. Software plans start at Free Get it now	 Clear Linux OS By Clear Linux Project A reference Linux distribution optimized for Intel Architecture. Bring your own license	 SUSE Linux Enterprise Server By SUSE SUSE Linux Enterprise Server Software plans start at Free Get it now	 Red Hat Enterprise Linux 7.4 By Red Hat Red Hat Enterprise Linux 7 is the world's leading enterprise Linux platform built to meet the needs of toda... Get it now
---	--	---	--

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 machines (Documentation) - <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/>

Linux VM Connections

When you create a Linux VM, you can decide to authenticate with an **SSH public key** or **Password**.



What is SSH?

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.

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.



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

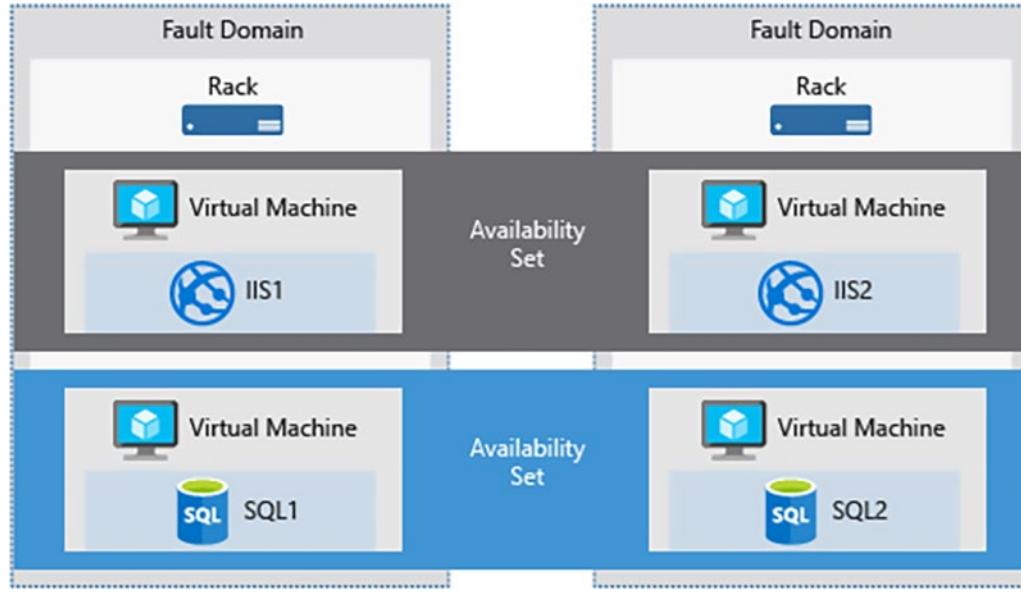
Update Domains and Fault Domains helps Azure maintain high availability and fault tolerance when deploying and upgrading applications. Each virtual machine in an availability set is placed in one update domain and two fault domains.

What is an update domain?

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.

What is a fault domain?

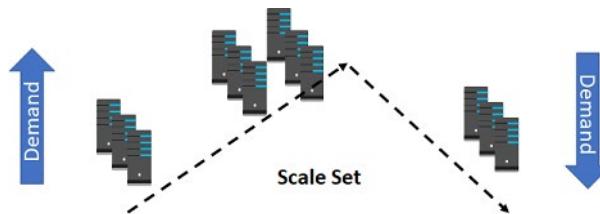
A **fault domain** defines a group of virtual machines that share a common set of hardware, switches, that share a single point of failure. For example, a server rack serviced by a set of power or networking switches. VMs in an availability set are placed in at least two fault domains. This mitigates against the effects of hardware failures, network outages, power interruptions, or software updates.



- ✓ 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.

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 sets works in a way that provides many 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

Create virtual machine scale set

INSTANCES

* Instance count Standard DS1 v2
1 vcpu, 3.5 GB memory [Change size](#)

Deploy as low priority
Low priority is not available for the selected instance size

Use managed disks

Enable scaling beyond 100 instances

- 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. Some size may only be available using templates, PowerShell, or CLI due to the recommended portal defaults.
- Deploy as low priority.** Deploying your scale set as low priority can save up to 80% over usual on-demand costs. The VMs in the scale set may be evicted at any time. This option can help save costs on stateless workloads. Low priority is not available for all selected sizes.
- 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.

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.



Benefits of autoscale

- **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.

Create virtual machine scale set

AUTOSCALE

Autoscale Disabled Enabled

* Minimum number of VMs

* Maximum number of VMs

Scale out

* CPU threshold (%)

* Number of VMs to increase by

Scale in

* CPU threshold (%)

* Number of VMs to decrease by

- **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 - <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 Windows - <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/features-windows?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json>

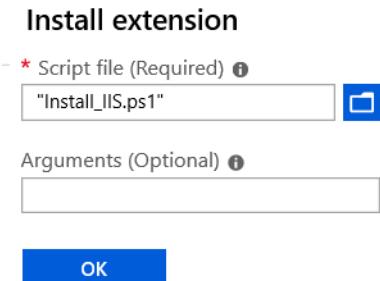
Virtual machine extensions and features for Linux - <https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/features-linux>

Custom Script Extensions

Custom Script Extension (CSE) can be used to automatically launch and execute virtual machine customization tasks post configuration. Your script extension may perform 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.

Implementation

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"
```

Things to consider

- **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 the **WindowsFeature resource**³. 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?

For more information:

Built-In Windows PowerShell Desired State Configuration Resources - <https://docs.microsoft.com/en-us/powershell/dsc/resources/resources#built-in-resources>

Demonstration - Custom Script Extension

In this demonstration, we will explore Custom Script Extensions.

Run a PowerShell script on a virtual machine

Note: This scenario requires a Windows virtual machine in the running state.

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
```

3. Create a file **Install_IIS.ps1** on your local machine.
4. Edit the file and add this command:

```
Install-WindowsFeature -Name Web-Server
```

5. In the Azure Portal, access your virtual machine, and select **Extensions**.
6. Click + **Add**. Take a minute to review the many different extensions that are available.
7. Locate the **Custom Script Extension** resource, select, and click **Create**.
8. Browse to your PowerShell script and upload the file. There will be a notification that the file was uploaded.
9. Click **OK**.

³ <https://docs.microsoft.com/en-us/powershell/dsc/windowsfeatureresource>

-
10. Select your **CustomScriptExtension**.
 11. Click **View detailed status** and verify provisioning succeeded.
 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.

```
Set-AzVmCustomScriptExtension -FileUri https://scriptstore.blob.core.windows.net/scripts/DeployWebServer.ps1 -Run "PowerShell.exe" -VmName vmName -ResourceGroupName resourceGroup -Location "location"
```

Lab and Review Questions

Lab - Deploy and Manage Virtual Machines

Scenario

Adatum Corporation wants to implement its workloads by using Azure virtual machines (VMs) and Azure VM scale sets.

Objectives

After completing this lab, you will be able to:

- Deploy Azure VMs by using the Azure portal, Azure PowerShell, and Azure Resource Manager templates.
- Configure networking settings of Azure VMs running Windows and Linux operating systems.
- Deploy and configure Azure VM scale sets.

Exercise 1: Deploy Azure VMs by using the Azure portal, Azure PowerShell, and Azure Resource Manager templates.

The main tasks for this exercise are as follows:

- Deploy an Azure VM running Windows Server 2016 Datacenter into an availability set by using the Azure portal.
- Deploy an Azure VM running Windows Server 2016 Datacenter into the existing availability set by using Azure PowerShell.
- Deploy two Azure VMs running Linux into an availability set by using an Azure Resource Manager template.

Result: After you completed this exercise, you have deployed an Azure VM running Windows Server 2016 Datacenter into an availability set by using the Azure portal, deployed another Azure VM running Windows Server 2016 Datacenter into the same availability set by using Azure PowerShell, and deployed two Azure VMs running Linux Ubuntu into an availability set by using an Azure Resource Manager template.

Exercise 2: Configure networking settings of Azure VMs running Windows and Linux operating systems

The main tasks for this exercise are as follows:

- Configure static private and public IP addresses of Azure VMs.
- Connect to an Azure VM running Windows Server 2016 Datacenter via a public IP address.
- Connect to an Azure VM running Linux Ubuntu Server via a private IP address.

Result: After you completed this exercise, you have configured static private and public IP addresses of Azure VMs, connected to an Azure VM running Windows Server 2016 Datacenter via a public IP address, and connect to an Azure VM running Linux Ubuntu Server via a private IP address

Exercise 3: Deploy and configure Azure VM scale sets

The main tasks for this exercise are as follows:

- Identify an available DNS name for an Azure VM scale set deployment
- Deploy an Azure VM scale set
- Install IIS on a scale set VM by using DSC extensions

Result: After you completed this exercise, you have identified an available DNS name for an Azure VM scale set deployment, deployed an Azure VM scale set, and installed IIS on a scale set VM by using the DSC extension.

Module 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?

- 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. Choose 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

You deploy a new VM with default settings to a resource group named RG1. You validate that you can connect to it by using Remote Desktop Connection. However, when you attempt to connect to it through PowerShell remoting, the connection fails. You need to ensure that you can manage the VM by using PowerShell remoting. What should you do? Select one.

- Create an inbound security rule to allow TCP port 80 and TCP port 443.
- Create an inbound security rule to allow TCP port 5985 and TCP port 5986.
- Create an inbound security rule to allow TCP port 3389.
- Create an inbound security rule to allow TCP port 20 and TCP port 21.

Review Question 5

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?

- 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 6

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 7

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 8

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 9

You deploy an Azure VM into an availability set. The VM is the only VM in the availability set. The VM runs an application named App1. The VM has the following characteristics:

- The VM uses Azure standard storage.
- The VM does not have any data disks.

- The VM was built with a custom image.

During an Azure planned maintenance event, the VM experiences downtime. The company issues a new requirement for App1:

- App1 must remain available during Azure planned maintenance events

You need to reconfigure your environment to meet the new requirements. What should you do? (Each answer presents a complete solution. Choose two.)

- Deploy a second Azure VM and add it to the same availability set.
- Deploy a second Azure VM and add it to the same update domain.
- Deploy a second Azure VM and add it to the same fault domain.
- Convert the VM storage to premium storage.
- Convert the VM to a Standard size or higher.
- Convert the VM storage to use zone redundant storage.

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?

- 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. Choose 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

You deploy a new VM with default settings to a resource group named RG1. You validate that you can connect to it by using Remote Desktop Connection. However, when you attempt to connect to it through PowerShell remoting, the connection fails. You need to ensure that you can manage the VM by using PowerShell remoting. What should you do? Select one.

- Create an inbound security rule to allow TCP port 80 and TCP port 443.
- Create an inbound security rule to allow TCP port 5985 and TCP port 5986.
- Create an inbound security rule to allow TCP port 3389.
- Create an inbound security rule to allow TCP port 20 and TCP port 21.

Explanation

This was not explicitly covered in the course materials, but is an interesting learning point. PowerShell Remoting requires TCP port 5985 and TCP port 5986. While you can customize the ports, this scenario presents the default configuration. Some administrators opt to use TCP port 80 and TCP port 443 because of their familiarity with them.

Review Question 5

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?

- 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 6

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 7

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 8

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 9

You deploy an Azure VM into an availability set. The VM is the only VM in the availability set. The VM runs an application named App1. The VM has the following characteristics:

During an Azure planned maintenance event, the VM experiences downtime. The company issues a new requirement for App1:

You need to reconfigure your environment to meet the new requirements. What should you do? (Each answer presents a complete solution. Choose two.)

- Deploy a second Azure VM and add it to the same availability set.
- Deploy a second Azure VM and add it to the same update domain.
- Deploy a second Azure VM and add it to the same fault domain.
- Convert the VM storage to premium storage.
- Convert the VM to a Standard size or higher.
- Convert the VM storage to use zone redundant storage.

Explanation

When an availability set only has a single member, an outage might occur during an Azure planned maintenance event. To ensure the app has at least one server available during a planned maintenance event, you should add a second VM to the same availability set. Instead of adding a second VM, you can convert the VM storage to premium storage. VMs with premium storage will remain available during a planned maintenance event.

Module 3 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.

For more information:

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

Azure Storage Services

Azure Storage services

Azure Storage includes these data services, each of which is accessed through a storage account.

- **Azure 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.

Blob storage

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data. Blob storage is ideal for:

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

Objects in Blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

Azure Files

Azure Files enables you to set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol. That means that multiple VMs can share the same files with both read and write access. You can also read the files using the REST interface or the storage client libraries.

One thing that distinguishes Azure Files from files on a corporate file share is that you can access the files from anywhere in the world using a URL that points to the file and includes a shared access signature (SAS) token. You can generate SAS tokens; they allow specific access to a private asset for a specific amount of time.

File shares can be used for many common scenarios:

- Many on-premises applications use file shares. This feature makes it easier to migrate those applications that share data to Azure. If you mount the file share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with minimal, if any, changes.

- Configuration files can be stored on a file share and accessed from multiple VMs. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them, and that they use the same version.
- Diagnostic logs, metrics, and crash dumps are just three examples of data that can be written to a file share and processed or analyzed later.

At this time, Active Directory-based authentication and access control lists (ACLs) are not supported, but they will be at some time in the future. The storage account credentials are used to provide 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.

Standard and Premium Accounts

General purpose storage accounts have two tiers: **Standard** and **Premium**.

Create storage account



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.

Storage Types

When you create a storage account you can choose from: Storage (general purpose v1), Storage V2 (general purpose v2), and Blob storage.

Create storage account

The screenshot shows a user interface for creating an Azure storage account. At the top, there are tabs for 'Basics', 'Advanced', 'Tags', and 'Review + create'. The 'Basics' tab is currently selected. Below the tabs, there is a section titled 'Account kind' with a help icon. A dropdown menu is open, showing four options: 'StorageV2 (general purpose v2)' (which is highlighted in blue), 'StorageV2 (general purpose v2)', 'Storage (general purpose v1)', and 'BlobStorage'. There is also a small upward-pointing arrow icon next to the dropdown.

Azure Storage offers three 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 three types of storage accounts are:

- **General-purpose v2 accounts.** General-purpose v2 storage accounts support the latest Azure Storage features and incorporate all of the functionality of general-purpose v1 and Blob storage accounts. General-purpose v2 accounts deliver the lowest per-gigabyte capacity prices for Azure Storage, as well as industry-competitive transaction prices. General-purpose v2 storage accounts support many services: Blobs (all types: Block, Append, Page), Files, Disks, Queues, and Tables. Microsoft recommends using a general-purpose v2 storage account for most scenarios. You can easily upgrade a general-purpose v1 or Blob storage account to a general-purpose v2 account with no downtime and without the need to copy data.
- **General-purpose v1 accounts.** General-purpose v1 accounts provide access to all Azure Storage services, but may not have the latest features or the lowest per gigabyte pricing. Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.
- **Blob storage accounts** A Blob storage account is a specialized storage account for storing unstructured object data as block blobs. Blob storage accounts provide the same durability, availability, scalability, and performance features that are available with general-purpose v2 storage accounts. Blob storage accounts support storing block blobs and append blobs, but not page blobs. Blob storage accounts offer multiple access tiers for storing data based on your usage patterns.

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:

- Blob 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 (preview). 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.

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.

Demonstration - Creating Storage Accounts

In this demonstration, we will review creating storage accounts.

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**.

Create a storage account using PowerShell

Use the following code to create a storage account using PowerShell. Swap out the storage types and names to suit your requirements.

```
Get-AzLocation | select Location
$location = "westus"
$resourceGroup = "storage-demo-resource-group"
New-AzResourceGroup -Name $resourceGroup -Location $location
New-AzStorageAccount -ResourceGroupName $resourceGroup -Name "storagedemo" -Location $location -SkuName Standard_LRS -Kind StorageV2
```

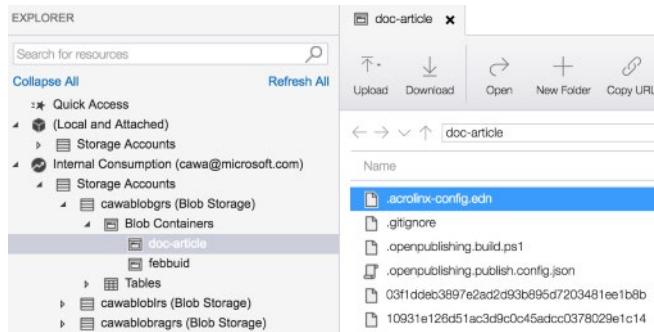
Create a storage account using Azure CLI

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
```

Azure Storage Explorer

Microsoft Azure Storage Explorer is a standalone app from Microsoft that allows you to easily work with Azure Storage data.



Some of the benefits of Azure Storage Explorer include the ability to access multiple accounts and subscriptions across Azure,

Azure Stack, and the sovereign Cloud. Additionally you can use Azure Storage Explorer to create, delete, view and edit Blob,

Queue, Table, File, Cosmos DB storage and Data Lake storage. Storage Explorer is available for Windows, Mac, and Linux.

Azure Storage Explorer Features

The following features are present in the latest version of Storage Explorer.

Blob storage

- View, delete, and copy blobs and folders.
- Upload and download blobs while maintaining data integrity.
- Manage snapshots for blobs.

Table storage

- Query entities with OData or query builder.
- Add, edit, and delete entities.
- Import and export tables and query results.

Azure Cosmos DB storage

- Create, manage, and delete databases and collections.
- Generate, edit, delete, and filter documents.
- Manage stored procedure, triggers, and user-defined functions.

Queue storage

- Peek most recent 32 messages.
- View, add, and dequeue messages.
- Clear queue.

File storage

- Navigate files through directories.
- Upload, download, delete, and copy files and directories.
- View and edit file properties.

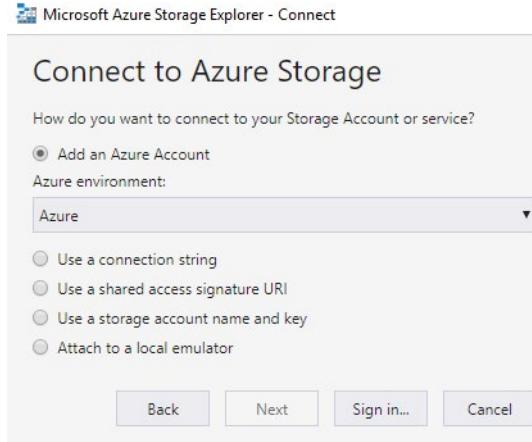
Azure Data Lake storage

- Navigate ADLS resources across multiple ADL accounts.
- Upload, download files and folders.
- Copy folders or files to the clipboard.
- Delete files and folders.

Storage Explorer Connection Options

Storage Explorer provides several ways to connect to storage accounts. For example, you can:

- 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.

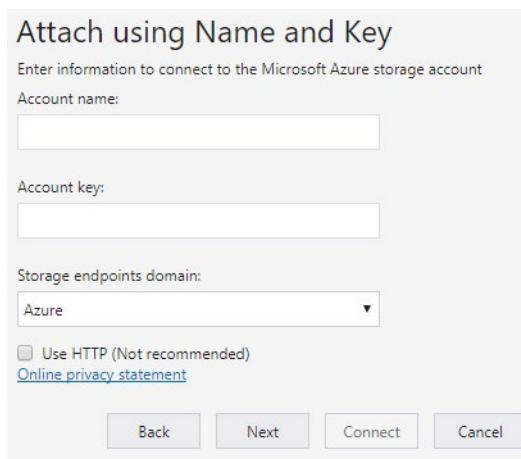


In addition, you can work with storage accounts in global and national Azure:

- **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.

Demonstration - Storage Explorer

Note: If you have an older version of the Storage Explorer, be sure to upgrade. These steps use version 1.6.2.

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.

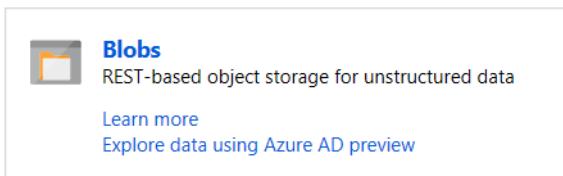
Attach an Azure storage account

1. Access the Azure portal, and your storage account.
2. Explore the choice for **Storage Explorer**, which is now in preview.
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**.

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:

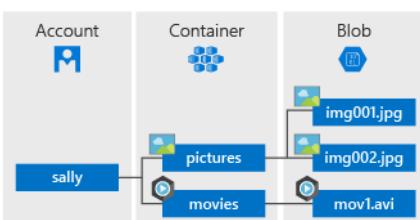
- Serving images or documents directly to a browser.
- Storing files for distributed access, such as installation.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

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.



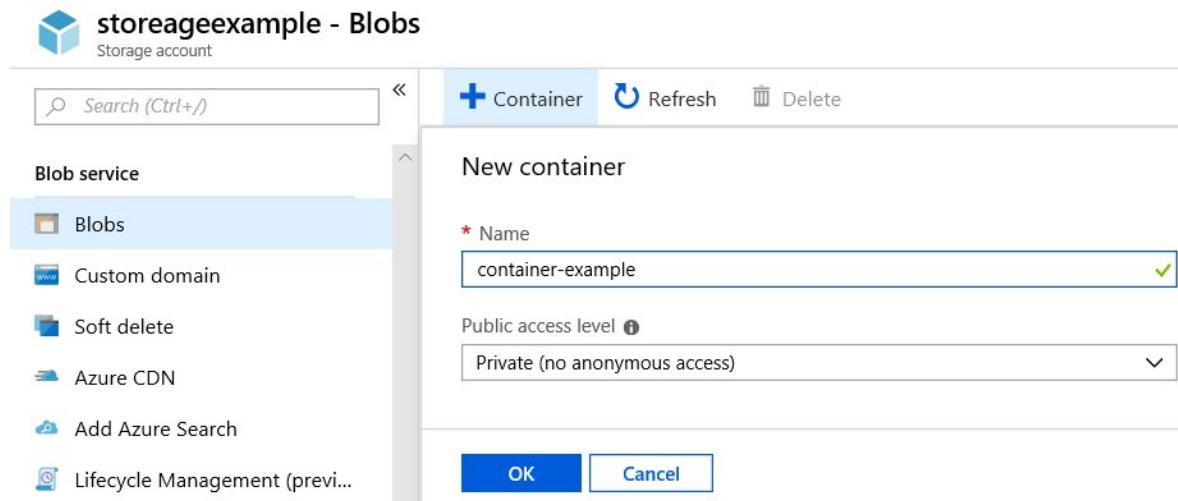
- ✓ Within the storage account, you can group as many blobs as needed in a container.

For more information:

Azure Blob Storage - <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 Performance 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

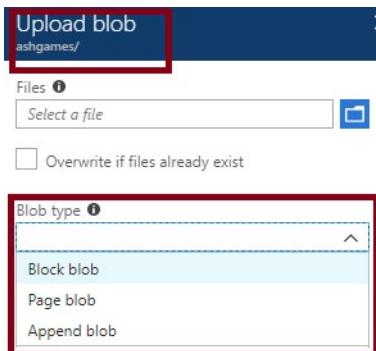
Optimize storage costs by placing your data in the appropriate access tier.



- **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.

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 when you create the blob. The default is a block blob.



- *Block blobs* 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.
- ✓ You can also upload a local file to blob storage using the PowerShell **Set-AzStorageBlobContent** command.

Blob upload tools

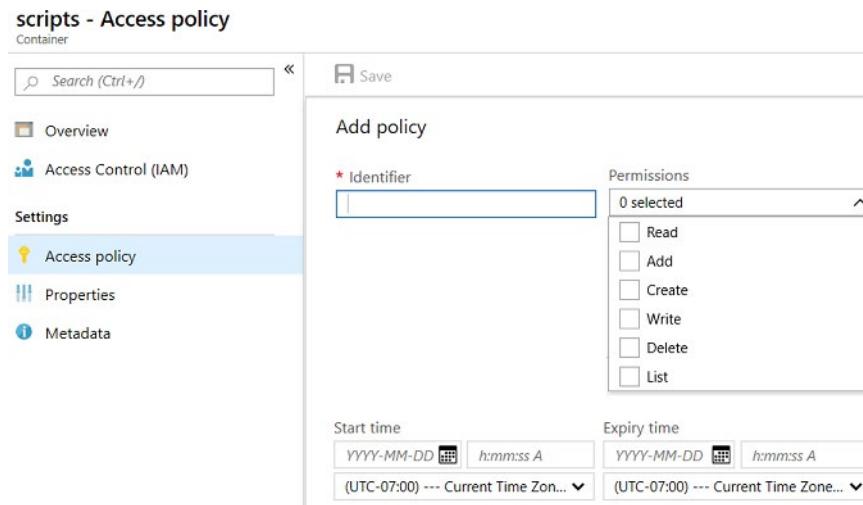
There are multiple methods to upload data to blob storage, including the following methods:

- **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.

Blob Access Policies

A stored access policy provides an additional level of control over service-level shared access signatures (SAS) on the server side. Establishing a stored access policy serves to group shared access signatures and to provide additional restrictions for signatures that are bound by the policy. You can use a stored access policy to change the start time, expiry time, or permissions for a signature, or to revoke it after it has been issued.



The following storage resources support stored access policies:

- Blob containers
- File shares
- Queues
- Tables

A stored access policy on a container can be associated with a shared access signature granting permissions to the container itself or to the blobs it contains. Similarly, a stored access policy on a file share can be associated with a shared access signature granting permissions to the share itself or to the files it contains.

Stored access policies are currently not supported for account SAS.

- ✓ SAS will be covered in more detail in the last lesson, Storage Security.

Blob 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**.

Note: As you have time, explore using Azure Storage Explorer for managing blob storage.

Azure Files

Azure Files



File storage¹ offers shared storage for applications using the industry standard **SMB protocol**². 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 include:

- **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.

✓ Which of the usage cases for files are you most interested in?

For more information:

What is Azure Files?- <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

Files vs Blobs

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. Additionally, Azure File shares can be cached on Windows Servers with Azure File Sync (next lesson) for fast access near where the data is being used.

¹ <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

² <https://msdn.microsoft.com/library/windows/desktop/aa365233.aspx>

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.
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.

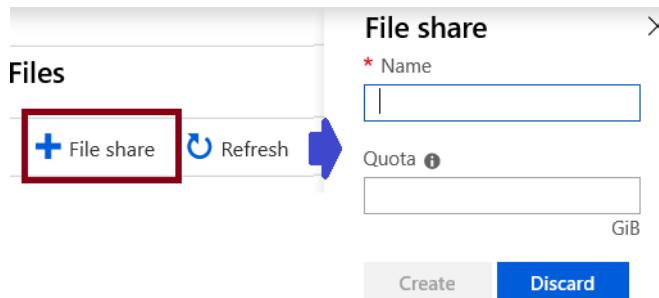
- Azure files are true directory objects. Azure blobs are a flat namespace.
- Azure files are accessed through file shares. Azure blobs are accessed through a container.
- Azure files provide shared access across multiple virtual machines. Azure disks are exclusive to a single virtual machine.
- ✓ When selecting which storage feature to use, you should also consider pricing. Take a minute to view the [Azure Storage Overview pricing³](#) page.

Creating File Shares

To access your files, you will need a file share. There are several ways to create a file share.

Creating a file share (Portal)

Before you can create a file share 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. Be sure to test by uploading and accessing a file.



³ <https://azure.microsoft.com/en-us/pricing/details/storage/>

The rules for file service share names are more restrictive than what is prescribed by the SMB protocol for SMB share names, so that the Blob and File services can share similar naming conventions for containers and shares. The naming restrictions for shares are as follows:

- A share name must be a valid DNS name.
- Share names must start with a letter or number, and can contain only letters, numbers, and the dash (-) character.
- Every dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in share names.
- All letters in a share name must be lowercase.
- Share names must be from 3 through 63 characters long.

Creating a file share (PowerShell)

You can also use PowerShell to create a file share.

```
# Retrieve storage account and storage account key
$storageContext = New-AzStorageContext <storage-account-name> <storage-ac-
count-key>
# Create the file share, in this case "logs"
$share = New-AzStorageShare logs -Context $storageContext
```

Mapping File Shares (Windows)

You can connect to your Azure file share with Windows or Windows Server. Here is what you will need:

- **Mapping Drive Letter:** Your choice.
- **UNC Path:** In the form \\storagename.file.core.windows.net\filesharename

To map the Windows drive you will also need to supply the account credentials in the Windows Security dialog box.

- **Account User:** In the form AZURE\storagename
- **Storage Account Key:** To mount an Azure file share, you will need the primary (or secondary) storage key.

All of this information is available by selecting **Connect** from your file share page.

Connect

test

Windows [Linux](#) [MacOS](#)

Drive letter
Z ▾

To connect to this file share from a Windows computer, run these PowerShell commands:

```
net use Z: \\rgtest11.file.core.windows.net\test
/u:AZURE\rgtest11
k3b
HtX
JEEy0YX41g
J==
```

When connecting from a computer from outside Azure, remember to open outbound TCP port 445 in your local network. Some Internet service providers may block port 445. Check with your service provider for details.

- ✓ 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)

Azure file shares can be mounted in Linux distributions using the CIFS kernel client. There are two ways to mount an Azure file share:

- On-demand with the mount command.
- On-boot (persistent) by creating an entry in /etc/fstab.

Prerequisites for mounting the file share in Linux

In addition to the Windows prerequisites, you also need:

- **Install the cifs-utils package.** Consult the documentation to ensure you are running a Linux distribution that supports this package.
- **Understand the SMB client requirements.** Azure Files can be mounted either via SMB 2.1 or SMB 3.0. For connections coming from clients on-premises or in other Azure regions, Azure Files will reject SMB 2.1 (or SMB 3.0 without encryption). If **secure transfer required** is enabled for a storage account, Azure Files will only allow connections using SMB 3.0 with encryption.
- **Decide on the directory/file - chmod permissions⁴.**

Mount the file share

You can use the file share **Connect** page for your file share to view the mount command.

⁴ <https://en.wikipedia.org/wiki/Chmod>

Connect

test

Windows Linux MacOS

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

```
sudo mount -t cifs //rgtest11.file.core.windows.net/test
[mount point] -o
vers=3.0,username=rgtest11,password=k3bNxncDkoP70DO
34gr                                     'orPKA
JcOD                                     .mode=
0777,sec=ntlmssp
```

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.

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.

rgtest11 - Configuration
Storage account

Settings

Save Discard

Performance Standard Premium

* Secure transfer required
Enabled

Access tier (default) Cool Hot

When you are using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some versions of the Linux SMB client.

You can also use tooling to enable this feature. Here is how to use PowerShell and the **EnableHttpsTrafficOnly** parameter.

```
Set-AzStorageAccount -Name <StorageAccountName> -ResourceGroupName <ResourceGroupName> -EnableHttpsTrafficOnly $True
```

- ✓ 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.

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 $resource-
GroupName -Name $storageAccountName
```

3. Create a context for your storage account and key. The context encapsulates the storage account name and account key.

```
$storageContext = New-AzStorageContext -StorageAccountName "YourStorageAc-
countName" -StorageAccountKey $storageAccountKeys[0].value
```

4. Create the file share. The name of your file share must be all lowercase.

```
$share = New-AzStorageShare "YourFileShareName" -Context $storageContext
```

Mount a file share (PowerShell)

Note: Run the following commands from a regular (i.e. not an elevated) PowerShell session to mount the Azure file share. Remember to replace <your-resource-group-name>, <your-storage-account-name>, <your-file-share-name>, and desired-drive-letter with the proper information.

```
$resourceGroupName = "your-resource-group-name"
$storageAccountName = "your-storage-account-name"
$fileShareName = "your-file-share-name"

# These commands require you to be logged into your Azure account, run
Login-AzAccount if you haven't
# already logged in.
$storageAccount = Get-AzStorageAccount -ResourceGroupName $resourceGroupName
-Name $storageAccountName
$storageAccountKeys = Get-AzStorageAccountKey -ResourceGroupName $resource-
GroupName -Name $storageAccountName
$fileShare = Get-AzStorageShare -Context $storageAccount.Context | Where-Ob-
ject {
    $_.Name -eq $fileShareName -and $_.IsSnapshot -eq $false
}

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

# The value given to the root parameter of the New-PSDrive cmdlet is the
```

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

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

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

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 in preview 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. Azure AD integration is currently available in preview for the Blob and Queue services. 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.



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: Blob, Queue, Table, or File service.

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>⁵

Configuring SAS Parameters

Configuring a SAS includes Permissions, Start and expiry date/time, Allowed IP addresses, Allowed protocols, and Signing key. In this example, we are generating a Blob SAS token and URL.

⁵ <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>

The screenshot shows the 'Permissions' dropdown set to 'Read'. The 'Start and expiry date/time' section shows 'Start' as 2019-02-27 7:32:03 AM and 'Expiry' as 2019-02-27 3:32:03 PM. The 'Allowed IP addresses' field contains '(UTC-08:00) --- Current Time Zone ---'. The 'Allowed protocols' section has 'HTTPS' selected. The 'Signing key' dropdown is set to 'Key 1'. A blue button at the bottom reads 'Generate blob SAS token and URL'.

- **Permissions.** Your choices are Read, Create, Write, and Delete. You may select any combination of permissions.
- **Start and expiry date/time.** The times during which the SAS is valid.
- **Allowed IP addresses.** The IP addresses from which to accept requests.
- **Allowed protocols.** Only allowing HTTPS requests is recommended.
- **Signing key.** Your choices are: key1 or key2.

PowerShell Options

Create a storage account level SAS with full permissions.

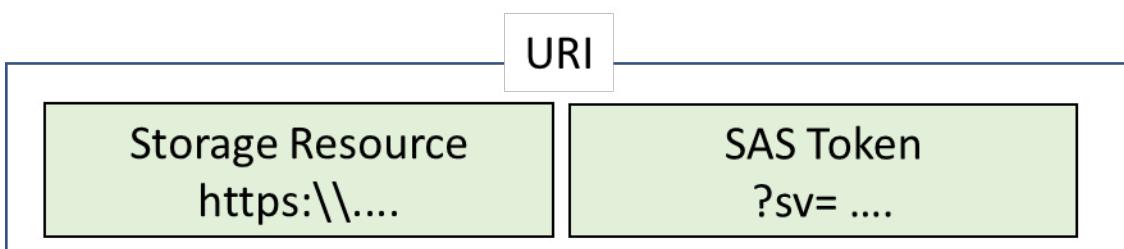
```
New-AzStorageAccountSASToken -Service Blob,File,Table,Queue -ResourceType Service,Container,Object -Permission "racwdlup"
```

Create a Blob level SAS will full permisions.

```
New-AzStorageBlobSASToken -Container "ContainerName" -Blob "BlobName" -Permission rwd
```

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.
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 parameters - <https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1?toc=%2fazure%2fstorage%2fblobs%2ftoc.json#shared-access-signature-parameters>⁶

⁶ <https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

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.

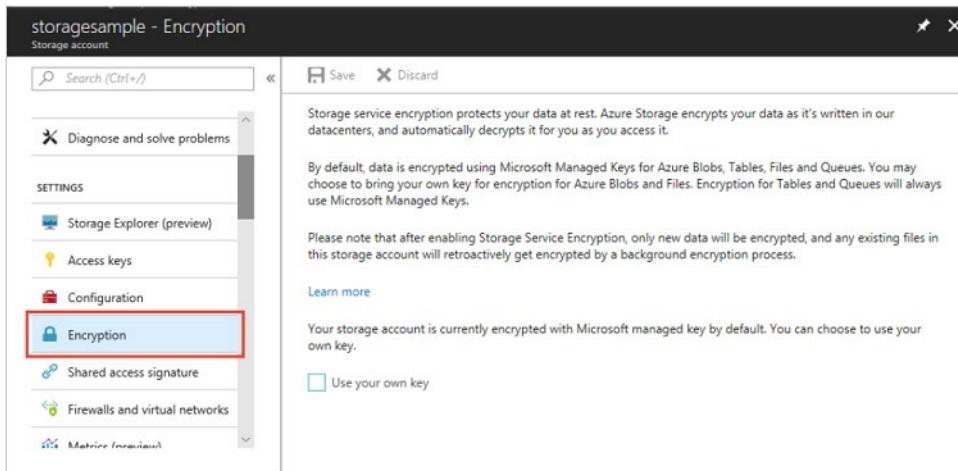
Create a SAS at the account level

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 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.



- ✓ 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.

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

Use your own key

Encryption key

Enter key URI
 Select from Key Vault

* Key Vault

USW-Vault-4

* Encryption key

USW-App24-Data

- ✓ 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.

- ✓ The key vault can also be used to store BitLocker keys.

SAS Best Practices

Risks

When you use shared access signatures in your applications, you need to be aware of two potential risks:

- If a SAS is leaked, it can be used by anyone who obtains it, which can potentially compromise your storage account.

- 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 these 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.

Demonstration - SAS (Storage Explorer)

In this demonstration, you will attach a storage account by using a Shared Access Signature.

Note: This demonstration requires a storage account and access to Storage Explorer.

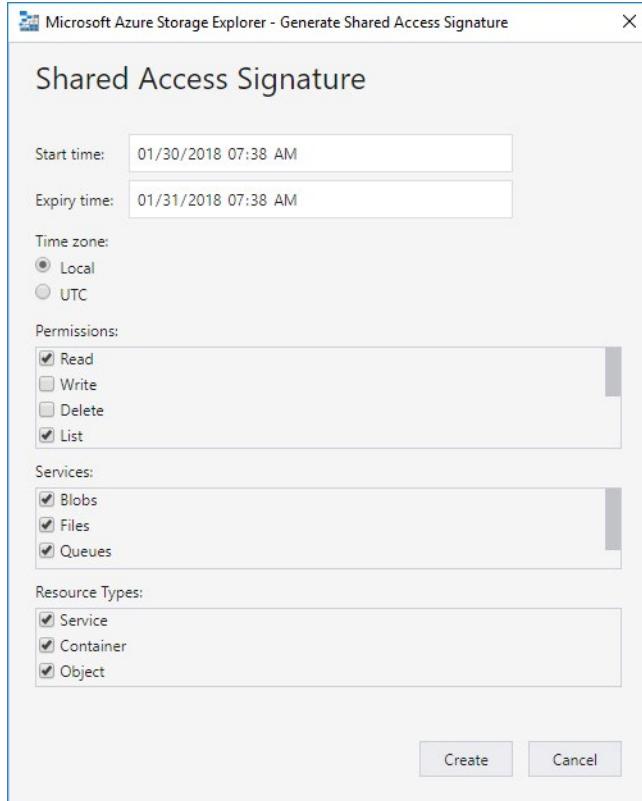
Scenario

A Shared Access Signature lets the admin of an Azure subscription grant temporary access to a storage account without having to provide Azure subscription credentials. To illustrate this scenario, let's say that UserA is an admin of an Azure subscription, and UserA wants to allow UserB to access a storage account for a limited time with certain permissions:

- UserA generates a SAS connection string for a specific time period and with the desired permissions.
- UserA shares the SAS with the person (UserB, in this example) who wants access to the storage account.
- UserB uses Storage Explorer to attach to the account that belongs to UserA by using the supplied SAS.

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**.

Note: This Connection string would be provided to UserB.

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.

Note: UserB will now have access to the storage. Notice that you can also provide access for Azure Cosmos DB and Azure Data Lake Store.

MCT USE ONLY. STUDENT USE PROHIBITED

Lab and Review Questions

Lab - Implement and Manage Storage

Scenario

Adatum Corporation wants to leverage Azure Storage for hosting its data

Objectives

After completing this lab, you will be able to:

- Deploy an Azure VM by using an Azure Resource Manager template.
- Implement and use Azure Blob Storage.
- Implement and use Azure File Storage.

Exercise 0: Prepare the lab environment.

The main task for this exercise is as follows:

- Deploy an Azure VM by using an Azure Resource Manager template.

Result: After you completed this exercise, you have initiated template deployment of an Azure VM az1000201-vm1 that you will use in the second exercise of this lab.

Exercise 1: Implement and use Azure Blob Storage.

- The main tasks for this exercise are as follows:
- Create Azure Storage accounts.
- Review configuration settings of Azure Storage accounts.
- Manage Azure Storage Blob Service.
- Copy a container and blobs between Azure Storage accounts.
- Use a Shared Access Signature (SAS) key to access a blob.

Result: After you completed this exercise, you have created two Azure Storage accounts, reviewed their configuration settings, created a blob container, uploaded blobs into the container, copied the container and blobs between the storage accounts, and used a SAS key to access one of the blobs.

Exercise 2: Implement and use Azure File Storage.

The main tasks for this exercise are as follows:

- Create an Azure File Service share.
- Map a drive to the Azure File Service share from an Azure VM.

Result: After you completed this exercise, you have created an Azure File Service share, mapped a drive to the file share from an Azure VM, and used File Explorer from the Azure VM to create a folder and a file in the file share.

Module 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

When you created a virtual machine you selected standard storage because the data was accessed infrequently. The data is now being used for a Business Intelligence application and you need better performance. What should you do? Select one.

- Create a new storage account with premium storage and copy the data there.
- Change the standard storage to premium storage.
- Create a general-purpose v2 account and use that for the data.
- Create a blob storage account and use that for the data.

Review Question 8

Your company requires all data to be encrypted with 256-bit AES encryption. What should you do? Select one.

- Enable storage service encryption.
- Enable customer managed keys.
- Enable shared access signatures.
- You do not need to do anything.

Review Question 9

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 10

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. Choose 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.

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

When you created a virtual machine you selected standard storage because the data was accessed infrequently. The data is now being used for a Business Intelligence application and you need better performance. What should you do? Select one.

- Create a new storage account with premium storage and copy the data there.
- Change the standard storage to premium storage.
- Create a general-purpose v2 account and use that for the data.
- Create a blob storage account and use that for the data.

Explanation

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.

Review Question 8

Your company requires all data to be encrypted with 256-bit AES encryption. What should you do? Select one.

- Enable storage service encryption.
- Enable customer managed keys.
- Enable shared access signatures.
- You do not need to do anything.

Explanation

Storage service encryption 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.

Review Question 9

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 10

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. Choose 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.

Module 4 Virtual Networking

Virtual Networks

Azure Networking Components

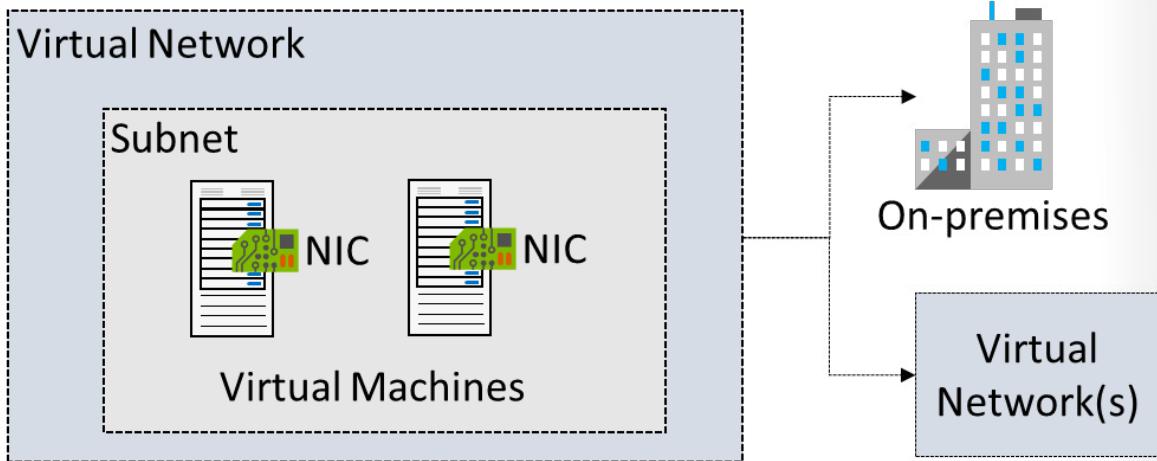
A major incentive for adopting cloud solutions such as Azure is to enable information technology (IT) departments to move server resources to the cloud. This can save money and simplify operations by removing the need to maintain expensive datacenters with uninterruptible power supplies, generators, 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.

 Networking Overview An integrated view of the networking services in Azure	 Content Delivery Network Ensure secure, reliable content delivery with broad global reach	 ExpressRoute Dedicated private network fiber connections to Azure
 Azure DNS Host your DNS domain in Azure	 Virtual Network Provision private networks, optionally connect to on-premises datacenters	 Traffic Manager Route incoming traffic for high performance and availability
 Load Balancer Deliver high availability and network performance to your applications	 VPN Gateway Establish secure, cross-premises connectivity	 Application Gateway Build secure, scalable, and highly available web front ends in Azure
 Azure DDoS Protection Protect your applications from Distributed Denial of Service (DDoS) attacks	 Network Watcher Network performance monitoring and diagnostics solution	 Azure Firewall Highly available and scalable cloud-based network security service
 Virtual WAN Build secure global scale branch connectivity	 Azure Front Door Service Scalable and secure entry point to deliver global web apps	

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.



You can use virtual networks to:

- **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.

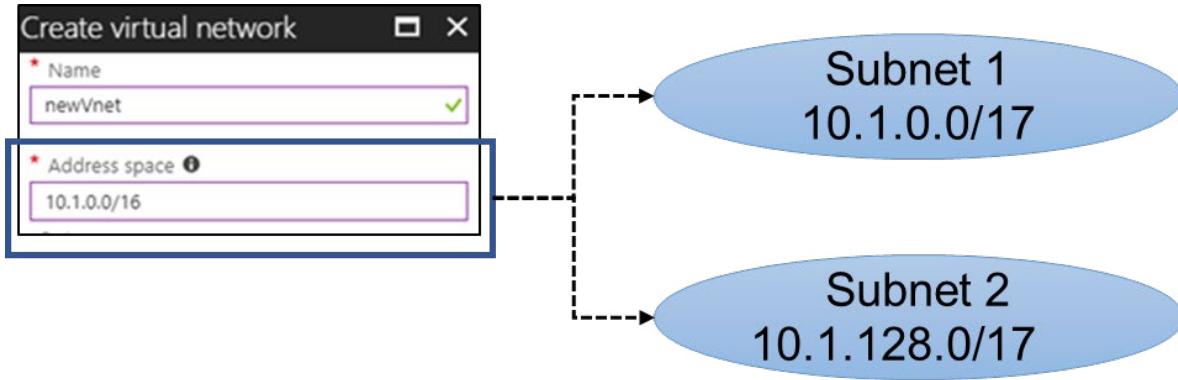
For more information:

Virtual Network Documentation - <https://docs.microsoft.com/en-us/azure/virtual-network/>

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.



It is important to carefully plan your subnets. Here are some things to think about.

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

* Name
newVNet ✓

* Address space ⓘ
10.1.0.0/16

Subnet

* Name
default

* Address range ⓘ
10.1.0.0/24 ✓
10.1.0.0 - 10.1.0.255 (256 addresses)

- ✓ 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
```

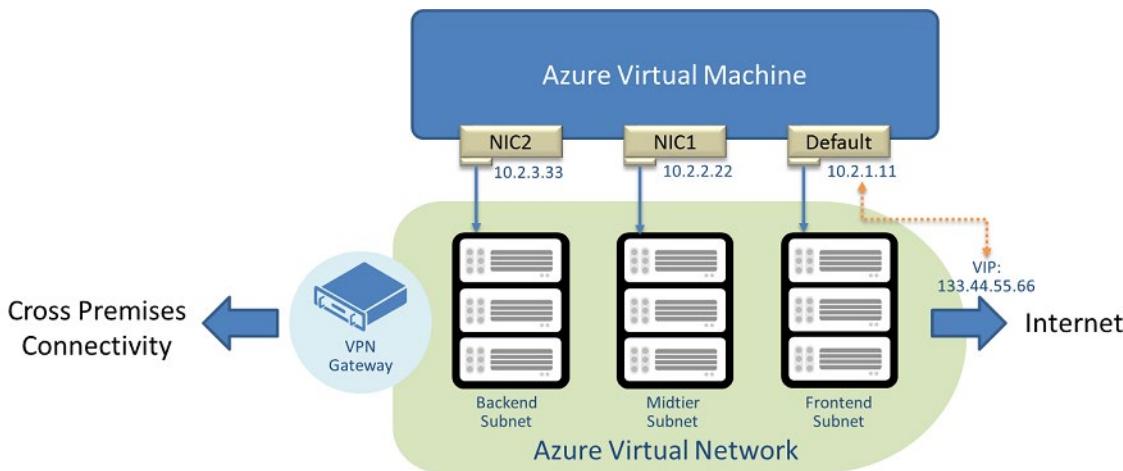
5. Associate the subnet to the virtual network.

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

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

Multiple NICs in Virtual Machines

You can create virtual machines in Azure and attach multiple network interfaces (NICs) to each of your VMs. Having multiple NICs is a requirement for many network virtual appliances, such as application delivery and WAN optimization solutions. Having multiple NICs also provides more network traffic management functionality, including isolation of traffic between a front-end NIC and back-end NIC(s), or separation of data plane traffic from management plane traffic.



The figure above shows a VM with three NICs, each connected to a different subnet.

- The order of the NICs from inside the VM will be random and could also change across Azure infrastructure updates. However, the IP addresses, and the corresponding ethernet MAC addresses will remain the same. For example, assume Eth1 has IP address 10.1.0.100 and MAC address 00-0D-3A-B0-39-0D; after an Azure infrastructure update and reboot, it could be changed to Eth2, but the IP and MAC pairing will remain the same. When a restart is customer-initiated, the NIC order will remain the same.
- The address for each NIC on each VM must be in a subnet and multiple NICs on a single VM can each be assigned addresses that are in the same subnet.
- The VM size determines the number of NICs that you can create for a VM.

Here are some things to consider when using multiple NICs.

- To add a virtual NIC to an existing VM, you deallocate the VM, add the virtual NIC, then start the VM.

- To remove a virtual NIC from an existing VM, you deallocate the VM, remove the virtual NIC, then start the VM.
- You can associate multiple NICs on a VM to multiple subnets, but those subnets must all reside in the same virtual network (vNet).

Demonstration - Create VMs with Multiple NICs

In this demonstration, you will learn how to create and configure multiple NICs and then attach those NICs to a VM. You can replace example parameter names with your own values if you prefer.

This demonstration uses the Azure CLI and assumes the following preparatory steps:

1. You are using the latest version of the **Azure CLI**¹ and are logged in to your Azure account.
2. You have created a resource group in an appropriate location and a virtual network with a subnet, an additional backend subnet, and a network security group. For example, using **az network vnet create**, create a virtual network named *myVnet* and subnet named *mySubnetFrontEnd*:

```
az network vnet create \
--resource-group myResourceGroup \
--name myVnet \
--address-prefix 10.0.0.0/16 \
--subnet-name mySubnetFrontEnd \
--subnet-prefix 10.0.1.0/24
```

3. Using **az network vnet subnet create** create a subnet for the back-end traffic named *mySubnetBackEnd*:

```
az network vnet subnet create \
--resource-group myResourceGroup \
--vnet-name myVnet \
--name mySubnetBackEnd \
--address-prefix 10.0.2.0/24
```

4. Now using **az network nsg create**, create a network security group named *myNetworkSecurityGroup*:

```
az network nsg create \
--resource-group myResourceGroup \
--name myNetworkSecurityGroup
```

Create and configure multiple NICs

- Using **az network nic create**, create two NICs, named *myNic1* and *myNic2*, connect the network security group,

with one NIC connecting to each subnet:

```
az network nic create \
--resource-group myResourceGroup \
--name myNic1 \
--vnet-name myVnet \
--subnet mySubnetFrontEnd \
--network-security-group myNetworkSecurityGroup
```

¹ <https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest>

```
az network nic create \
--resource-group myResourceGroup \
--name myNic2 \
--vnet-name myVnet \
--subnet mySubnetBackend \
--network-security-group myNetworkSecurityGroup
```

Create a VM and attach the NICs

- When you create the VM, specify the NICs you created with the `--nics` parameter. You also need to take care when you select the VM size. There are limits for the total number of NICs that you can add to a VM. Using **az vm create**, create a Linux VM named *myVM*:

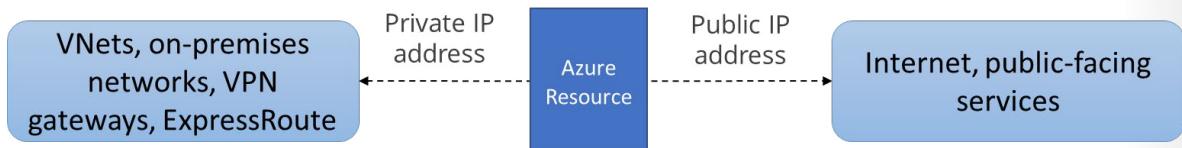
```
az vm create \
--resource-group myResourceGroup \
--name myVM \
--image UbuntuLTS \
--size Standard_DS3_v2 \
--admin-username azureuser \
--generate-ssh-keys \
--nics myNic1 myNic2
```

Note: Return to the portal and verify the virtual machine now has two interfaces.

IP Addressing and Endpoints

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.

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.

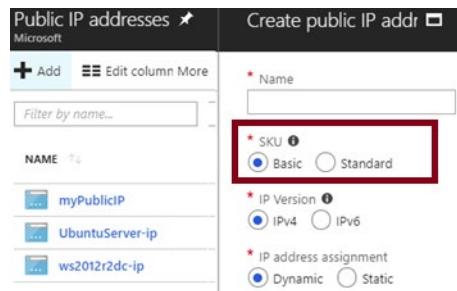
Public IP Addresses

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways. Azure can provide an IP address (dynamic assignment) or you can assign the IP address (static assignment). The type of resource affects the assignment.

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	No
Application Gateway	Front-end configuration	Yes	No

Address SKUs

When you create a public IP address you are given a SKU choice of either Basic or Standard.



Your SKU choice affects the IP assignment method, security, available resources, and redundancy. This table summarizes the differences.

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

Private IP Addresses

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

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

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

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

Demonstration - Manage IP Addresses

In this demonstration, you will learn how to retrieve static private IP address information for a network interface.

Note: You will need a VM to run these commands. These commands will work on the virtual networks created in the previous lesson. If you did not do that demonstration, substitute values for your situation.

Retrieve static private IP address information

- To view the static private IP address information for a VM, run the following PowerShell command and note the values for *PrivateIpAddress* and *PrivateIpAllocationMethod*:


```
Get-AzNetworkInterface -Name myNic1 -ResourceGroupName myResourceGroup
```
- Review the information returned which includes: Name, ResourceGroupName, Location, Id, ProvisioningState, VirtualMachine, IpConfigurations, DnsSettings, EnableIPForwarding, and NetworkSecurityGroup. The information also includes whether the NIC is primary.
- Notice in the IpConfigurations area there is a PrivateIPAddress and the PrivateIpAllocationMethod is static.

Remove a static private IP address - change to dynamic

- To remove the static private IP address, run the following PowerShell commands:

```
# Retrieve the NIC information
$nic=Get-AzNetworkInterface -Name myNic1 -ResourceGroupName myResourceGroup

# Change to the Dynamic allocation method
$nic.IpConfigurations[0].PrivateIpAllocationMethod = "Dynamic"

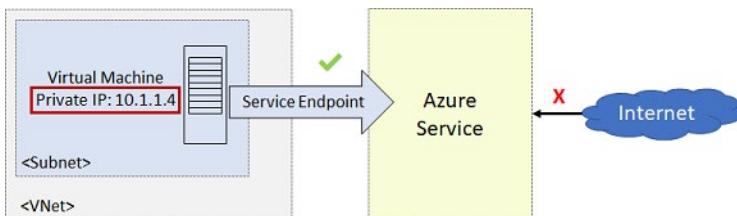
# Implement your changes
Set-AzNetworkInterface -NetworkInterface $nic
```

- Review the output.
- Notice in the IpConfigurations area, The PrivateIPAllocationMethod is now Dynamic.

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?

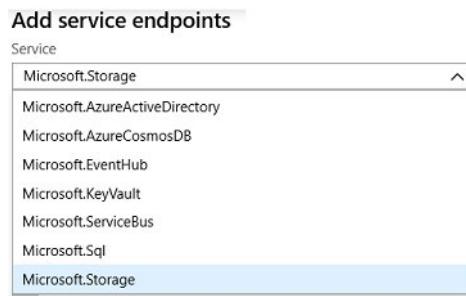
- Improved security for your Azure service resources.** VNet private address space can be overlapping and so, cannot be used to uniquely identify traffic originating from your VNet. Service endpoints provide the ability to secure Azure service resources to your virtual network, by extending VNet identity 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.

Azure Data Lake Store Gen 1. Generally available in all Azure regions where ADLS Gen1 is available. This feature helps to secure your Data Lake Storage account from external threats.

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

Secure Access to 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	SUBSCRIPTION
MyVNet1	1	10.1.0.0/24	Enabled	StorageFWTest	...
	MySubnet1	10.1.0.0/24	Enabled	StorageFWTest	...

ADDRESS RANGE	
16.17.18.0/24	...

- ✓ It is important to test and ensure the service endpoint is limiting access as expected.

Demonstration - Service Endpoints

In this demonstration, you will work with virtual network endpoints.

Note: This demonstration requires a Storage Account with an uploaded file.

Note: You could use Storage Explorer (Preview) in the portal.

Create a storage account

1. Create a **Storage Account**.

2. Within the Storage Account, create a **file share**, and **upload** a file.
3. For the Storage Account, use the **Shared Access Signature** blade to **Generate SAS and connection string**.
4. Use Storage Explorer and the connection string to access the file share.
5. 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
```

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.

Azure DNS

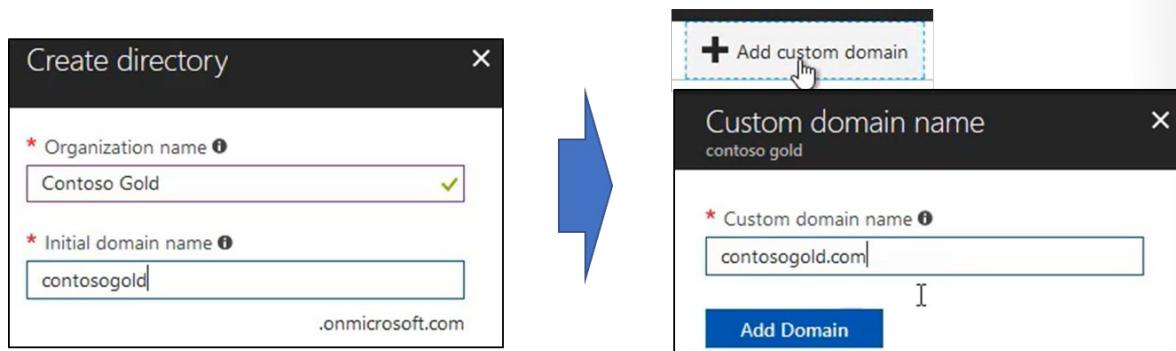
Domains and Custom Domains

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

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.

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.

- ✓ 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.

NAME	NUMBER OF RECORDS	RESOURCE GROUP	LOCATION	SUBSCRIPTION	NAME SERVERS
adatum.net	2 / 5000	adatumDNS	global	Microsoft Azure In...	ns1-05.azure-dns.c... ns1-04.azure-dns.c...
gwcontoso.com	3 / 5000	gwcontoso	global	Microsoft Azure In...	ns1-04.azure-dns.c...

When creating a DNS zone in Azure DNS remember:

- 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.

For more information:

DNS Zones - <https://docs.microsoft.com/en-us/azure/dns/dns-zones-records#dns-zones>

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.

Record set Move Delete zone Refresh

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 queried.

Add record set

contoso1.com

Name:

Type:

Alias record set (?)
 Yes No

* TTL: TTL unit:

IP ADDRESS: ...

OK

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 portal interface for managing a DNS zone. At the top, there are buttons for 'Record set', 'Move', 'Delete zone', and 'Refresh'. Below these are sections for 'Resource group (change)', 'Subscription (change)', and 'Subscription ID'. The 'Name server' section is highlighted with a red box and contains the following entries:

- Name server 1
ns1-08.azure-dns.com.
- Name server 2
ns2-08.azure-dns.net.
- Name server 3
ns3-08.azure-dns.org.
- Name server 4
ns4-08.azure-dns.info.

You can also discover the NS records with PowerShell, use `Get-AzDnsZone` and `Get-AzDnsRecordSet`. Note that the record name "@" is used to refer to records at the apex of the zone.

```
# Retrieve the zone information
$zone = Get-AzDnsZone -Name contoso.net -ResourceGroupName MyResourceGroup

# Retrieve the name server records
Get-AzDnsRecordSet -Name "@" -RecordType NS -Zone $zone
```

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 following PowerShell example demonstrates how this works. The same steps can be executed via the Azure Portal, or via the cross-platform Azure CLI.

```
# Create the parent zone
$parent = New-AzDnsZone -Name contoso.com -ResourceGroupName RG1

# Create the child zone
$child = New-AzDnsZone -Name partners.contoso.com -ResourceGroupName RG1

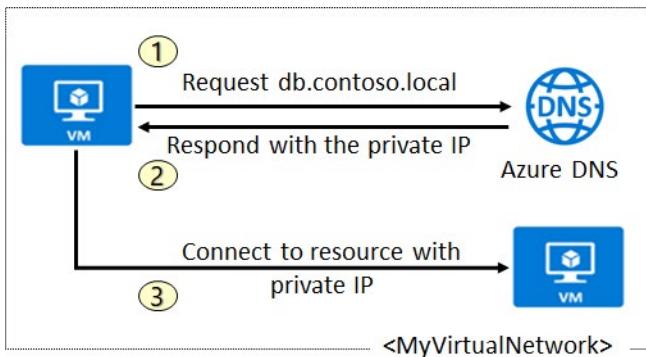
# Retrieve NS records for the child zone
$child_ns_recordset = Get-AzDnsRecordSet -Zone $child -Name "@" -RecordType NS

# Create the NS record set in the parent zone.
$parent_ns_recordset = New-AzDnsRecordSet -Zone $parent -Name "partners" -RecordType NS -Ttl 3600
$parent_ns_recordset.Records = $child_ns_recordset.Records
Set-AzDnsRecordSet -RecordSet $parent_ns_recordset
```

- ✓ 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 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 provides the many benefits:

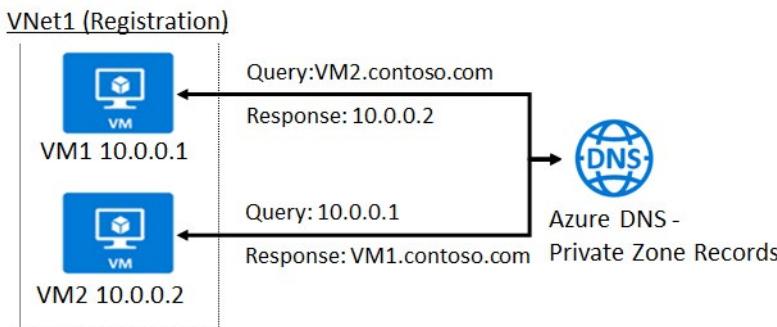
- **Removes the need for custom DNS solutions.** Previously, many customers created custom DNS solutions to manage DNS zones in their virtual network. You can now perform DNS zone management by using the native Azure infrastructure, which removes the burden of creating and managing custom DNS solutions.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

- ✓ At the time of this writing, the Azure DNS Private Zone feature is currently in public preview. This preview version is provided without a service level agreement, and is not recommended for production workloads.

Private Zones Scenarios

Scenario: 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.

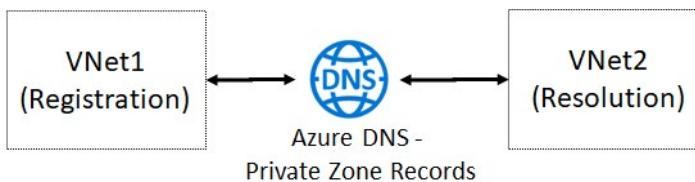


In this scenario, VNET1 contains two VMs (VM1 and VM2). Each of these VMs have Private IPs. So, if you create a Private Zone named contoso.com and link this virtual network as a Registration virtual network, Azure DNS will automatically create two A records in the zone. Now, DNS queries from VM1 to resolve 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: 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 functionality²** 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.

² <https://docs.microsoft.com/en-us/azure/dns/private-dns-scenarios#scenario-split-horizon-functionality>

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
```

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:

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

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	Location	Subscription	Associated with
ASH	South Central US	Visual Studio Enterprise	0 subnets, 1 network interfaces

- ✓ 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 Groups - <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#network-security-groups>³

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.

³ <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

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

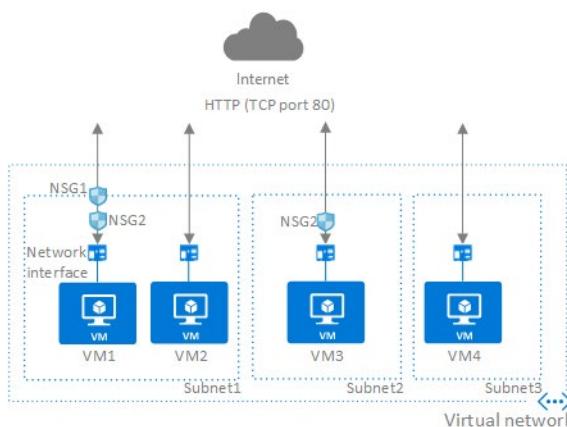
VM1-nsg - Inbound security rules						
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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

VM1-nsg - Outbound security rules						
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

NSG Effective Rules

Be cautious when you want to apply NSG to both VM (NIC) and subnet level at the same time. 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.

The screenshot shows the 'Add inbound security rule' dialog for a network security group named 'UbuntuServer-nsg'. The 'Advanced' tab is selected. The configuration includes:

- Service:** Custom (selected)
- Port ranges:** 8080
- Priority:** 310
- Name:** Port_8080

A vertical list of predefined services is shown on the right, with 'Custom' selected. Other options include HTTP, HTTPS, SSH, RDP, MS SQL, MySQL, PostgreSQL, FTP, SMTP, DNS (TCP), and DNS (UDP). A blue arrow points from the 'Custom' selection in the list to the 'Custom' dropdown in the dialog.

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?

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.

MCT USE ONLY. STUDENT USE PROHIBITED

3. If you have virtual machines, you may already have NSGs. Notice the ability to filter the list.

Add a new NSGs

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.

Lab and Review Questions

Lab - Configure Azure DNS

Scenario

Adatum Corporation wants to implement public and private DNS service in Azure without having to deploy its own DNS servers.

Objectives

After completing this lab, you will be able to:

- Configure Azure DNS for public domains.
- Configure Azure DNS for private domains.

Exercise 1: Configure Azure DNS for public domains.

The main tasks for this exercise are as follows:

- Create a public DNS zone.
- Create a DNS record in the public DNS zone.
- Validate Azure DNS-based name resolution for the public domain.

Result: After you completed this exercise, you have created a public DNS zone, created a DNS record in the public DNS zone, and validated Azure DNS-based name resolution for the public domain.

Exercise 2: Configure Azure DNS for private domains.

The main tasks for this exercise are as follows:

- Provision a multi-virtual network environment.
- Create a private DNS zone.
- Deploy Azure VMs into virtual networks.
- Validate Azure DNS-based name reservation and resolution for the private domain.

Result: After completing this exercise, you have provisioned a multi-virtual network environment, created a private DNS zone, deployed Azure VMs into virtual networks, and validated Azure DNS-based name reservation and resolution for the private domain.

Module 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 have several VMs in Microsoft Azure. All the VMs are configured with the default IP addressing solution. A VM named VM1 is assigned the 172.16.10.100 IP address. You stop and deallocate VM1 to perform some disk maintenance activities. During that time, another administrator deploys a new VM named VM25. Later, after VM1 comes back online, you notice that its IP address changed. Now, VM25 is assigned the 172.16.10.100 IP address. You need to ensure that VM1 maintains the IP address of 172.16.10.100. All other VMs should have their IP addresses automatically allocated. What should you do? (Each answer presents part of the solution. Choose two.)

- Stop and deallocate VM1.
- Start VM1.
- Stop and deallocate VM25.
- Start VM25.
- Configure VM1 with a static IP address of 172.16.10.100.
- Configure VM25 with a new static IP address.

Review Question 8

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 9

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 10

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

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 have several VMs in Microsoft Azure. All the VMs are configured with the default IP addressing solution. A VM named VM1 is assigned the 172.16.10.100 IP address. You stop and deallocate VM1 to perform some disk maintenance activities. During that time, another administrator deploys a new VM named VM25. Later, after VM1 comes back online, you notice that its IP address changed. Now, VM25 is assigned the 172.16.10.100 IP address. You need to ensure that VM1 maintains the IP address of 172.16.10.100. All other VMs should have their IP addresses automatically allocated. What should you do? (Each answer presents part of the solution. Choose two.)

- Stop and deallocate VM1.
- Start VM1.
- Stop and deallocate VM25.
- Start VM25.
- Configure VM1 with a static IP address of 172.16.10.100.
- Configure VM25 with a new static IP address.

Explanation

Because VM25 has the 172.16.10.100 address, you need to stop the VM to release the address. After the address is released, you can statically assign it to VM1. Thereafter, VM1 will maintain that IP address.

Review Question 8

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 9

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 10

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.

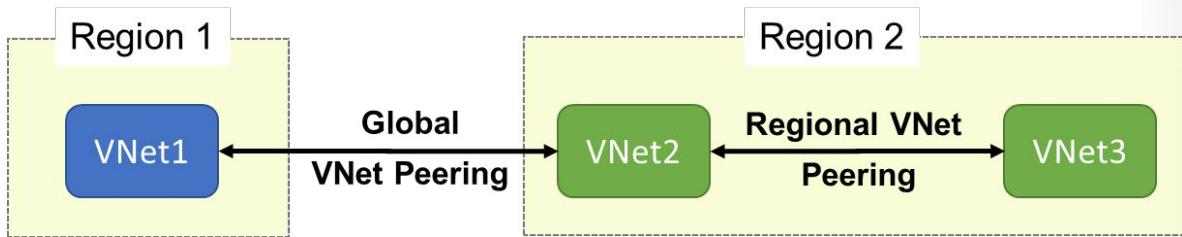
Module 5 Intersite Connectivity

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.

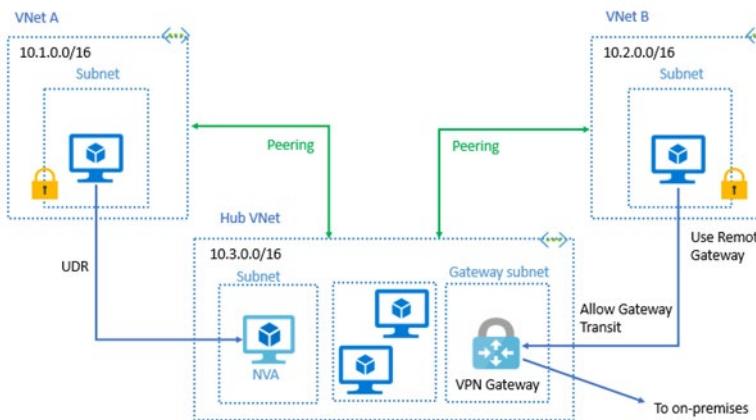
- **Cloud regions.** When creating a global peering, the peered virtual networks can exist in any Azure public cloud region or China cloud regions, but not in Government cloud regions. You can only peer virtual networks in the same region in Azure Government cloud regions.
- **Virtual network resources.** 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 peering - <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

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.

- ✓ 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.

Add peering
vnet1

Configuration

Configure virtual network access settings

Allow virtual network access from vnet1 to remote virtual network ⓘ

Disabled Enabled

Allow virtual network access from remote virtual network to vnet1 ⓘ

Disabled Enabled

Configure forwarded traffic settings

Allow forwarded traffic from remote virtual network to vnet1 ⓘ

Disabled Enabled

Allow forwarded traffic from vnet1 to remote virtual network ⓘ

Disabled Enabled

Configure gateway transit settings

Allow gateway transit ⓘ

- **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

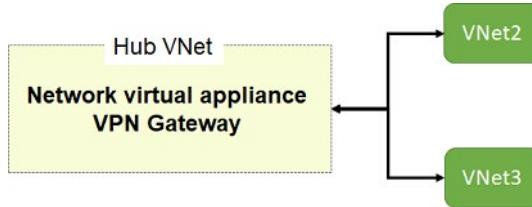
VNet Peering is nontransitive. This means that if you establish VNet Peering between VNet1 and VNet2 and between VNet2 and VNet3, VNet Peering capabilities do not apply between VNet1 and VNet3.

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	myVirtualNetwork1-myVirtualNetwork2	Updating	myVirtualNetwork2	Disabled
Peering				

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.

For more information:

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

How to create a hub and spoke network topology - <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?toc=%2fazure%2fvirtual-network%2ftoc.json>

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

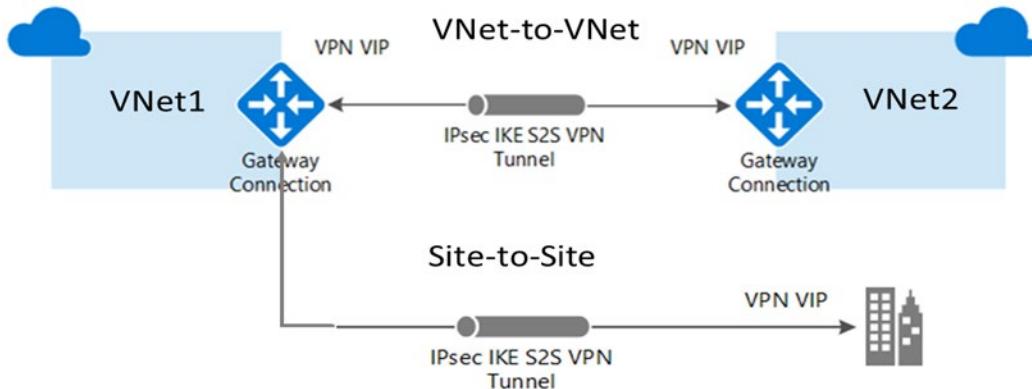
1. In the **Azure portal**, select the second virtual network.
2. Under **SETTINGS**, select **Peerings**.

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.

VNet-to-VNet Connections

VNet-to-VNet Connections

You can connect your VNets with a VNet-to-VNet VPN connection. Using this connection method, you create a VPN gateway in each virtual network. A secure tunnel using **IPsec/IKE¹** provides the communication between the networks.



With a VNet-to-VNet connection your VNets can be:

- in the same or different regions.
- in the same or different subscriptions.
- in the same or different deployment models.
- in Azure or on-premises.

Benefits

Cross region geo-redundancy and geo-presence

- You can set up your own geo-replication or synchronization with secure connectivity without going over Internet-facing endpoints.
- With Azure Traffic Manager and Load Balancer, you can set up highly available workload with geo-redundancy across multiple Azure regions.

Regional multi-tier applications with isolation or administrative boundary

- Within the same region, you can set up multi-tier applications with multiple virtual networks connected together due to isolation or administrative requirements.
- VNet-to-VNet communication can be combined with multi-site configurations. This lets you establish network topologies that combine cross-premises connectivity with inter-virtual network connectivity.
- ✓ You will use VNet-to-VNet connections when you cannot use VNet peering.
- ✓ Connections to on-premises virtual networks are called Site-to-Site (S2S) connections.

For more information:

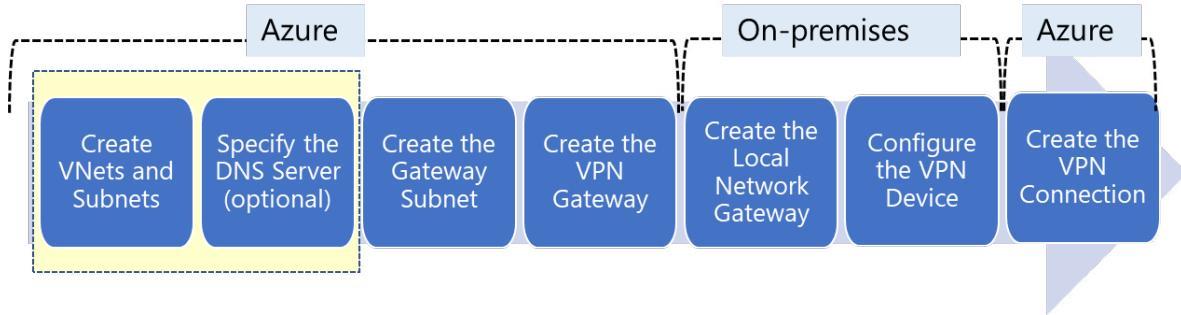
VNet-to-VNet Connectivity - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal#vnet-to-vnet>

¹ <https://docs.microsoft.com/en-us/windows/desktop/FWP/ipsec-configuration>

Site-to-Site Connectivity - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-how-to-site-to-site-resource-manager-portal>

Implement VNet-to-VNet 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.



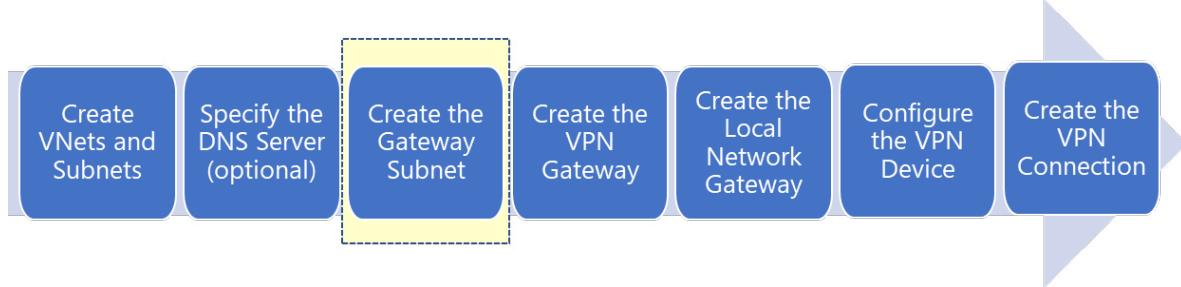
Create VNets and subnets. By now you should be familiar with creating virtual networks and subnets. Remember for this VNet to connect to an on-premises location. You need to coordinate with your on-premises network administrator to reserve an IP address range that you can use specifically for this virtual 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.

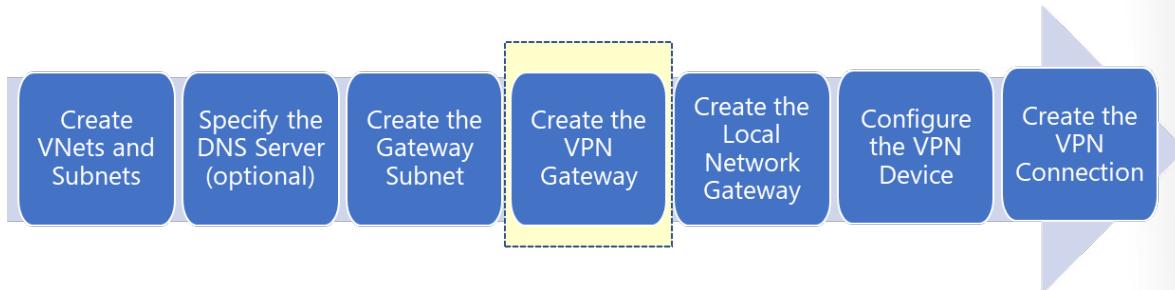
When you create your gateway subnet, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings. You must never deploy other resources (for example, additional VMs) to the gateway subnet. The gateway subnet must be named *GatewaySubnet*.

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

The screenshot shows the 'Subnets' blade in the Azure portal. At the top, there are two buttons: '+ Subnet' and '+ Gateway subnet'. The '+ Gateway subnet' button is highlighted with a red box. Below these buttons is a search bar labeled 'Search subnets'. The main table lists one subnet named 'default' with the address range '10.1.0.0/24' and available addresses '251'. There is also a column for 'SECURITY GROUP' which is currently empty.

- ✓ 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.

Create the VPN Gateway



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.

The screenshot shows the 'Create virtual network gateway' wizard. The first step is 'Create a virtual network gateway'. It includes fields for 'Name' (set to 'VGateway1'), 'SKU' (set to 'VpnGw1'), 'Gateway type' (radio button selected for 'VPN'), 'VPN type' (radio button selected for 'Route-based'), 'Virtual network' (button to 'Choose a virtual network'), and 'Public IP address' (radio button selected for 'Create new').

- **Name and Gateway Type.** Name your gateway and use the VPN Gateway type.
- **VPN Type.** Most VPN types are Route-based.
- **SKU.** Use the drop-down to select a gateway SKU. Your choice will affect the number of tunnels you can have and the aggregate throughput benchmark. The benchmark is based on measurements of

multiple tunnels aggregated through a single gateway. It is not a guaranteed throughput due to Internet traffic conditions and your application behaviors.

- **Virtual Networks.** Associate a virtual network with the gateway. Before you do this, you must configure the Gateway subnet. Each virtual network will need its own VPN gateway.
- **Public IP Address.** The gateway needs a public IP address to enable it to communicate with the remote network. Make a note of this information. You will need the address when you configure your VPN device.

It can take up to 45 minutes to provision the VPN 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. In this last step you will create a connection for the device.

VPN 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

There are two VPN types:

- **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.
- **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).

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

Gateway SKUs

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.

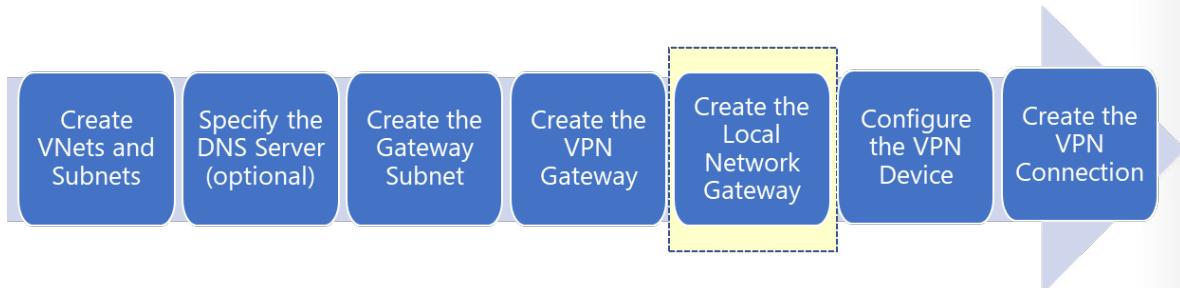
SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2 Connections	Aggregate Throughput Benchmark
Basic	Max. 10	Max. 128	Not Supported	100 Mbps
VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps
VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps
VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps

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.

These connection limits are separate. For example, you can have 128 SSTP connections and also 250 IKEv2 connections on a VpnGw1 SKU.

- ✓ The Basic SKU is considered a legacy SKU. The Basic SKU has certain feature limitations. You can't resize a gateway that uses a Basic SKU to one of the new gateway SKUs, you must instead change to a new SKU, which involves deleting and recreating your VPN gateway.

Create the Local Network Gateway



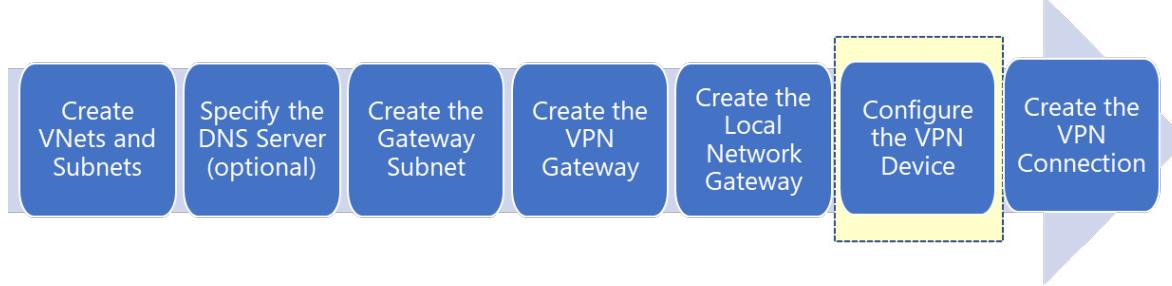
The local network gateway typically refers to the on-premises location. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device for the connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located in the on-premises network.

The screenshot shows the 'Create local network gateway' configuration page. It includes fields for 'Name' (set to 'VNet1LocalNet'), 'IP address' (set to '33.2.1.5'), and 'Address space' (set to '192.168.3.0/24'). There are also 'Add additional address range' and '...' buttons.

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.

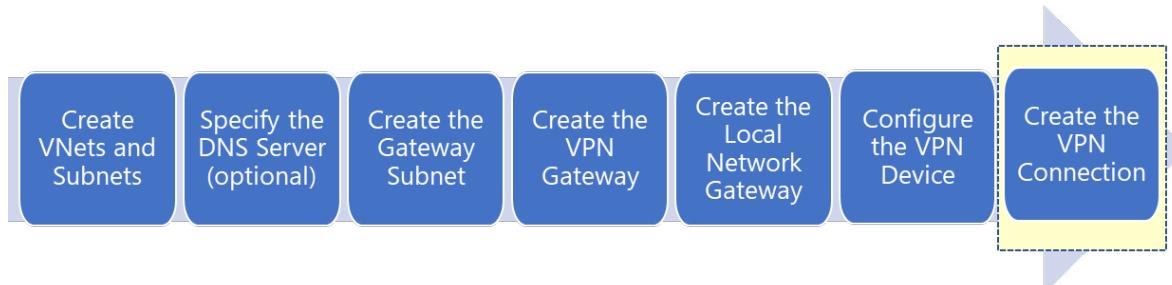
To configure your VPN device, you need the following:

- **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 list - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#devicetable³>

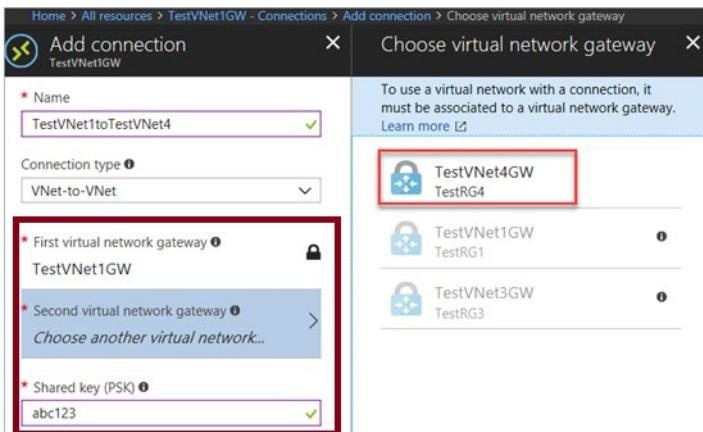
Create the VPN Connection



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

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

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.



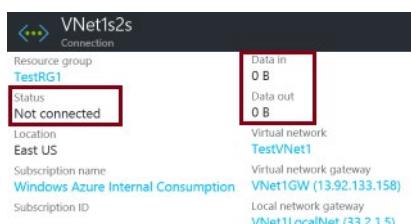
- **Name.** Enter a name for your connection.
- **Connection type.** Select VNet-to-VNet from the drop-down.
- **First virtual network gateway.** This field value is automatically filled in because you're creating this connection from the specified virtual network gateway.
- **Second virtual network gateway.** This field is the virtual network gateway of the VNet that you want to create a connection to.
- **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.
- ✓ If your VNets are in different subscriptions, you must use PowerShell to make the connection. You can use the New-AzVirtualNetworkGatewayConnection.

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.

Portal

When you view your connection in the Azure portal the Status should be Succeeded or Connected. Also, you should have data flowing in the Data in and Data out information.



PowerShell

To verify your connection with PowerShell, use the Get-AzVirtualNetworkGatewayConnection cmdlet. For example,

```
Get-AzVirtualNetworkGatewayConnection -Name MyGWConnection -ResourceGroupName MyRG
```

After the cmdlet has finished, review the values. The connection status should show 'Connected' and there will be information on ingress and egress bytes.

```
"connectionStatus": "Connected",
"ingressBytesTransferred": 33509044,
"egressBytesTransferred": 4142431
```

Demonstration - VNet to VNet Connections

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.

VNet1 - Connected devices			
DEVICE	TYPE	IP ADDRESS	SUBNET
vm2858	Network interface	10.0.1.4	Subnet2
vm2512	Network interface	10.0.1.5	Subnet2
vm152	Network interface	10.0.0.4	Subnet1
vm1448	Network interface	10.0.0.5	Subnet1
vnet1	Virtual network gateway	-	GatewaySubnet

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

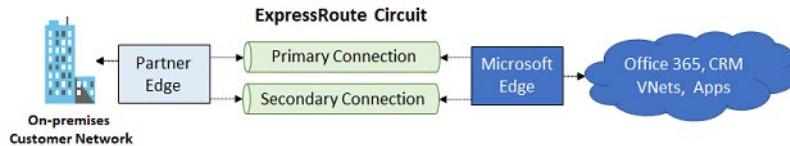
1. Search for **Connections**.
2. Click **+ Add**.
3. Notice the **Connection type** can be VNet-to-VNet, Site-to-Site (IPsec), or ExpressRoute.
4. Provide enough information, so you can click the **Ok** button.
5. On the **Settings** page, notice that you will need select the two different virtual networks.
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.

MCT USE ONLY. STUDENT USE PROHIBITED

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

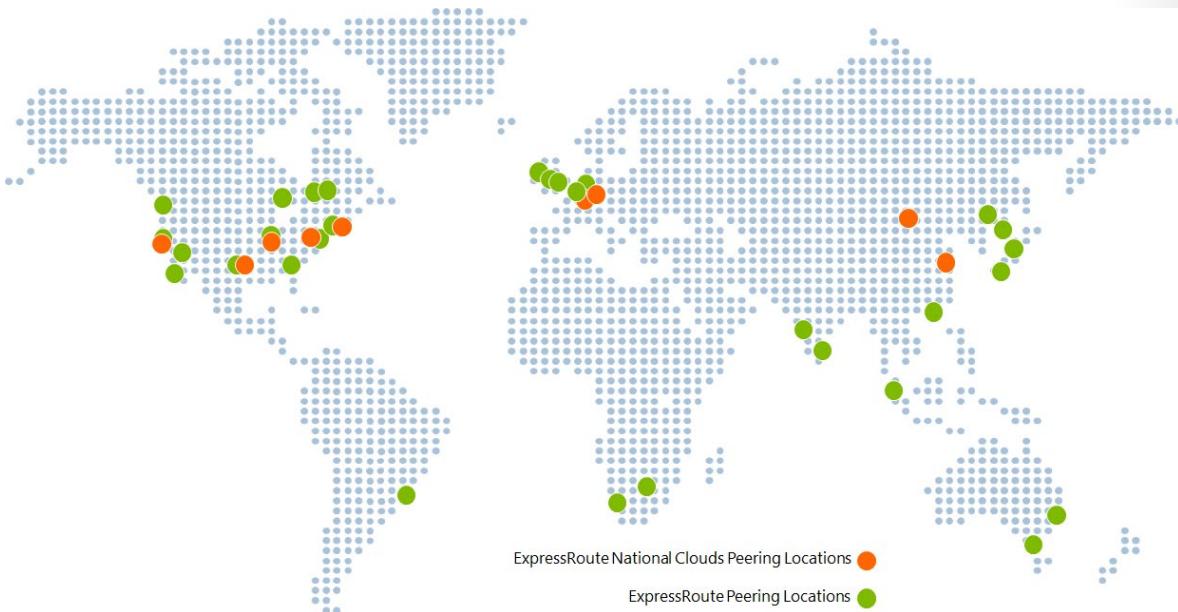
With predictable, reliable, and high-throughput connections offered by ExpressRoute, build applications that span on-premises infrastructure and Azure without compromising privacy or performance. For example, run a corporate intranet application in Azure that authenticates your customers with an on-premises Active Directory service, and serve all of your corporate customers without traffic ever routing through the public Internet.

For more information:

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

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.



There are many benefits to using ExpressRoute.

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**⁴.

Connectivity to all regions within a geopolitical region

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

⁴ <https://docs.microsoft.com/en-us/office365/enterprise/azure-expressroute>

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.

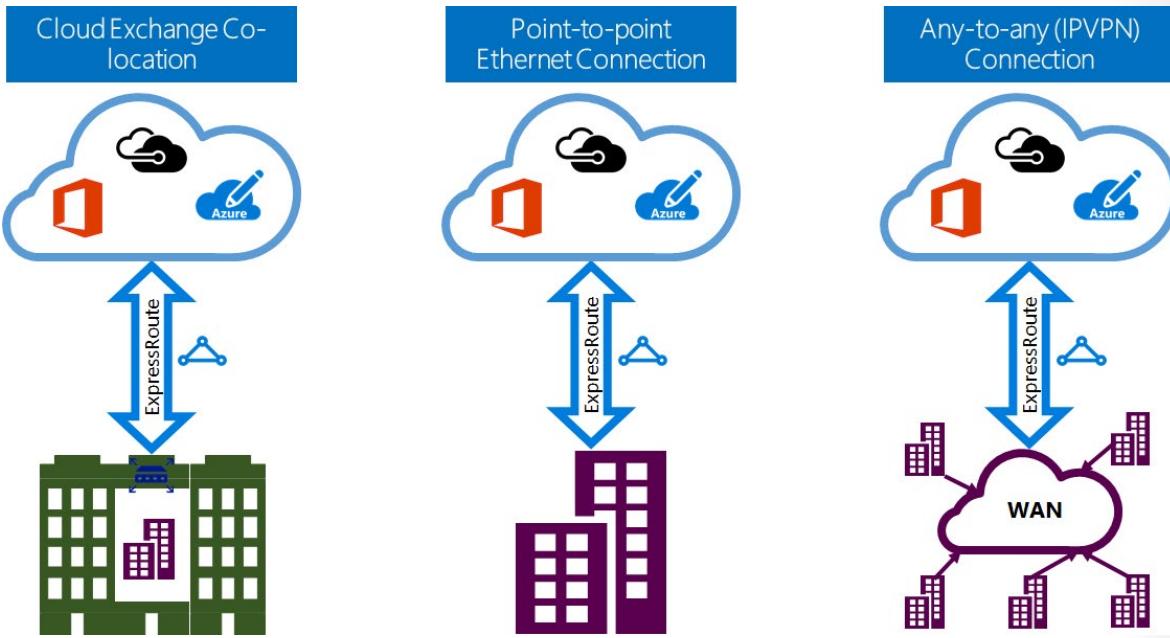
- **Unlimited data.** Billing is based on a monthly fee; all inbound and outbound data transfer is included free of charge.
- **Metered data.** Billing is based on a monthly fee; all inbound data transfer is free of charge. Outbound data transfer is charged per GB of data transfer. Data transfer rates 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.

For more information:

FAQ - Azure ExpressRoute - <https://docs.microsoft.com/en-us/azure/expressroute/express-route-faqs>

ExpressRoute Connections

You can create a connection between your on-premises network and the Microsoft cloud in three different ways, CloudExchange Co-location, 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.



CloudExchange Co-location

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.

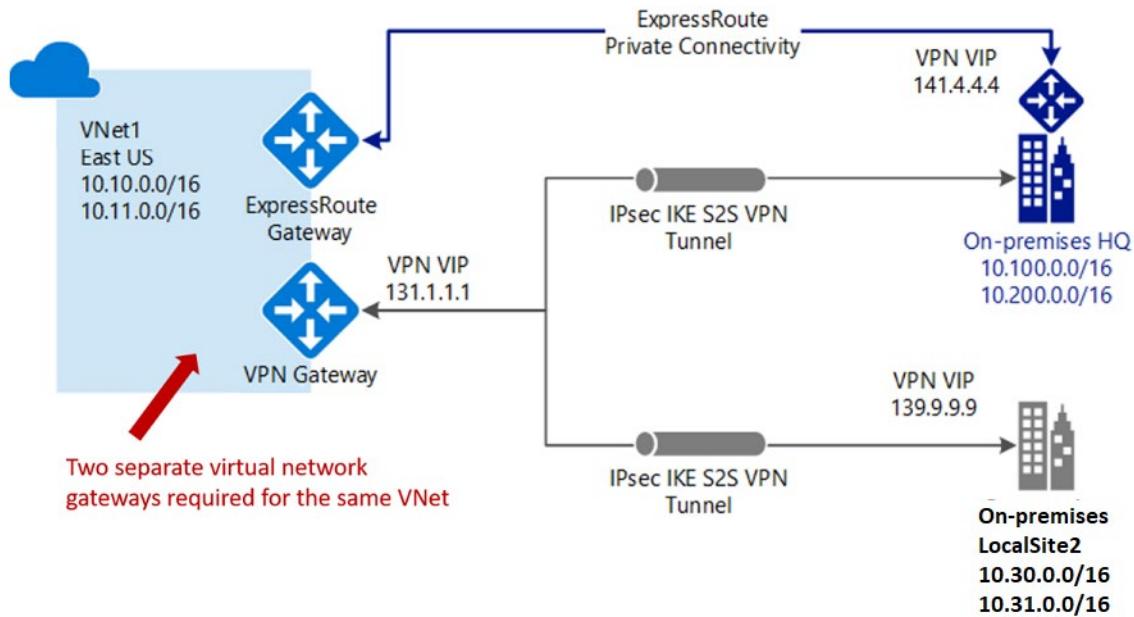
- ✓ ExpressRoute capabilities and features are all identical across all the above connectivity models.

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



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

Lab and Review Questions

Lab - VNet Peering and Service Chaining

Scenario

ADatum Corporation wants to implement service chaining between Azure virtual networks in its Azure subscription.

Objectives

After completing this lab, you will be able to:

- Create Azure virtual networks and deploy Azure VM by using Azure Resource Manager templates.
- Configure VNet peering.
- Implement custom routing.
- Validate service chaining.

Exercise 0: Prepare the Azure environment.

The main tasks for this exercise are as follows:

- Create the first virtual network hosting two Azure VMs by using an Azure Resource Manager template.
- Create the second virtual network in the same region hosting a single Azure VM by using an Azure Resource Manager template.

Result: After you completed this exercise, you have created two Azure virtual networks and initiated deployments of three Azure VM by using Azure Resource Manager templates.

Exercise 1: Configure VNet peering.

The main tasks for this exercise are as follows:

- Configure VNet peering for the first virtual network.
- Configure VNet peering for the second virtual network.

Result: After you completed this exercise, you have configured virtual network peering between the two virtual networks.

Exercise 2: Implement custom routing.

The main tasks for this exercise are as follows:

- Enable IP forwarding for a network interface of an Azure VM.
- Configure user defined routing.
- Configure routing in an Azure VM running Windows Server 2016.

Result: After completing this exercise, you have implemented custom routing between peered Azure virtual networks.

Exercise 3: Validating service chaining

The main tasks for this exercise are as follows:

- Configure Windows Firewall with Advanced Security on the target Azure VM.
- Test service chaining between peered virtual networks.

Result: After you completed this exercise, you have validated service chaining between peered Azure virtual networks.

Module Review Questions

Review Question 1

When establishing connections between virtual networks with VNet-to-VNet VPN connections, your virtual networks cannot be _____. Select one.

- in different regions.
- in Azure.
- in the cloud using a dedicated private connection.
- in the same deployment model.
- in different subscriptions.

Review Question 2

Which two statements regarding an Azure VPN gateway are true?

- 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 3

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? (Choose two)

- The virtual networks can exist in any Azure cloud region.
- Security: 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 4

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. Choose 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 5

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 6

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.

Review Question 7

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?

- 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 8

The _____ routes traffic between VMs and PaaS cloud services in a virtual network and computers at the other end of the connection. Select one.

- VPN gateway
- server
- DNS
- load balancer
- local gateway

Review Question 9

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 10

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.

Answers

Review Question 1

When establishing connections between virtual networks with VNet-to-VNet VPN connections, your virtual networks cannot be _____. Select one.

- in different regions.
- in Azure.
- in the cloud using a dedicated private connection.
- in the same deployment model.
- in different subscriptions.

Explanation

The exception in the list of options is that a dedicated private connection is part of ExpressRoute and must be facilitated by a connectivity partner. ExpressRoute is not generally available to everybody and is used where there is a need for extremely fast connectivity with low latency.

Review Question 2

Which two statements regarding an Azure VPN gateway are true?

- 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 3

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? (Choose two)

- The virtual networks can exist in any Azure cloud region.
- Security: 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 4

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. Choose 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 (which you don't already have as part of the scenario) 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 5

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 6

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 7

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?

- 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 8

The _____ routes traffic between VMs and PaaS cloud services in a virtual network and computers at the other end of the connection. Select one.

- VPN gateway
- server
- DNS
- load balancer
- local gateway

Explanation

Whenever you want to connect to an Azure virtual network, you must provision a VPN gateway in Azure. The VPN gateway routes traffic between VMs and PaaS cloud services in the virtual network, and computers at the other end of the connection.

Review Question 9

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 10

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.

Module 6 Monitoring

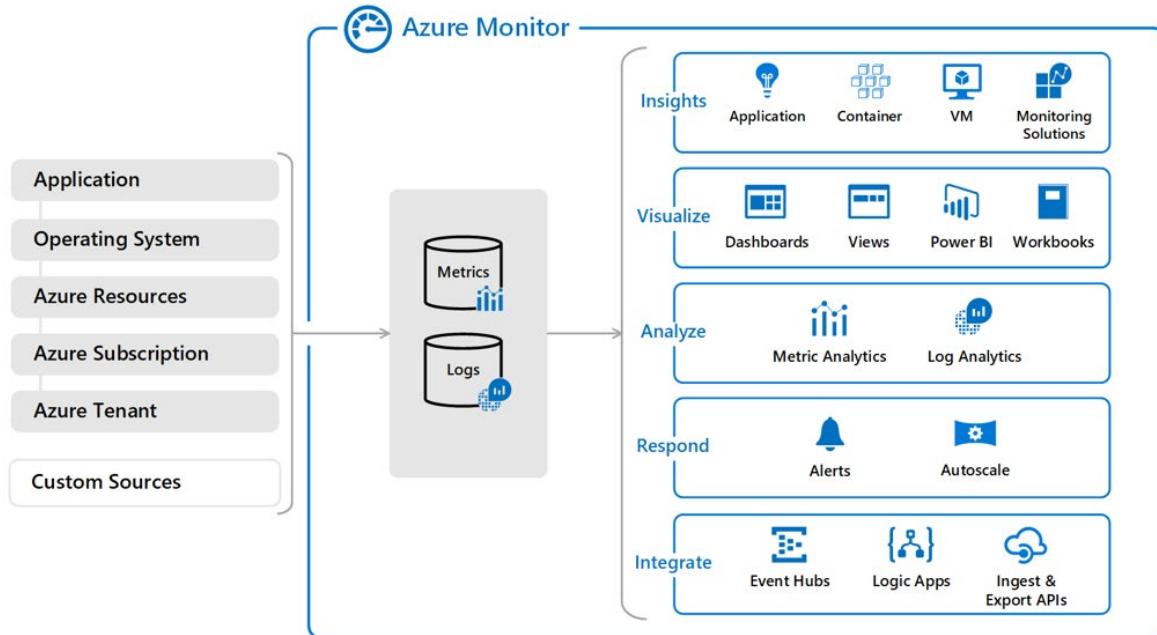
Azure Monitor

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 Documentation- <https://docs.microsoft.com/en-us/azure/azure-monitor/>

Video - Azure Monitor Overview - https://youtu.be/_hGff5bVtkM

Key Capabilities

Azure Monitor provides three main 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](#)

Monitoring Data Platform

All data collected by Azure Monitor fits into one of two fundamental types, **metrics and logs**¹.

- **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.

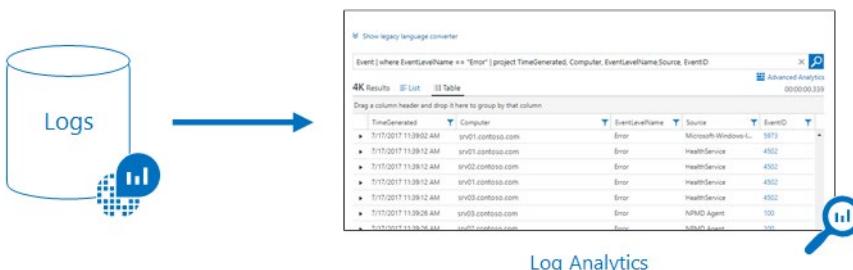
For many Azure resources, the data collected by Azure Monitor is displayed on the Overview page in the Azure portal. For example, virtual machines have several charts displaying performance metrics. Click on any of the graphs to open the data in Metric explorer in the Azure portal, which allows you to 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 language**² 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 Explorer**³ 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.



¹ <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-collection>

² <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview>

³ <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.

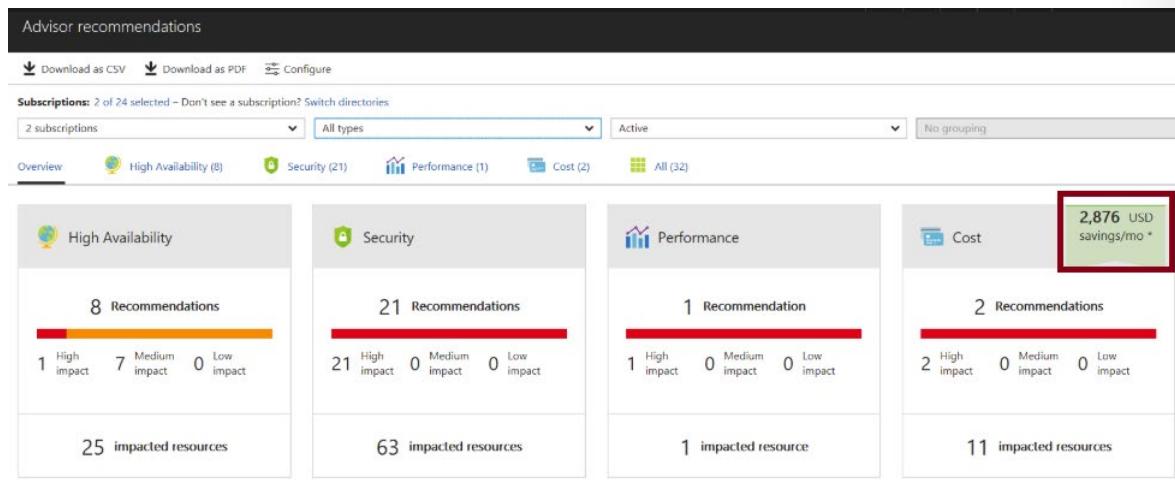
For more information:

Azure Fridays, Azure Monitor - <https://channel9.msdn.com/Shows/Azure-Friday/Azure-Monitor-player>

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.

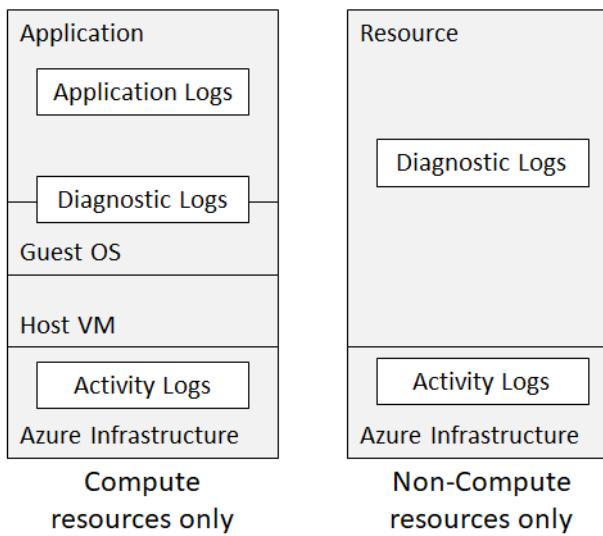
Activity Log

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.

MCT USE ONLY. STUDENT USE PROHIBITED



- ✓ 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

The screenshot shows the Azure Activity Log search interface with the following filters applied:

- Subscription: Visual Studio Enterprise
- Timespan: Last 6 hours
- Event severity: All
- Resource group: All resource groups
- Resource: All resources
- Resource type: None
- Operation: None
- Event initiated by: All
- Event category: All categories

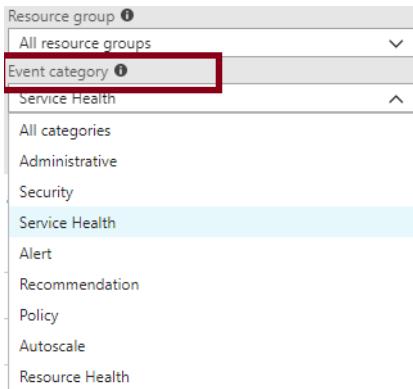
In the Azure portal, you can filter your Activity Log by these fields:

- **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.
- **Event Category.** The event category is described in the next topic.
- **Search.** This is an open text search box that searches for that string across all fields in all events.

- 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.

Event Categories

The Activity Log provides several event categories. You may select one or more.



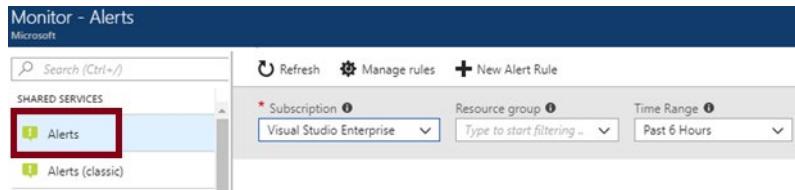
- Administrative.** This category contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of the types of events you would observe in this category include "create virtual machine" and "delete network security group". The Administrative category 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.
- 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 and Resource Health.** These categories do not contain any events; they are reserved for future use.

MCT USE ONLY. STUDENT USE PROHIBITED

Azure Alerts

Azure Monitor Alerts

Alerting is now available with Azure Monitor.

A screenshot of the Azure Monitor - Alerts interface. The top navigation bar says "Monitor - Alerts Microsoft". Below it is a search bar and a "New Alert Rule" button. A sidebar on the left lists "SHARED SERVICES" with "Alerts" highlighted with a red box. Other options include "Alerts (classic)". The main area has filters for "Subscription" (Visual Studio Enterprise), "Resource group" (Type to start filtering...), and "Time Range" (Past 6 Hours).

The Monitor Alerts experience has many benefits.

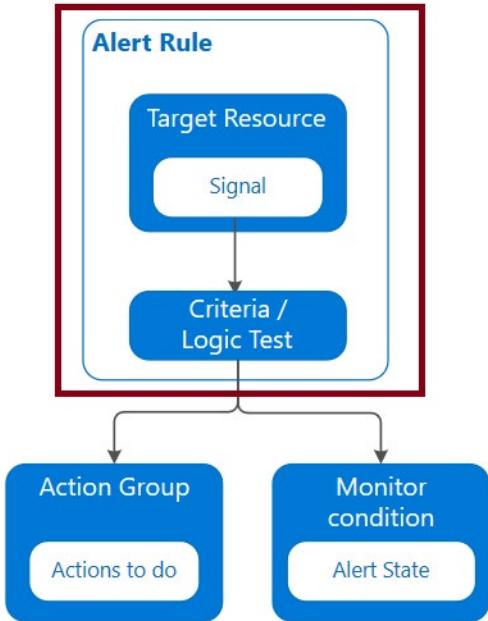
- **Better notification system.** All newer alerts use action groups, which are named groups of notifications and actions that can be reused in multiple alerts.
- **A unified authoring experience.** All alert creation for metrics, logs and activity log across Azure Monitor, Log Analytics, and Application 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.

For more information:

The new alerts experience in Azure Monitor - <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-unified-alerts>

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.



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. The 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 he / she has been added to the action group.

Add action group

* Action group name <small>i</small>	Sample action group	<input checked="" type="checkbox"/>	
* Short name <small>i</small>	SamleAG	<input checked="" type="checkbox"/>	
* Subscription <small>i</small>	<Subscription ID>	<input type="button" value="▼"/>	
* Resource group <small>i</small>	Default-ActivityLogAlerts	<input type="button" value="▼"/>	
Actions			
ACTION NAME	ACTION TYPE	STATUS	DETAILS
	Email/SMS/Push/Voice		
	Azure Function		
	LogicApp		
	Webhook		
	ITSM		
	Automation Runbook		

- **Email** – Emails will be sent to the email addresses. Ensure that your email filtering is configured appropriately. You may have up to 1000 email actions in an Action Group.
- **ITSM** – You may have up to 10 ITSM actions in an Action Group ITSM Action requires an ITSM Connection.
- **Logic App** – You may have up to 10 Logic App actions in an Action Group.
- **Function App** – The function keys for Function Apps configured as actions are read through the Functions API.
- **Runbook** – You may have up to 10 Runbook actions in an Action Group.
- **SMS** – You may have up to 10 SMS actions in an Action Group.
- **Voice** – You may have up to 10 Voice actions in an Action Group.
- **Webhook** – You may have up to 10 Webhook actions in an Action Group. Retry logic - The timeout period for a response is 10 seconds. The webhook call will be retried a maximum of 2 times when the following HTTP status codes are returned: 408, 429, 503, 504 or the HTTP endpoint does not respond. The first retry happens after 10 seconds. The second and last retry happens after 100 seconds.
- ✓ You may have up to 10 Azure app actions in an Action Group. At this time the Azure app action only supports ServiceHealth alerts.

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 resolved. The alert state isn't changed until the user changes it.

Alerts Experience

The default Alerts page provides a summary of alerts that are created within a particular time window. It displays the total alerts for each severity with columns that identify the total number of alerts in each state for each severity.



Column	Description
Subscription	Select up to five Azure subscriptions. Only alerts in the selected subscriptions are included in the view.
Resource group	Select a single resource group. Only alerts with targets in the selected resource group are included in the view.
Time range	Only alerts fired within the selected time window are included in the view. Supported values are the past hour, the past 24 hours, the past 7 days, and the past 30 days.

✓ You can select Total Alerts, Smart Groups, and Total Alert Rules to open a new page.

Alert Detail Page

The Alert detail page is displayed when you select an alert. It provides details of the alert and enables you to change its state.

All Alerts > Heartbeat alerts on all...

Alert Name Heartbeat alerts on all Windows computers in a workspace [Log to Metric]	Created Time 10/30/2018, 11:06:16 AM	Severity Sev3	State New
Change alert state			

Section	Description
Essentials	Displays the properties and other significant information about the alert.
History	Lists each action taken by the alert and any changes made to the alert. Currently limited to state changes.
Smart group	Information about the smart group the alert is included in. The alert count refers to the number of alerts that are included in the smart group. Includes other alerts in the same smart group that were created in the past 30 days regardless of the time filter in the alerts list page. Select an alert to view its detail.
More details	Displays further contextual information for the alert, which is typically specific to the type of source that created the alert.

Create an Alert

Alerts can be authored in a consistent manner regardless of the monitoring service or signal type. All fired alerts and related details are available in single page. You create a new alert rule with the following three steps:

The screenshot shows the 'Create rule' blade in the Azure portal. At the top, it says 'Create rule' and 'Rules management'. The first section is 'RESOURCE' with a computer icon, titled '* RESOURCE'. It says 'Select the target(s) that you wish to monitor' and has a 'Select' button. The second section is 'CONDITION' with a clipboard icon, titled '* CONDITION'. It says 'No condition defined, click on 'Add condition' to select a signal and define its logic' and has a 'Add condition' button. The third section is 'ACTION GROUPS' with a robot icon. It says '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](#)'. It has two sub-sections: 'ACTION GROUP NAME' and 'ACTION GROUP TYPE', both showing 'No action group selected'. Below these are 'Select existing' and 'Create New' buttons.

- **Resource.** Select the resource you want to monitor. For example, resource group, virtual machine, or storage account.
 - **Condition.** Select the signal and define its logic. The signal could be All, Metrics, or Activity log.
 - **Action Group.** Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions.
 - **Alert rule name.** Specify a name to identify your alert.
 - **Description.** Provide a description for your alert rule.
 - **Enable rule upon creation.** You can enable and disable your alert rules.
- We currently support configuring only two metrics signals or one log search signal or one activity log signal per alert rule. An alert will be triggered when the conditions for all the above configured criteria are met.

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 Scenarios

One of the challenges with any broad data analytics solution is figuring out where you can provide value for your organization. Out of all the things that are possible, what does your business need? What we hear from customers is that the following areas all have the potential to deliver significant business value:

Example 1 - Assessing updates

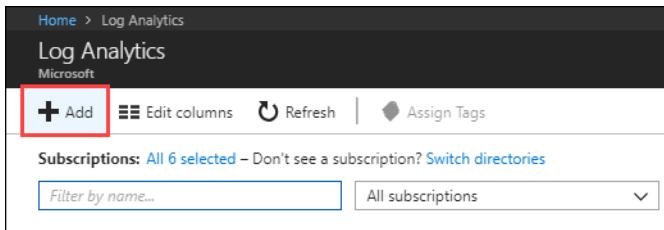
An important part of the daily routine for any IT administrator is assessing systems update requirements and planning patches. Accurate scheduling is critical, as it directly relates to SLAs to the business and can seriously impact business functions. In the past, you had to schedule an update with only 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.

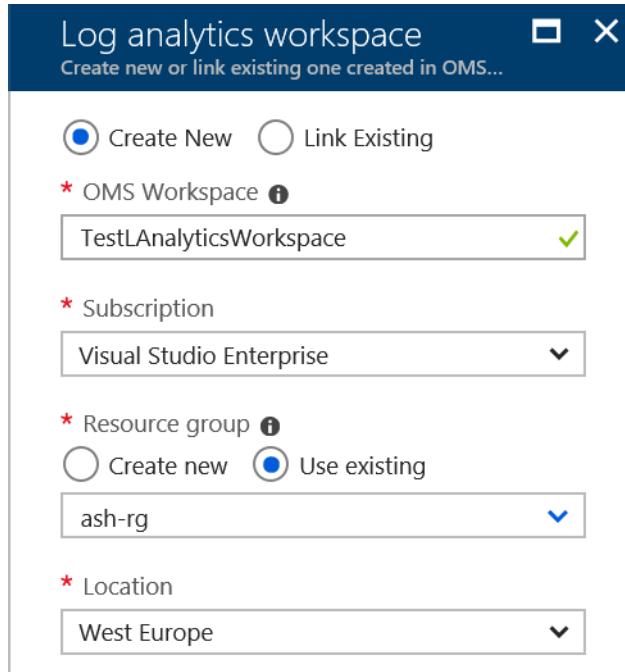
Create a Workspace

To get started with Log Analytics you need to add a workspace. In the Azure portal, click **All services**. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics**.



The screenshot shows the Azure Log Analytics service page. At the top, there's a navigation bar with 'Home > Log Analytics'. Below it, the title 'Log Analytics Microsoft' is displayed. A red box highlights the '+ Add' button, which is located next to other buttons: 'Edit columns', 'Refresh', and 'Assign Tags'. Below these buttons, a message says 'Subscriptions: All 6 selected – Don't see a subscription? Switch directories'. There are two input fields: 'Filter by name...' and 'All subscriptions' with a dropdown arrow. The background of the page is white, and the overall layout is clean and modern.

You can then click Create and select your choices for the new workspace.



- Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace.
- 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.

For more information:

Log analytics regions -<https://azure.microsoft.com/regions/services/>

Connected Sources

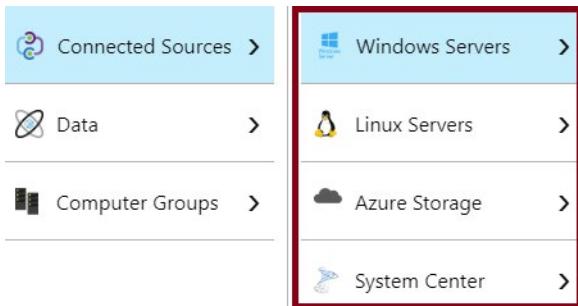
Connected Sources are the computers and other resources that generate data collected by Log Analytics. This can include agents installed on **Windows⁴** and **Linux⁵** computers that connect directly or agents in a connected **System Center Operations Manager management group⁶**. Log Analytics can also collect data from **Azure storage⁷**.

⁴ <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents>

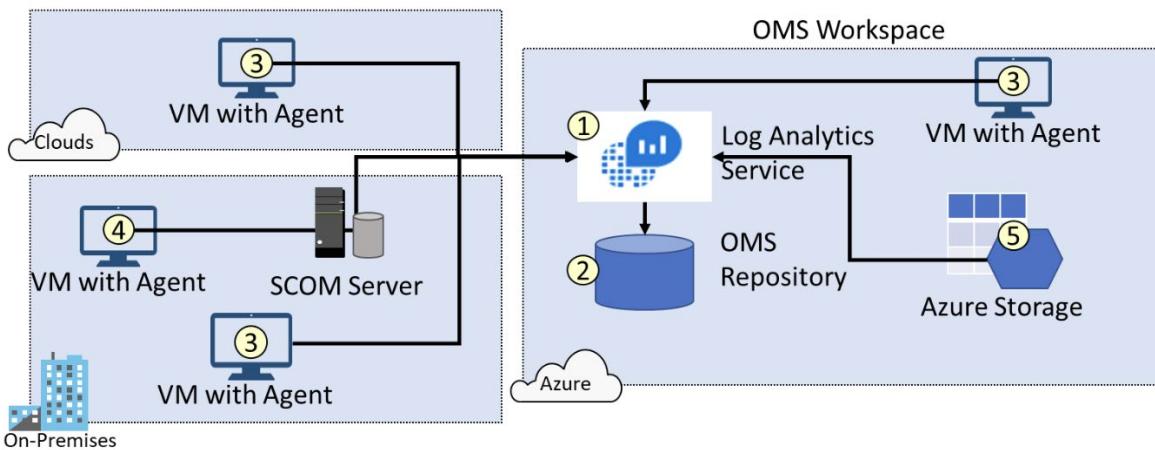
⁵ <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-linux-agents>

⁶ <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-om-agents>

⁷ <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-storage>



This following diagram shows how Connected Sources flow data to the Log Analytics service.

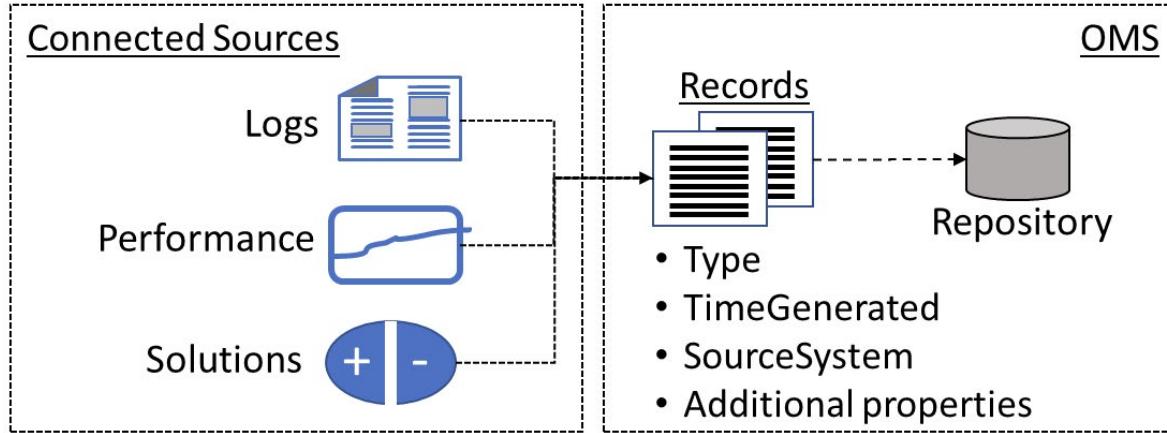


Ensure you can locate each of the following.

- The Log Analytics service (1) collects data and stores it in the OMS repository (2). The OMS 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.

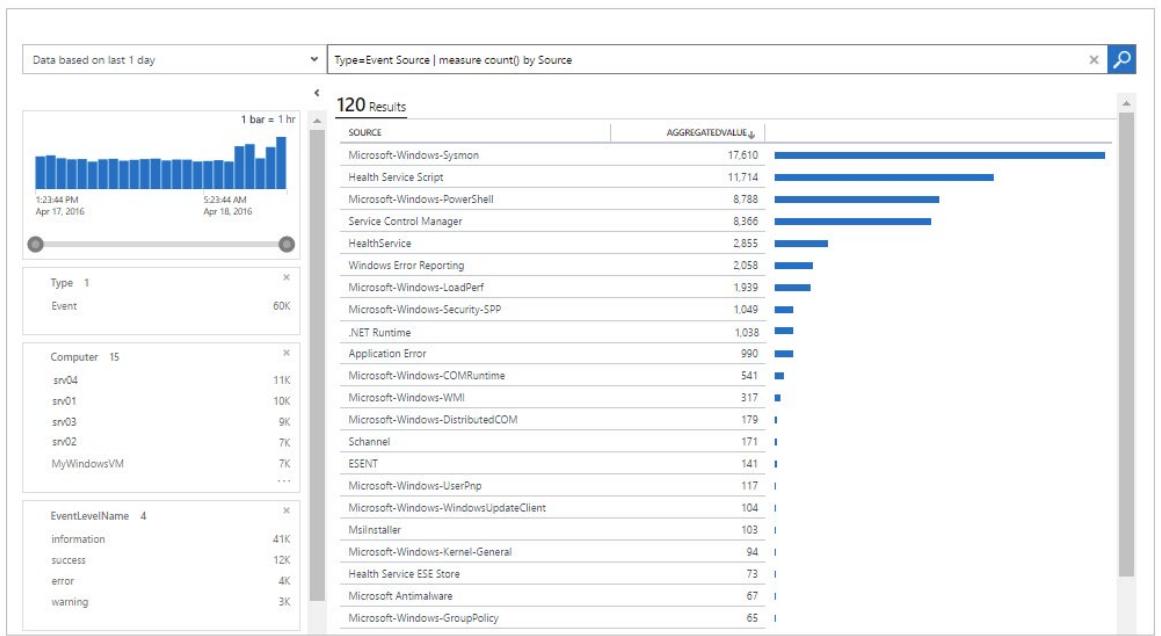
The screenshot shows the 'Data Sources' configuration page in the Log Analytics portal. The left sidebar includes 'Solutions', 'Connected Sources', **Data** (selected), 'Computer Groups', 'Accounts', 'Alerts', and 'Preview Features'. The main area is titled 'Data Sources' and lists several data collection options:

- Windows Event Logs
- Windows Performance Counters
- Linux Performance Counters
- IIS Logs
- Custom Fields
- Custom Logs
- Syslog

To the right, there's a section for collecting events from event logs, with a table for selecting log levels (ERROR, WARNING, INFORMATION) for Application, Operations Manager, and System logs.

Log Analytics Querying

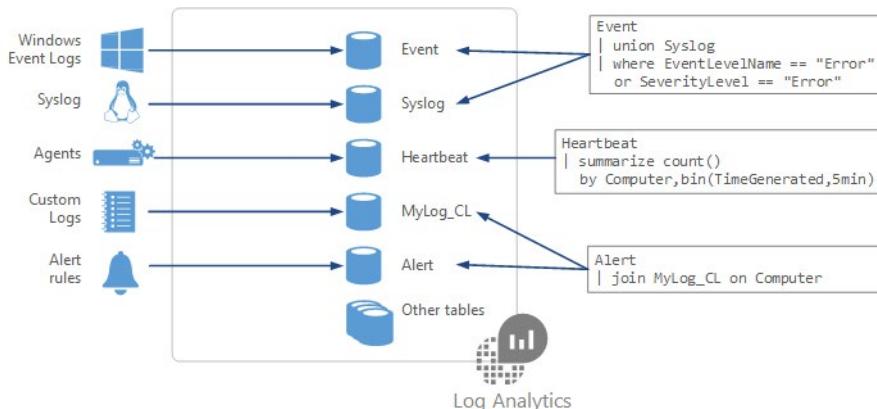
Log Analytics provides a query syntax to quickly retrieve and consolidate data in the repository. You can create and save Log Searches to directly analyze data in the OMS portal or have log searches run automatically to create an alert if the results of the query indicate an important condition.



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.

Querying 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 queries - <https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/query-language>

Demonstration - Log Analytics

In this demonstration, you will work with the Log Analytics query language.

Access the demonstration environment

1. Access the **Log Analytics Querying Demonstration**⁸ 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.

⁸ <https://portal.loganalytics.io/demo>

5. As you have time experiment with other **Favorites** and also **Saved Queries**.

- ✓ Is there a particular query you are interested in?

MCT USE ONLY. STUDENT USE PROHIBITED

Network Watcher

Network Watcher

Azure Network Watcher provides tools to **monitor**, **diagnose**, view **metrics**, and enable or disable **logs** for resources in an Azure virtual network.

- **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.

Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level.

Network Watcher		
Microsoft		
NAME	REGION	STATUS
ASC DEMO	▼ 27 regions	Partially enabled
	West US	Enabled
	East US	Enabled
	North Europe	Enabled
	West Europe	Enabled

For more information:

Network Watcher - <https://azure.microsoft.com/en-us/services/network-watcher/>

Monitoring and Visualization

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.

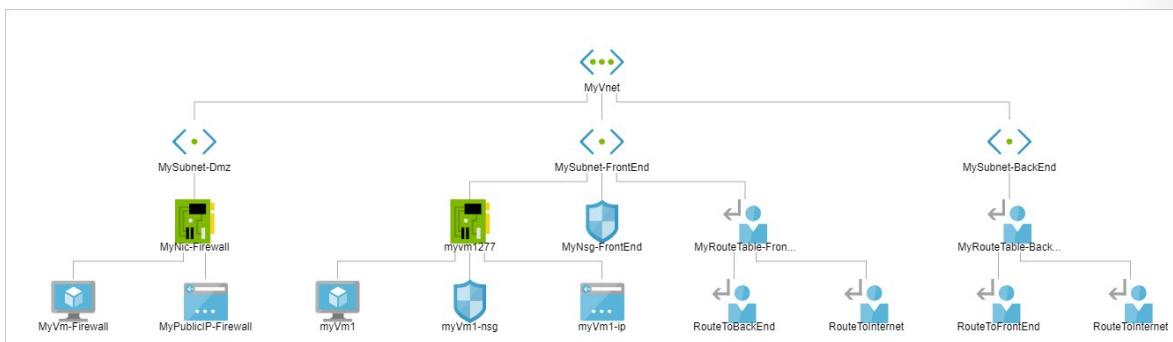
If an endpoint becomes unreachable, connection troubleshoot informs you of the reason. Potential reasons might be DNS name resolution problem, the CPU, memory, or firewall within the operating system of a VM, or the hop type of a custom route, or security rule for the VM or subnet of the outbound connection. 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.

Topology

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:



- ✓ 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.

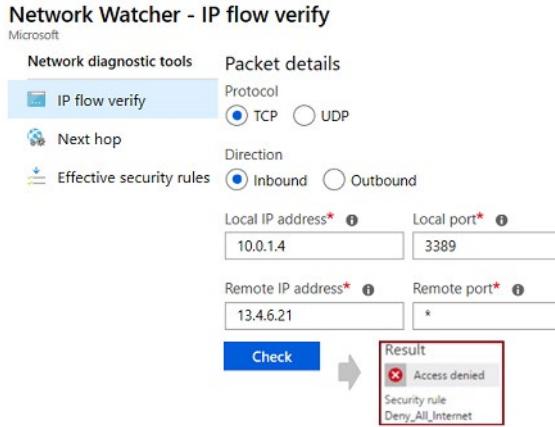
Diagnostics - IP Flow Verify

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.



If IP flow verify does not return the expected behavior you can investigate the security rule that was involved to determine what is going wrong and make an adjustment.

Inbound rules

NAME	PRIORITY	SOURCE	SOURCE PORTS
default-allow-rdp	1000	0.0.0.0/0	0-65535
AllowVnetInBound	65000	Virtual network (2 prefixes)	0-65535
AllowAzureLoadBalance...	65001	Azure load balancer (1 prefixes)	0-65535
Deny_All_Internet	65500	0.0.0.0/0	0-65535

- ✓ 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.

Network Watcher - Next hop

The screenshot shows the 'Network diagnostic tools' section with 'Next hop' selected. The configuration fields are as follows:

- Subscription:** MSDN Platforms
- Resource group:** NetworkWatcherRG
- Virtual machine:** LinuxVM
- Network interface:** linuxvm493
- Source IP address:** 10.0.1.4
- Destination IP address:** 10.1.1.4

A red box highlights the results area, which displays:

- Next hop type:** Virtual Appliance
- IP address:** 10.1.2.4
- Route table ID:** /subscriptions/6515xxxxx

A blue 'Next hop' button is at the bottom.

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 - VPN Diagnostics

VPN Diagnostics 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.

The screenshot shows the 'NETWORK DIAGNOSTIC TOOLS' section with 'VPN Diagnostics' selected. A red box highlights the 'Start troubleshooting' button. The main table displays two entries:

NAME	TROUBLESHOOTING STATUS	RESOURCE STATUS
VNet1GW	Unhealthy	Succeeded
VNet1toSite1	Running	Succeeded

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.

- ✓ You can select multiple gateways or connections to troubleshoot simultaneously or you can focus on an individual component.

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.

You can download flow logs from configured storage accounts. Navigate to the storage container and open the PT1H.JSON file.

NAME	RESOURCE TYPE	RESOURCE GROUP	STATUS
myVm-nsg	Network security group	myResourceGroup	Enabled

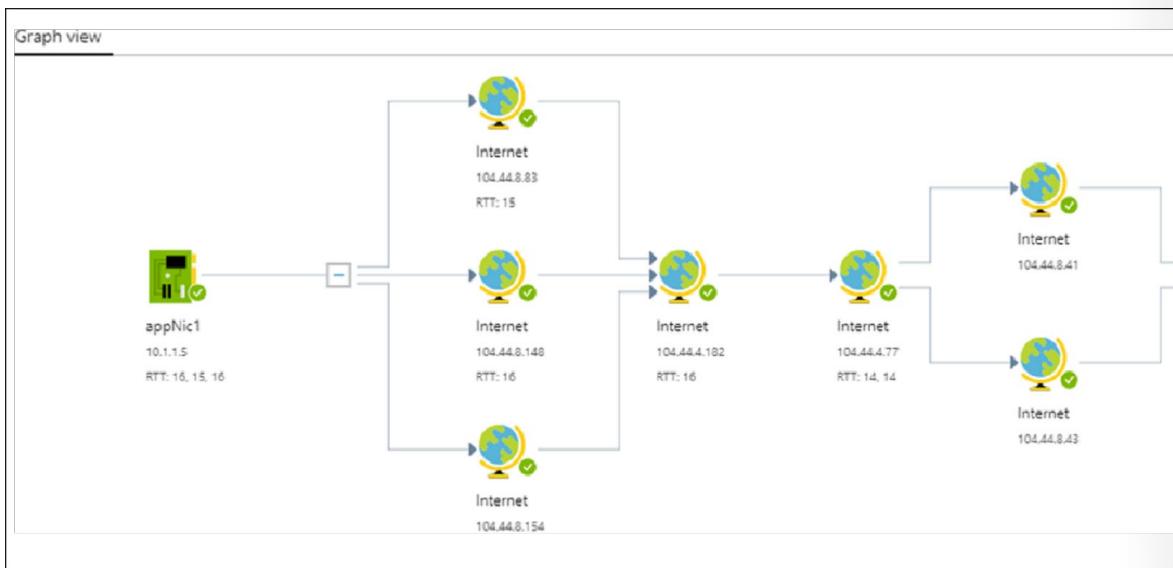
- ✓ These capabilities can be used in security compliance and auditing. You can define a prescriptive set of security rules as a model for security governance in your organization. A periodic compliance audit can be implemented in a programmatic way by comparing the prescriptive rules with the effective rules for each of the VMs in your network. Explore this feature with NSG Auditing practice.

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.

This adds to the current capabilities of Network Watcher in providing even more ways for you troubleshoot networking operations. You can use Connection Troubleshoot to:

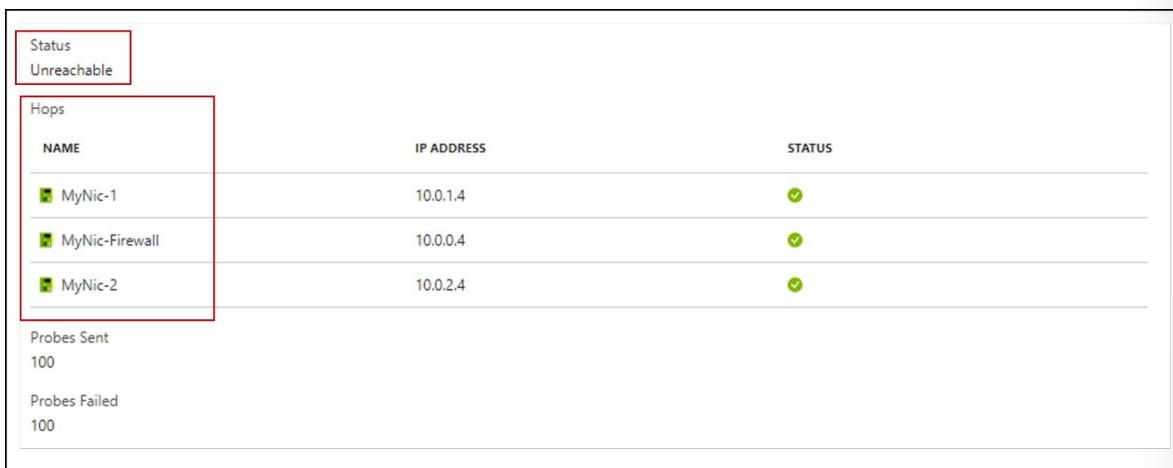
- Check connectivity between source (VM) and destination (VM, URI, FQDN, IP Address).
- Identify configuration issues that are impacting reachability.
- Provide all possible hop by hop paths from the source to destination.
- Hop by hop latency.
- Latency - min, max, and average between source and destination.
- View the number of packets dropped during the connection troubleshoot check.
- Connection Troubleshoot can also provide a topology (graphical) view from your source to destination, as shown in the following illustration.



Example Scenario

Connection Troubleshoot supports all networking scenarios where the source and destination is an Azure VM, FQDN, URI or an IPv4 Address.

In this example, an instance of Network Watcher is configured to check connectivity to a destination VM over port 80. When you open Connection Troubleshoot and select the VM and port to test, once you click Check, connectivity between the VMs on the port specified is checked. In this case, the destination VM is unreachable, and a listing of hops is shown.



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.

For more information:

Troubleshoot connections with Azure Network Watcher using the Azure portal - <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-connectivity-portal>

Lab and Review Questions

Lab - Network Watcher

Scenario

Adatum Corporation wants to monitor Azure virtual network connectivity by using Azure Network Watcher.

Objectives

After completing this lab, you will be able to:

- Deploy Azure VMs, Azure storage accounts, and Azure SQL Database instances by using Azure Resource Manager templates
- Use Azure Network Watcher to monitor network connectivity

Exercise 1: Prepare infrastructure for Azure Network Watcher-based monitoring

The main tasks for this exercise are as follows:

- Deploy Azure VMs, an Azure Storage account, and an Azure SQL Database instance by using an Azure Resource Manager template
- Enable Azure Network Watcher service
- Establish peering between Azure virtual networks
- Establish service endpoints to an Azure Storage account and Azure SQL Database instance

Result: After you completed this exercise, you have deployed Azure VMs, an Azure Storage account, and an Azure SQL Database instance by using Azure Resource Manager templates, enabled Azure Network Watcher service, established global peering between Azure virtual networks, and established service endpoints to an Azure Storage account and Azure SQL Database instance.

Exercise 2: Use Azure Network Watcher to monitor network connectivity.

The main tasks for this exercise are as follows:

- Test network connectivity to an Azure VM via virtual network peering by using Network Watcher
- Test network connectivity to an Azure Storage account by using Network Watcher
- Test network connectivity to an Azure SQL Database by using Network Watcher

Result: After you completed this exercise, you have used Azure Network Watcher to test network connectivity to an Azure VM via virtual network peering, network connectivity to Azure Storage, and network connectivity to Azure SQL Database.

Module 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 a 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 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
- Recommodation
- Policy

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 a 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.

Module 7 Data Protection

Data Replication

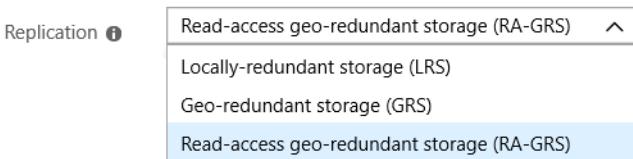
Replication Options

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. Review the SLA for information about Azure Storage guarantees for durability and availability.

When you create a Standard storage account there are four replications schemes: **Locally-redundant storage (LRS)**, **Geo-redundant storage (GRS)**, **Read-access geo-redundant storage (RA-GRS)**, and **Zone-redundant storage (ZRS)**.

Create storage account

Basics Advanced Tags Review + create



Are there any costs to changing my account's replication strategy?

It depends on your conversion path. Ordering from cheapest to the most expensive redundancy offering we have LRS, ZRS, GRS, and RA-GRS. For example, going from LRS to anything will incur additional charges because you are going to a more sophisticated redundancy level. Going to GRS or RA-GRS will incur an egress bandwidth charge because your data (in your primary region) is being replicated to your remote secondary region. This is a one-time charge at initial setup. After the data is copied, there are no further conversion charges. You will only be charged for replicating any new or updates to existing data.

If you change from GRS to LRS, there is no additional cost, but your replicated data is deleted from the secondary location.

- ✓ If you select Premium performance only LRS replication will be available.
- ✓ If you create availability sets for your virtual machines, then Azure uses Zone-redundant Storage (ZRS).

For more information:

Azure storage replication - <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

Locally-redundant Storage

Replication	Copies	Strategy
Locally redundant storage (LRS)	Maintains three copies of your data.	Data is replicated three time within a single facility in a single region.

Locally redundant storage (LRS) provides at least 99.99999999% (11 nines) durability of objects over a given year. LRS provides this object durability by replicating your data to a storage scale unit. A data-center, located in the region where you created your storage account, hosts the storage scale unit. A write request to an LRS storage account returns successfully only after the data is written to all replicas. Each replica resides in separate fault domains and upgrade domains within a storage scale unit. A storage scale unit is a collection of racks of storage nodes. A fault domain (FD) is a group of nodes that represent a physical unit of failure. Think of a fault domain as nodes belonging to the same physical rack. An upgrade domain (UD) is a group of nodes that are upgraded together during the process of a service upgrade (rollout). The replicas are spread across UD and FDs within one storage scale unit. This architecture ensures your data is available if a hardware failure affects a single rack or when nodes are upgraded during a service upgrade.

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. To mitigate this risk, Microsoft recommends using either zone-redundant storage (ZRS) or geo-redundant storage (GRS).

If your application stores data that can be easily reconstructed if data loss occurs, you may opt for LRS. Some applications are restricted to replicating data only within a country due to data governance requirements. In some cases, the paired regions across which the data is replicated for GRS accounts may be in another country.

LRS is a low-cost option for protecting your data from local hardware failures. If a datacenter-level disaster (for example, fire or flooding) occurs, all replicas may be lost or unrecoverable. To mitigate this risk, Microsoft recommends using either zone-redundant storage (ZRS) or geo-redundant storage (GRS).

However, LRS may be appropriate in these scenarios:

- If your application stores data that can be easily reconstructed if data loss occurs, you may opt for LRS.
 - Some applications are restricted to replicating data only within a country due to data governance requirements.
- ✓ Do you think LRS is a good choice for your organization?

Zone-redundant Storage

Replication	Copies	Strategy
Zone-redundant storage (ZRS)	Maintains three copies of your data.	Data is replicated three times across two to three facilities, either within a single region or across two regions.

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.

Support coverage and regional availability

ZRS currently supports standard general-purpose v2 account types. ZRS is available for block blobs, non-disk page blobs, files, tables, and queues.

What happens when a zone becomes unavailable?

Your data is still accessible for both read and write operations even if a zone becomes unavailable. Microsoft recommends that you continue to follow practices for transient fault handling. These practices include implementing retry policies with exponential back-off.

When a zone is unavailable, Azure undertakes networking updates, such as DNS repointing. These updates may affect your application if you are accessing your data before the updates have completed.

ZRS may not protect your data against a regional disaster where multiple zones are permanently affected. Instead, ZRS offers resiliency for your data if it becomes temporarily unavailable. For protection against regional disasters, Microsoft recommends using geo-redundant storage (GRS).

- ✓ Consider ZRS for scenarios that require strong consistency, strong durability, and high availability even if an outage or natural disaster renders a zonal data center unavailable.

Geo-redundant storage

Replication	Copies	Strategy
Geo-redundant storage (GRS)	Maintains six copies of your data.	Data is replicated three times within the primary region and is also replicated three times in a secondary region hundreds of miles away from the primary region.

Replication	Copies	Strategy
Read access geo-redundant storage (RA-GRS)	Maintains six copies of your data.	Data is replicated to a secondary geographic location and provides read access to your data in the secondary location.

Geo-redundant storage (GRS) is the default and recommended replication option and is sometimes called cross-regional replication. 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. Geo-redundant storage (GRS) is designed to provide at least 99.9999999999999% (16 9's) durability of objects over a given year by replicating your data to a secondary region that is hundreds of miles away from the primary region. 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.

What is the RPO and RTO with GRS?

Recovery Point Objective (RPO): In GRS and RA-GRS, the storage service asynchronously geo-replicates the data from the primary to the secondary location. In the event that the primary region becomes unavailable, you can perform an account failover (preview) to the secondary region. When you initiate a failover, recent changes that haven't yet been geo-replicated may be lost. The number of minutes of potential data that's lost is known as the RPO. The RPO indicates the point in time to which data can be recovered. Azure Storage typically has an RPO of less than 15 minutes, although there's currently no SLA on how long geo-replication takes.

Recovery Time Objective (RTO): The RTO is a measure of how long it takes to perform the failover and get the storage account back online. The time to perform the failover includes the following actions:

- The time until the customer initiates the failover of the storage account from the primary to the secondary region.
 - The time required by Azure to perform the failover by changing the primary DNS entries to point to the secondary location.
- ✓ If you enable RA-GRS and your primary endpoint for the Blob service is *myaccount.blob.core.windows.net*, then your secondary endpoint is *myaccount-secondary.blob.core.windows.net*. The access keys for your storage account are the same for both the primary and secondary endpoints.

Comparing Replication Strategies

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).

Replication Option	LRS	ZRS	GRS	RA-GRS
Node unavailability within a data center	Yes	Yes	Yes	Yes
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	No	Yes
Available in storage account types	GPv1, GPv2, Blob	Standard,GPv2	GPv1, GPv2, Blob	GPv1, GPv2, Blob

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?

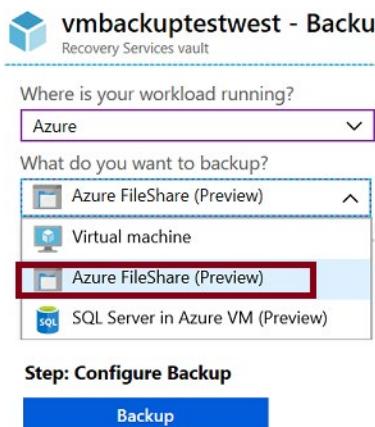
For more information:

What is Azure Backup - <https://docs.microsoft.com/en-us/azure/backup/backup-overview#why-use-azure-backup>

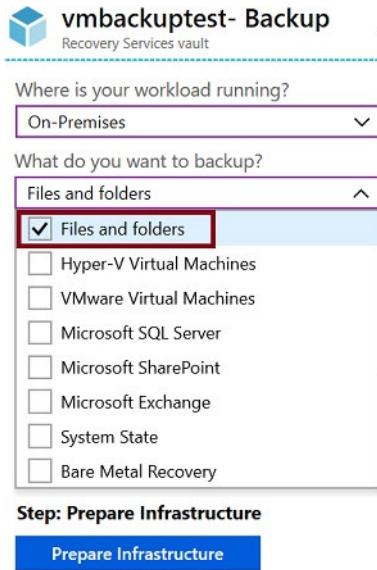
Recovery Service Vault Backup Options

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.



- ✓ 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 another lesson.

Demonstration - Backup Azure File Shares

In this demonstration, we will explore backing up a file share in the Azure portal.

Note: This demonstration requires an Azure file share and a storage account that can be used by the vault.

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 the vault

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**.

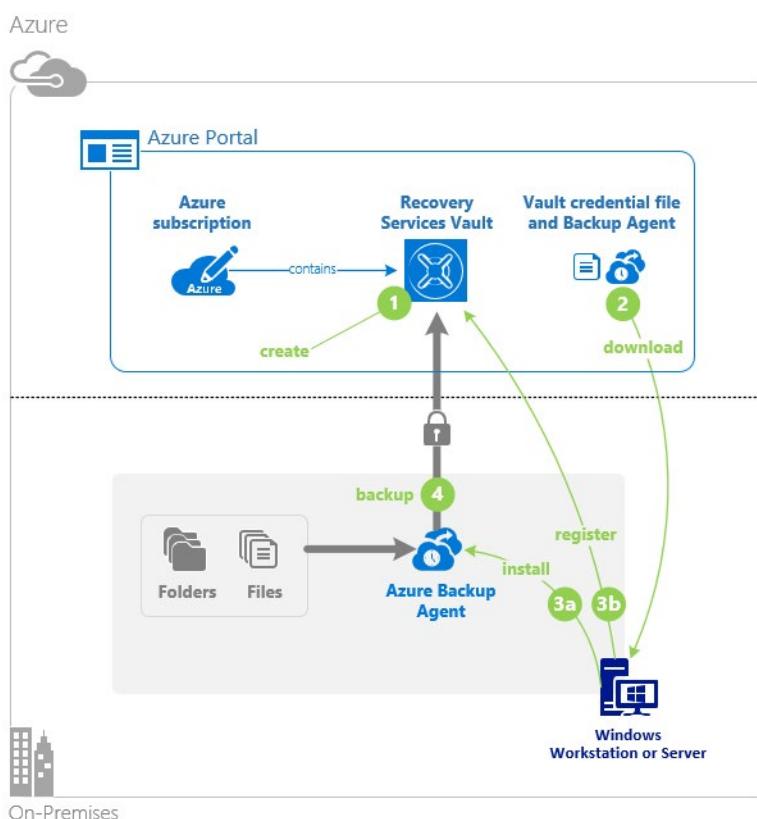
Explore Recovery Services vault information

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.



1. **Create the recovery services vault.** Within your Azure subscription you will need to create a recovery services vault for the backups.
2. **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 creden-

MCT USE ONLY. STUDENT USE PROHIBITED

tials 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.

3. **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.
4. **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.

MARS Agent

Azure Backup for files and folders relies on the Microsoft Azure Recovery Services (MARS) agent to be installed on the Window client or server.

The screenshot shows the Microsoft Azure Backup interface. At the top, it says "Microsoft Azure Backup". Below that, there's a message: "Microsoft Azure Backup supports scheduled backups of files and folders to an cloud storage account." A warning icon indicates that "Backups have not been configured for this server. Click 'Schedule Backup' in the Actions pane to config". It also says "You can also Configure Notifications from Alerts blade to receive email alerts for backup failures. [Learn More](#)". On the left, there's a "Jobs (Activity in the past 7 days, double click on the message to see details)" section 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.

On the right, there's an "Actions" pane with a dropdown menu set to "Backup". The menu includes: Register Server, Schedule Backup, Recover Data, Change Properties, Open Portal, Privacy & Cookies, View, and 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 Files and Folders

In this demonstration, we will step through the process to backup and restore files and folders from Windows to Azure.

Note: This demonstration assumes you have not used the Azure Backup Agent before and need a complete installation.

Create a Recovery Services vault

1. In the Azure portal, type Recovery Services and click **Recovery Services vaults**.
2. Click **Add**.
3. Provide a **Name, Subscription, Resource group**, and **Location**.
4. Click **Create**. It can take several minutes for the Recovery Services vault to be created. Monitor the status notifications in the upper right-hand area of the portal. Once your vault is created, it appears in the list of Recovery Services vaults.

5. If after several minutes you don't observe your vault, click **Refresh**.

Configure the vault

1. For your recovery services vault, click **Backup**.
2. From the **Where is your workload running?** drop-down menu, select **On-premises**.
3. From the **What do you want to backup?** menu, select **Files and folders**. Notice your other choices.
4. Click **Prepare infrastructure**.
5. Click **Download Agent for Windows Server or Windows Client**. A pop-up menu prompts you to run or **save** MARSagentInstaller.exe.
6. By default, the MARSagentinstaller.exe file is saved to your **Downloads** folder. When the installer completes, a pop-up asking if you want to run the installer, or open the folder. You **don't need** to install the agent yet. You can install the agent after you have downloaded the vault credentials.
7. Return to your recovery services vault, check the box **Already downloaded or using the latest recovery services agent**.
8. Click **Download**. After the vault credentials finish downloading, a pop-up asking if you want to open or **save** the credentials. Click **Save**. If you accidentally click **Open**, let the dialog that attempts to open the vault credentials, fail. You cannot open the vault credentials. Proceed to the next step. The vault credentials are in the **Downloads** folder.

Note: You must have the latest version of the MARS agent. Versions of the agent below 2.0.9083.0 must be upgraded by uninstalling and reinstalling the agent.

Install and register the agent

1. Locate and double-click the **MARSagentinstaller.exe** from the **Downloads** folder (or other saved location). The installer provides a series of messages as it extracts, installs, and registers the Recovery Services agent.
2. To complete the wizard, you need to:
 - Choose a location for the installation and cache folder.
 - Provide your proxy server info if you use a proxy server to connect to the internet.
 - Provide your user name and password details if you use an authenticated proxy.
 - If prompted, install any missing software.
 - Provide the downloaded vault credentials
 - Enter and save the encryption passphrase in a secure location.
3. Wait for the server registration to complete. This could take a couple of minutes.
4. The agent is now installed and your machine is registered to the vault. You're ready to configure and schedule your backup.

Create the backup policy

1. Open the **Microsoft Azure Recovery Services** agent. You can find it by searching your machine for Microsoft Azure Recovery Services.
2. If this is the first time you are using the agent there will be a **Warning** to create a backup policy. The backup policy is the schedule when recovery points are taken, and the length of time the recovery points are retained.

3. Click **Schedule Backup** to launch the Schedule Backup Wizard.

- Read the **Getting Started** page.
- **Add items** to include files and folders that you want to protect. Select just a few sample files. 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**.

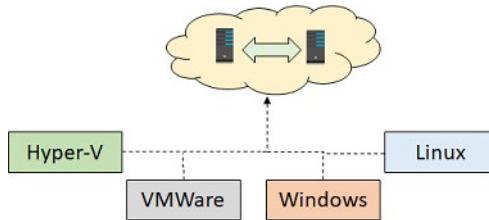
2. In the wizard, select **Stop using this backup schedule and delete all the stored backups.**
3. Verify your choices and click **Finish**.
4. You will be prompted for a recovery services vault security pin.
5. In the Azure portal locate your recovery services vault.
6. Select **Properties** and then Security PIN **Generate**.
7. Copy the PIN into the Backup agent to finish deleting the schedule.

MCT USE ONLY. STUDENT USE PROHIBITED

Virtual Machine Backups

Azure Site Recovery Scenarios

You can use **Azure Site Recovery** to replicate on-premises physical or virtual machines running Windows or Linux. Azure Site Recovery includes support for both Hyper-V and VMware virtual machines. You can replicate data from your on-premises datacenter to Azure or to a secondary site. Orchestration is built in with Azure Site Recovery, which means that the management of replication, failover, and recovery is included. For example, should a virtual machine or service fail in your datacenter, you can use Azure Site Recovery to failover to the replicated resource in either Azure or your secondary site.



Azure Site Recovery works in the following three scenarios:

- **Hyper-V Virtual Machine Replication.** When Virtual Machine Manager (VMM) is used to manage Hyper-V virtual machines, you can use Azure Site Recovery to replicate them to Azure or to a secondary datacenter. If you do not use VMM to manage your virtual machines, you can use Azure Site Recovery to replicate them to Azure only.
- **VMware Virtual Machine Replication.** You can perform the replication of virtual machines by VMware to a secondary site that is also running VMware. You also can replicate to Azure.
- **Physical Windows and Linux machines.** You can replicate physical machines running either Windows or Linux to a secondary site or to Azure.

Azure Site Recovery Benefits

A migration to the cloud can result in significant business benefits. Here are some reasons to use Azure Site Recovery.

- **Eliminate the need for disaster recovery sites.** Your environment can be protected by automating the replication of the virtual machines based on policies that you set and control. Site Recovery is heterogeneous and can protect Hyper-V, VMware, and physical servers.
- **Reduce infrastructure costs.** Lower your on-premises infrastructure costs by using Azure as a secondary site for conducting business during outages. Or, eliminate datacenter costs altogether by moving to Azure and setting up disaster recovery between Azure regions. You can pre-assess network, storage, and compute resources needed to replicate applications from on-premises to Azure—and pay only for compute and storage resources needed to run apps in Azure during outages.
- **Automatically replicate to Azure.** Automate the orderly recovery of services in the event of a site outage at the primary datacenter. Automate the orderly recovery of services in the event of a site outage at the primary datacenter.
- **Safeguard against outages of complex workloads.** Protect applications in SQL Server, SharePoint, SAP, and Oracle.
- **Extend or boost capacity.** Applications can be Migrated to Azure with just a few clicks or burst to Azure temporarily when you encounter a surge in demand.

- **Continuous health monitoring.** Site Recovery monitors the state of your protected instances continuously and remotely from Azure. When replicating between two sites you control, your virtual machines' data and replication remains on your networks. All communication with Azure is encrypted.
- ✓ 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 documentation - <https://azure.microsoft.com/en-us/services/site-recovery/>

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:

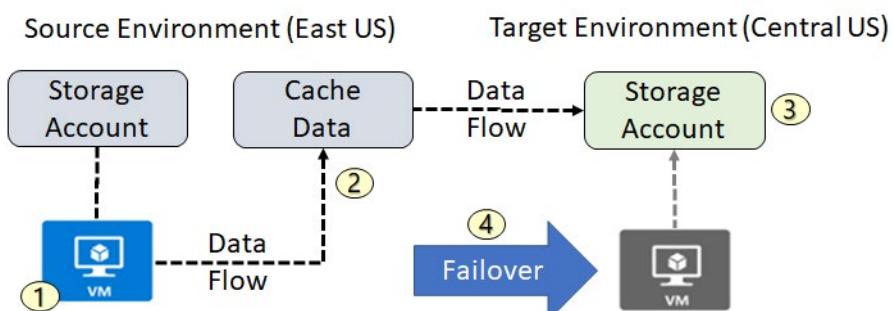
- Extending on-premises data protection solutions into Azure. In many cases, an organization can extend their backup strategy into Azure by choosing from many of the backup solutions available today in the Azure Marketplace.

The screenshot shows the Microsoft Azure Marketplace search results for the term "backup". The search bar at the top has "backup" highlighted with a red box. The results page displays 23 products under the heading "Product results (23)". The products are arranged in two rows of four. Each product card includes the provider's logo, name, and a brief description. Buttons for "Get it now" are visible at the bottom of each card.

Product Category	Product Name	Description	Action
Compute	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Networking	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Storage	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Web + Mobile	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Databases	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Intelligence + analytics	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Internet of Things	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Enterprise Integration	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Security + Identity	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Developer tools	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Monitoring + Management	Acronis Backup	By Acronis, Inc. The most complete, cost-effective and easy-to-manage hybrid local and cloud backup solution available	Get it now
Add-ons	Seagate Backup Services	By Seagate Seagate Backup Services for Microsoft Azure. Bring your own license	Get it now
Containers	Managed Backup Portal	By Veeam Managed Backup Portal for Service Providers and Resellers – fast start for your backup business Bring your own license	Get it now
Blockchain	OFFICE 365 CLOUD BACKUP	By UpSafe The more people work together on one project, the more is the risk of data loss. But UpSafe Office365 backu... Get it now	Get it now
Azure Active Directory apps	Quickbooks Online Backup	By Intuit, Inc. Use Azure AD to enable user access to Quickbooks Online Backup. Requires an existing Quickbooks Online Back... Get it now	Get it now
Test Drives			

- 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.

Azure to Azure Architecture



When you enable replication for an Azure VM, the following happens:

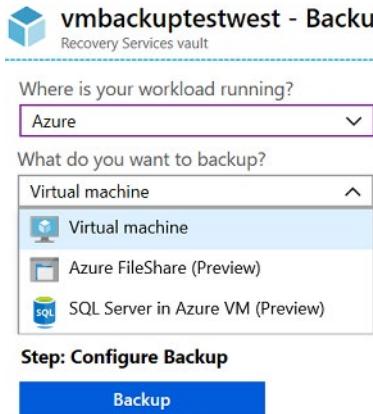
- The Site Recovery Mobility service extension is automatically installed on the VM. The extension registers the VM with Site Recovery. Continuous replication begins for the VM. Disk writes are immediately transferred to the cache storage account in the source location.

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.

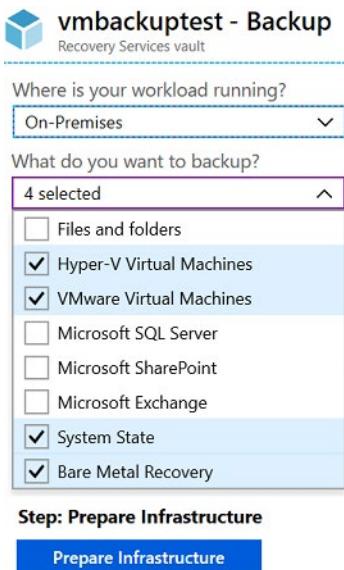
Recovery Services Vault VM Backup Options

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.

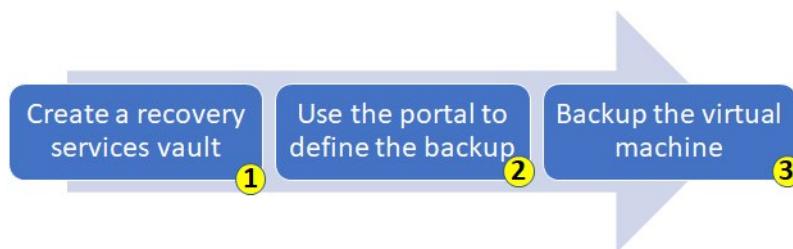


- The Recovery Services vault can be used to backup on-premises virtual machines including: Hyper-V, VmWare, System State, and Bare Metal Recovery.



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 Azure - <https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction>

Implementing VM Restore

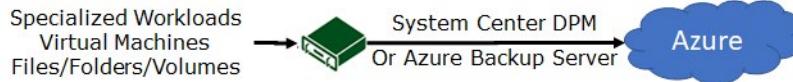
Once your virtual machine snapshots are safely in the recovery services vault it is easy to recover them.

The screenshot shows two windows side-by-side. The left window is titled 'Recovery Services vaults' and lists several vaults under 'Subscriptions'. One vault, 'JeremyVault', is highlighted with a red box. The right window is titled 'JeremyVault Recovery Services vault' and contains sections for 'Monitoring' and 'Backup'. Under 'Backup', there is a table with three columns: 'Backup Items', 'Backup Jobs', and 'Backup Usage'. The first row of this table, which corresponds to 'Azure Virtual Machines', is also highlighted with a red box.

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.
- 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

Component	Benefits	Limits	What is protected?	Where are backups stored?
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

Lab and Review Questions

Lab - Azure Site Recovery Between Regions

Scenario

Adatum Corporation wants to implement Azure Site Recovery to facilitate migration and protection of Azure VMs between regions.

Objectives

After completing this lab, you will be able to:

- Implement Azure Site Recovery Vault.
- Configure replication of Azure VMs between Azure regions by using Azure Site Recovery.

Exercise 1: Implement prerequisites for migration of Azure VMs by using Azure Site Recovery.

The main tasks for this exercise are as follows:

- Deploy an Azure VM to be migrated by using an Azure Resource Manager template.
- Create an Azure Recovery Services vault.

Result: After you completed this exercise, you have initiated deployment of an Azure VM by using an Azure Resource Manager template and created an Azure Site Recovery vault that will be used to replicate content of the Azure VM disk files.

Exercise 2: Migrate an Azure VM between Azure regions by using Azure Site Recovery.

The main tasks for this exercise are as follows:

- Configure Azure VM replication.
- Review Azure VM replication settings.

Result: After you completed this exercise, you have configured replication of an Azure VM and reviewed Azure VM replication settings.

Module 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 developing a storage plan that includes Premium storage. Which storage redundancy type is available to use? Select one.

- Locally redundant storage
- Zone-redundant storage
- Geo-redundant storage
- Read-access geo-redundant storage

Review Question 3

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 4

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 5

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 6

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 7

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 8

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 9

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

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 developing a storage plan that includes Premium storage. Which storage redundancy type is available to use? Select one.

- Locally redundant storage
- Zone-redundant storage
- Geo-redundant storage
- Read-access geo-redundant storage

Explanation

Locally redundant storage is best for high usage log information.

Review Question 3

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 4

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 5

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 6

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 7

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 8

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 9

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.

Module 8 Network Traffic Management

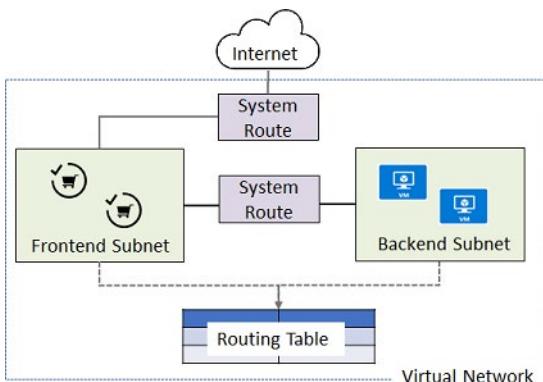
Network Routing

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.
- Communication between VMs using a VNet-to-VNet VPN.
- 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.

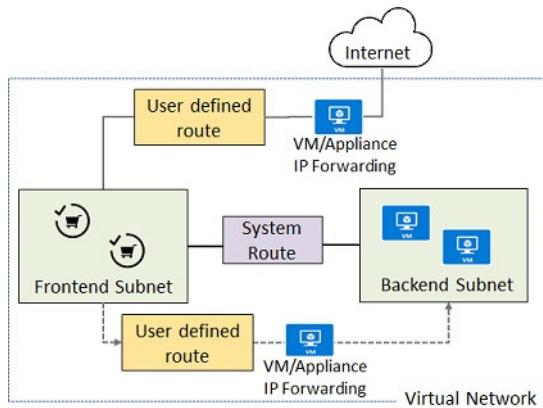


Information about the system routes is recorded in a route table. A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network. Route tables are associated to subnets, and each packet leaving a subnet is handled based on the associated route table.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

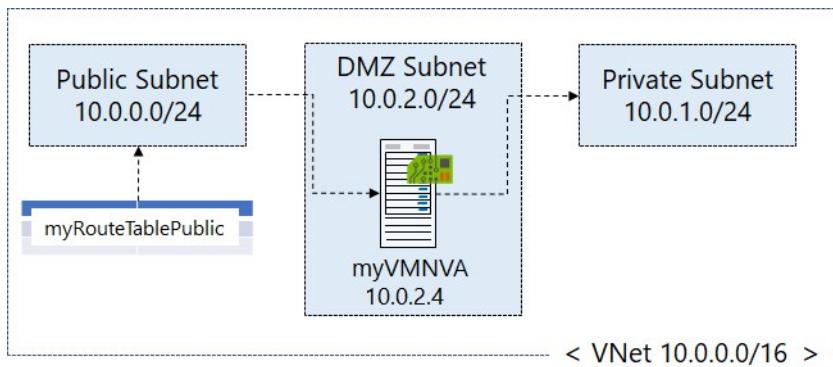
For more information:

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

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.



- ✓ In the next three topics we will review at how to: create the routing table, create a custom route, and associate the route to the subnet.

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 **Border Gateway Protocol (BGP)**¹ route propagation.

Create route table

You can add routes to this table after it's created.

* Name: myRouteTablePublic

* Subscription: Visual Studio Enterprise

* Resource group: Create new (radio button) Use existing (radio button) [dropdown]

* Location: East US

BGP route propagation: Disabled (button) Enabled (button, highlighted)

BGP is the standard routing protocol commonly used on the Internet to exchange routing and reachability information between two or more networks. Routes are automatically added to the route table for all subnets with BGP 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 our example, the routing table is named *myRouteTablePublic* and BGP is enabled.

For more information:

Overview of BGP with Azure VPN Gateways - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview?toc=%2fazure%2fvirtual-network%2ftoc.json>

Create a Custom Route

For our example,

- The new route is named *ToPrivateSubnet*.

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

- 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.

The screenshot shows the 'Add route' dialog box. It includes fields for 'Route name' (ToPrivateSubnet), 'Address prefix' (10.0.1.0/24), 'Next hop type' (Virtual appliance selected), and 'Next hop address' (10.0.2.4).

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

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.

The screenshot shows the Azure portal interface for managing subnets. It displays the 'Save' button, the 'Address range (CIDR block)' (10.0.0.0/24), and the 'Route table' dropdown. The 'Route table' dropdown is highlighted with a red box, showing options like 'None' and '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, you 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*
 - **BGP 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.

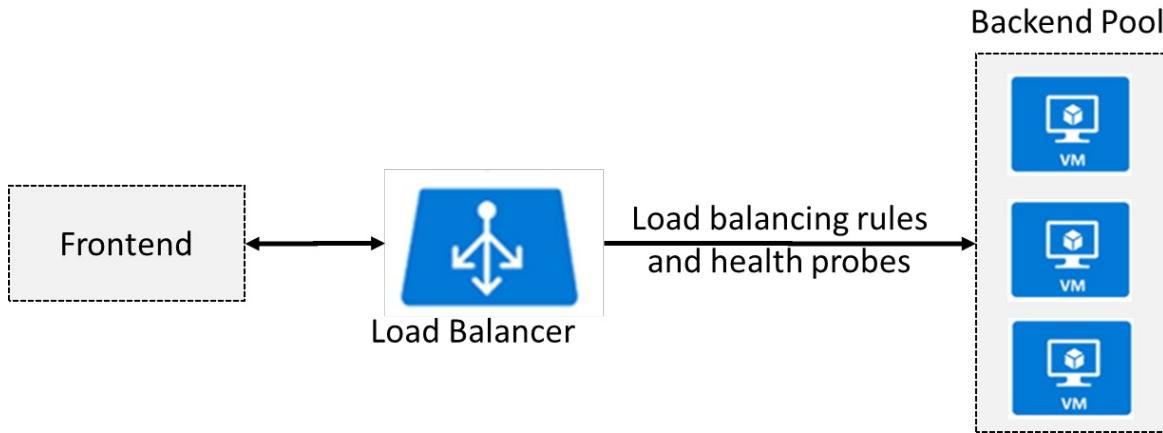
```
Get-AzRouteTable
```

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

Azure Load Balancer

Azure Load Balancer

The Azure Load Balancer delivers high availability and network performance to your applications. It is an OSI Layer 4 (TCP and UDP) load balancer that 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 flows for all TCP and UDP applications.

- ✓ 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:

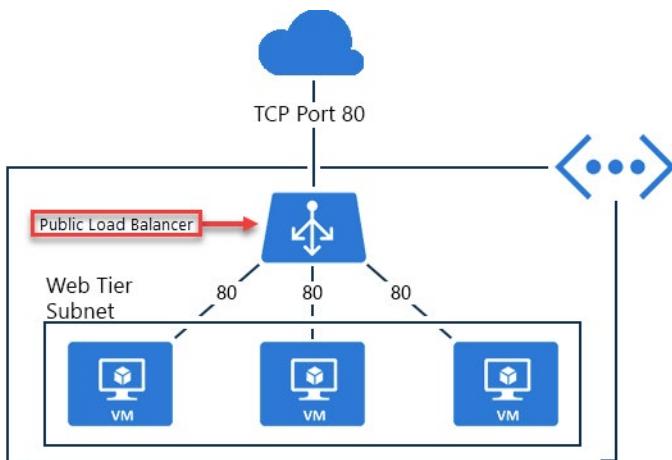
Load Balancer documentation - <https://docs.microsoft.com/en-us/azure/load-balancer/>

Public Load Balancer

There are two types of load balancers: **public** and **internal**.

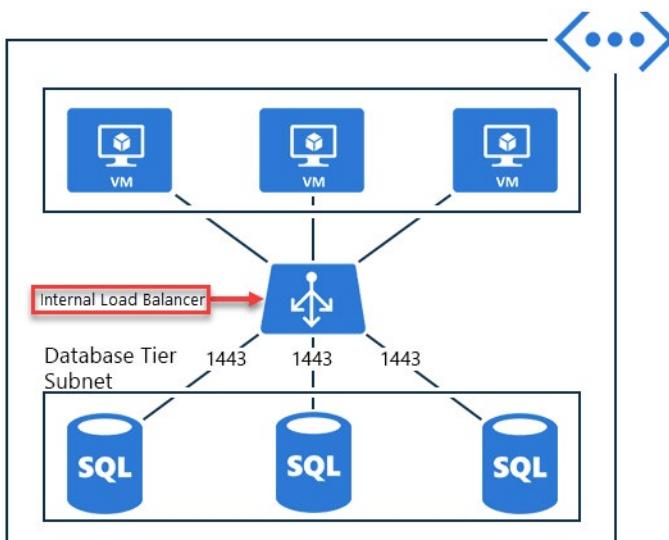
A public load balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the VM, and vice versa for the response traffic from the VM. By applying load-balancing rules, you can distribute specific types of traffic across multiple VMs or services. 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.



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.



Here is some general information about the SKUs.

- 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.

Backend Pools

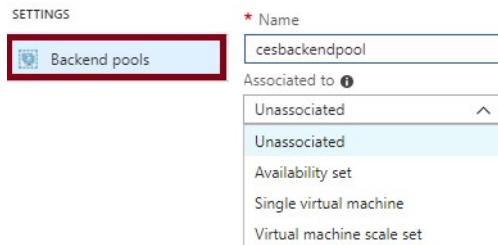
To distribute traffic, a back-end address pool contains the IP addresses of the virtual NICs that are connected to the load balancer.



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.

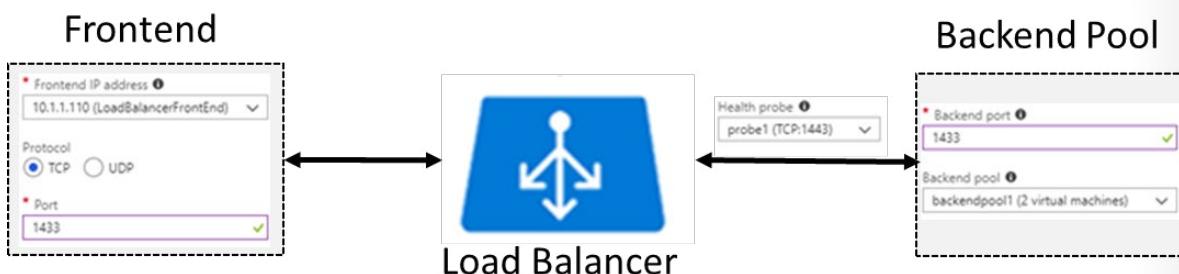
Backend pools are configured from the Backend Pool blade. For the Standard SKU you can connect to an Availability set, single virtual machine, or a virtual machine scale set.



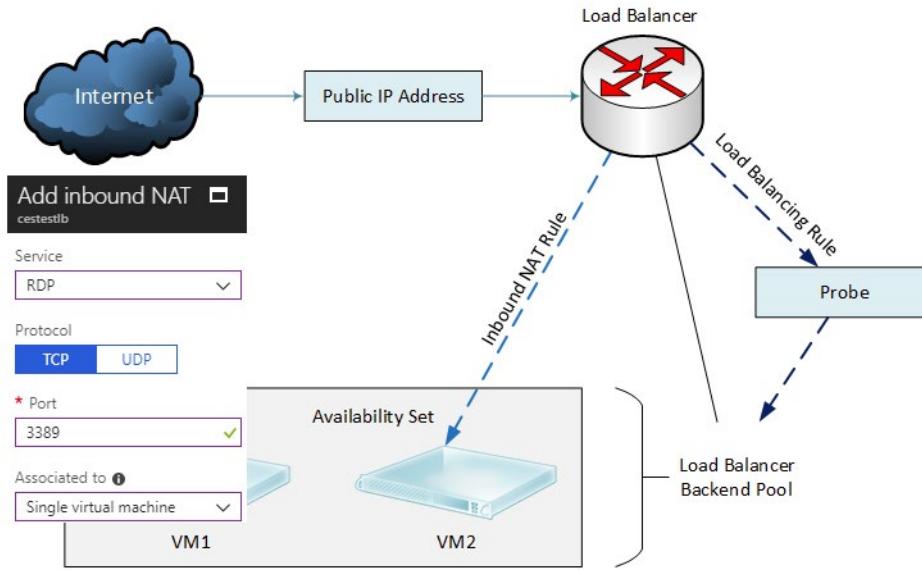
- ✓ In the Standard SKU you can have up to 1000 instances in the backend pool. In the Basic SKU you can have up to 100 instances.

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 SQL (port 1433) servers. The rule uses a health probe that checks on TCP 1443.



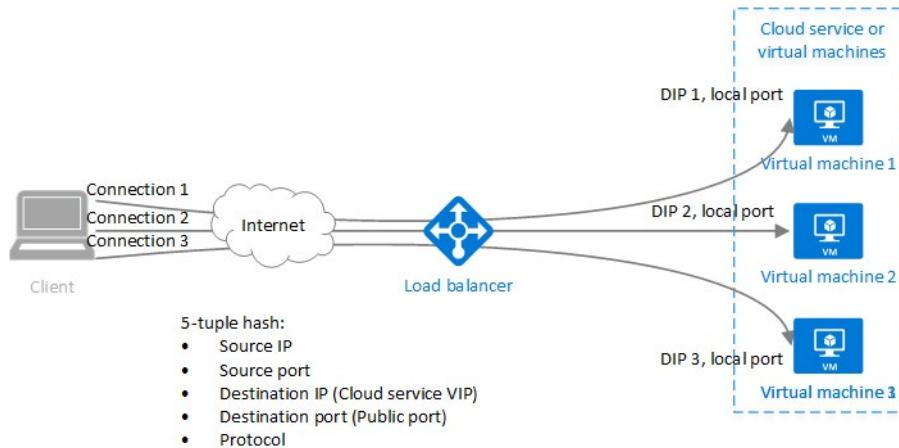
Load balancing rules can be used in combination with NAT rules. For example, you could use NAT from the load balancer's public address to TCP 3389 on a specific virtual machine. This allows remote desktop access from outside of Azure. Notice in this case, the NAT rule is explicitly attached to a VM (or network interface) to complete the path to the target; whereas a Load Balancing rule need not be.



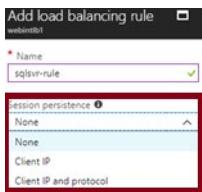
- ✓ Do you understand the difference between load balancing rules and NAT rules? Remember, this approach should only be used when you need connectivity from the Internet. Most normal communications would occur from on-premises to Azure connections such as site-to-site VPN and ExpressRoute.

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**.

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).

Protocol
HTTP
TCP
* Port
80
* Path
/
* Interval
5
seconds
* Unhealthy threshold
2
consecutive failures

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.

Protocol

HTTP TCP

* Port
80

* Interval ⓘ
5 seconds

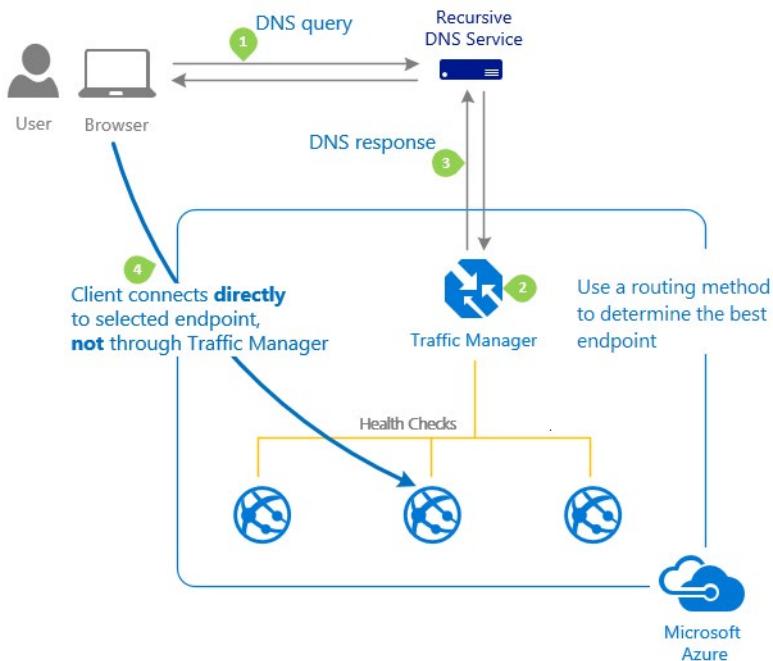
* Unhealthy threshold ⓘ
2 consecutive failures

- ✓ 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 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.

For more information:

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

Traffic Manager Features

Azure Traffic Manager provides quick setup, great performance, and application availability. Traffic Manager enables you to control how traffic is distributed across your application endpoints. An endpoint can be any Internet-facing endpoint, hosted in Azure or outside Azure.

Here are some specific ways you can use Traffic Manager.

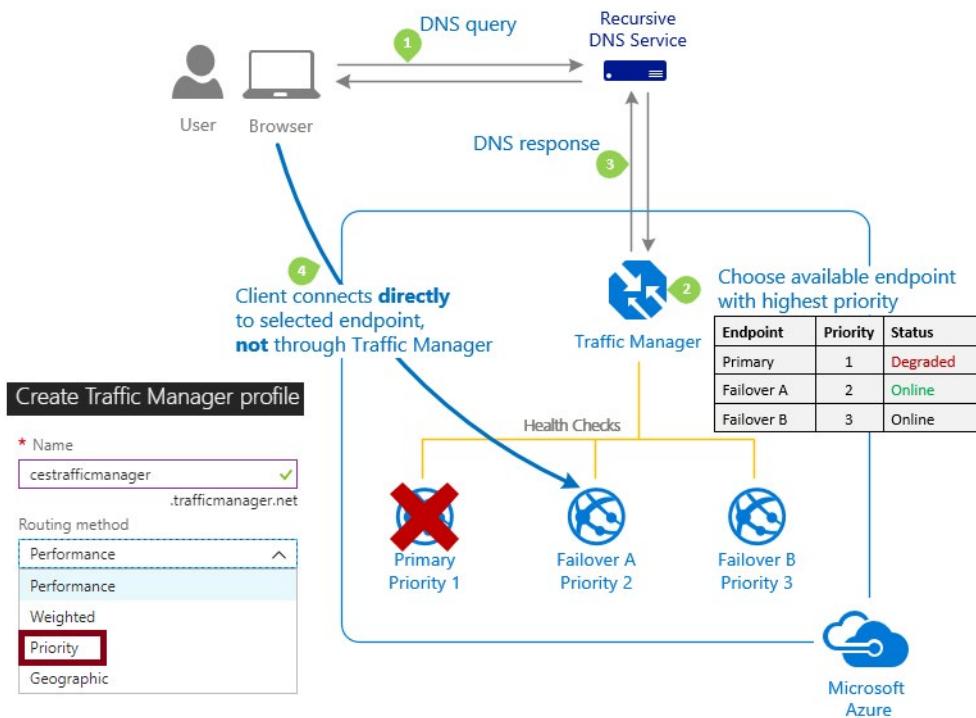
- **Improve availability of critical applications.** Traffic Manager allows you to deliver high availability for your critical applications by monitoring your endpoints in Azure and providing automatic failover when an endpoint goes down.

- **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.
- ✓ We will be covering the four basic routing methods: Priority, Performance, Geographic, and Weighted. These methods can be combined into what is known as nested Traffic Manager profiles. Azure recently added Multvalue and Subnet routing methods. These will not be covered in the course.

Priority Routing

Scenario: An organization wants to provide reliability for its services by deploying one or more backup services in case their primary service goes down.

In this case the Traffic Manager profile 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.



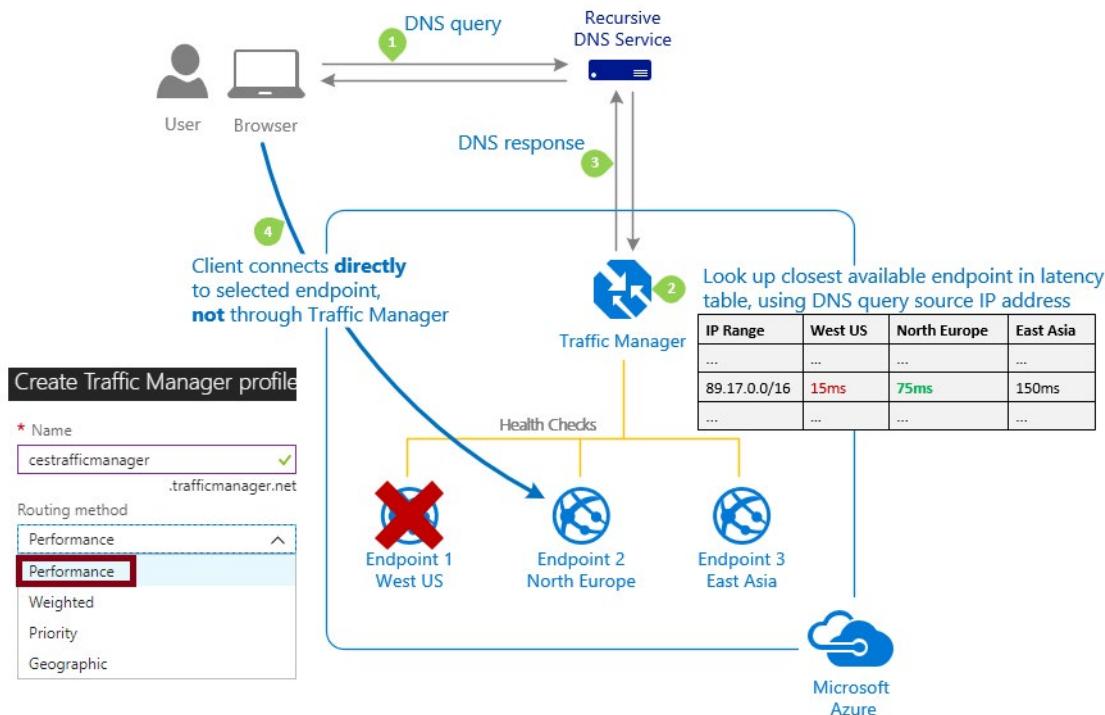
The Priority traffic routing method allows you to easily implement a failover pattern. You configure the endpoint priority explicitly or use the default priority based on the endpoint order.

- ✓ Can you think of another example, other than failover, where the Priority routing method could be used?

Performance Routing

Scenario: An organization has deployed endpoints in two or more locations across the globe and wants to ensure users are routed to achieve the best responsiveness. For example, an application can be hosted in West Europe and West US. A user from Denmark can reasonably expect to be served by the endpoint residing in the West Europe datacenter and should experience lower latency and higher responsiveness.

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 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.



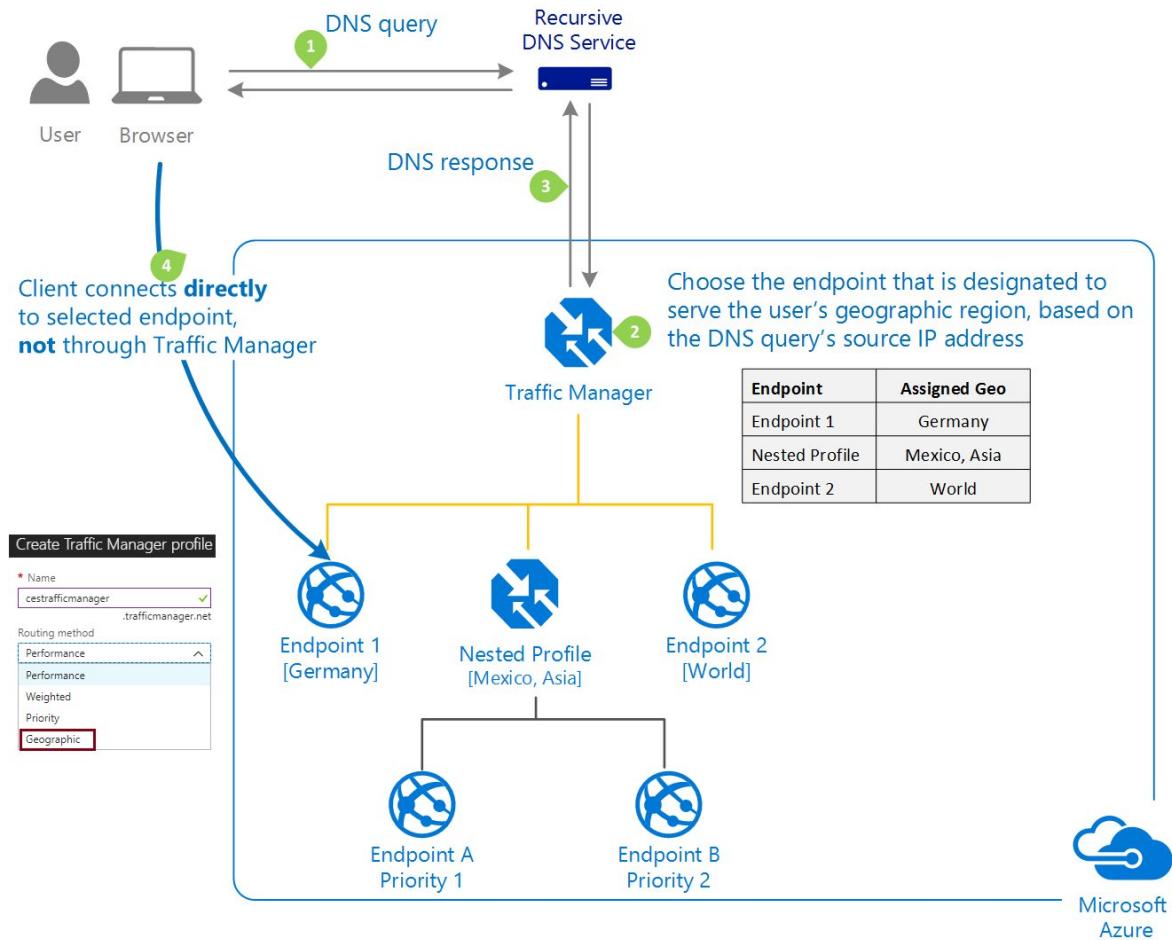
With this method Traffic Manager looks up the source IP address of the incoming DNS request in the Internet Latency Table. Traffic Manager chooses an available endpoint in the Azure datacenter that has the lowest latency for that IP address range, then returns that endpoint in the DNS response.

- ✓ Remember Traffic Manager does not receive DNS queries directly from clients. Rather, DNS queries come from the recursive DNS service that the clients are configured to use. Therefore, the IP address used to determine the 'closest' endpoint is not the client's IP address, but it is the IP address of the recursive DNS service. In practice, this IP address is a good proxy for the client.

Geographic Routing

Scenario: In certain organizations knowing a user's geographic region and routing them based on that is very important. Examples include complying with data sovereignty mandates, localization of content and user experience, and measuring traffic from different regions.

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.



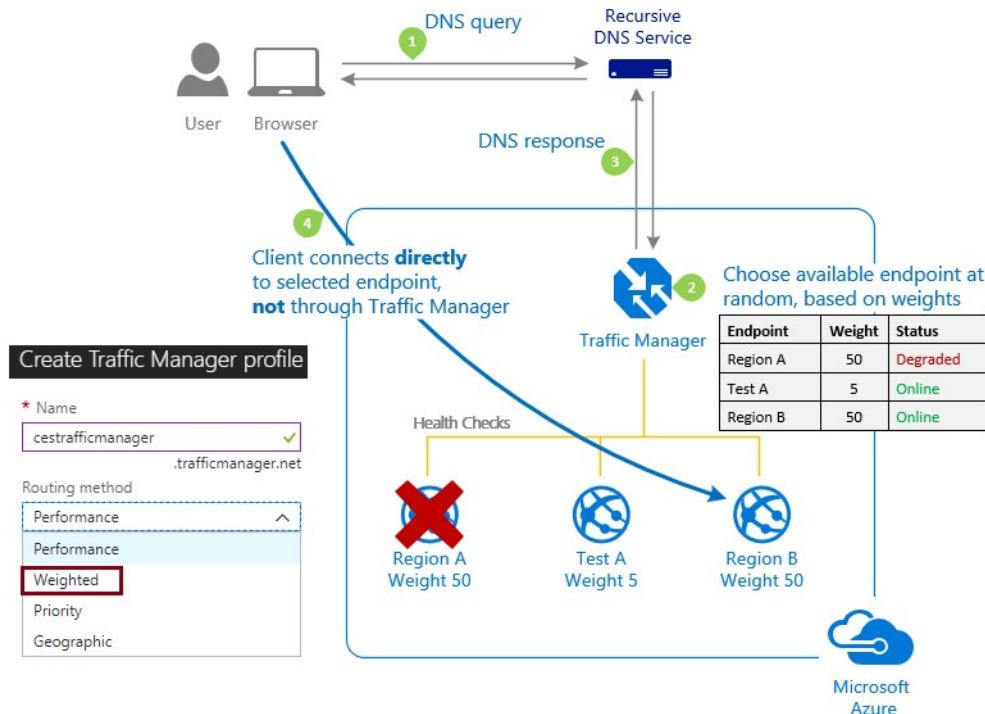
Some planning is required when you create a geographical endpoint. A location cannot be in more than one endpoint. You build the endpoint from a:

- **Regional Grouping.** For example, All (World), Europe, Middle East, or Asia.
- **Country/Region.** For example, Europe □ Denmark and Middle East □ Turkey.
- **State/Province** (only available in Australia, Canada, UK, and USA). For example, North America / Central America / Caribbean □ United States □ Maryland or North America / Central America / Caribbean □ Canada □ Ontario.
- ✓ Similar to Performance routing Traffic Manager uses the source IP address of the DNS query to determine the region from which a user is querying from. Usually, this is the IP address of the local DNS resolver doing the query on behalf of the user.

Weighted Routing

Scenario: Sometimes an organization wants to prefer one endpoint over another. For example, if you are testing or bringing a new endpoint online and want to gradually increase traffic over time.

The Weighted traffic-routing method allows you to distribute traffic evenly or to use a pre-defined weighting.



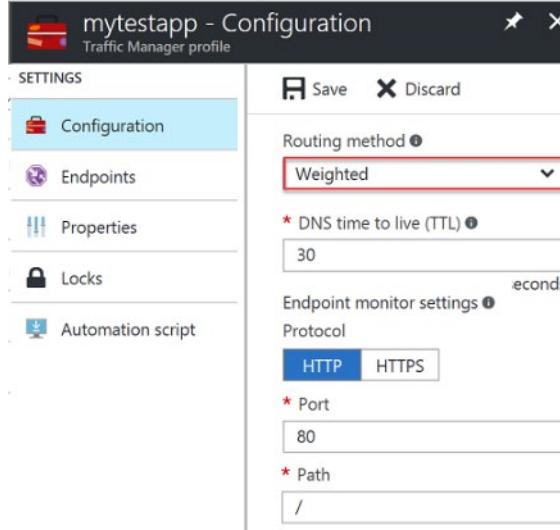
In the Weighted traffic-routing method, you assign a weight to each endpoint in the Traffic Manager profile configuration. The weight is an integer from 1 to 1000. This parameter is optional. If omitted, Traffic Manager uses a default weight of '1'. The higher weight, the higher the priority.

- ✓ Using the same weight across all endpoints results in an even traffic distribution. Using higher or lower weights on specific endpoints causes those endpoints to be returned more or less frequently in the DNS responses.

Implementing Traffic Manager Profiles

To implement Traffic Manager you must create a profile. The profile will include the routing method and the DNS time to live (TTL). The TTL value controls how often the client's local caching name server will query the Traffic Manager system for updated DNS entries. Any change that occurs with Traffic Manager, such as traffic routing method changes or changes in the availability of added endpoints, will take this period of time to be refreshed throughout the global system of DNS servers.

Traffic Manager can monitor your services to ensure they are available. For monitoring to work correctly, you must set it up the same way for every endpoint within this profile. You can specify the protocol, the port, and the relative path. Traffic Manager will try to access the file specified in the relative path via the defined protocol and port to check for uptime.



- ✓ You can Enable or Disable your profile at anytime.

Implementing Traffic Manager Endpoints

Your Traffic Manager profile must also define the endpoints. There are two basic **types** of endpoints:

- **Azure endpoints.** Use this type of endpoint to load balance traffic to a Cloud service, Web app, or Public IP address in the same subscription.
- **External endpoints.** Use this type of endpoint to load balance traffic to any fully-qualified domain name (FQDN), even for applications not hosted in Azure.

For example, you could create a weighted Traffic Manager profile and add endpoints for publicly accessible virtual machines.

- ✓ You will implement the weighted routing method in the lab.

Traffic Manager vs Load Balancer

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

Service	Azure Load Balancer	Traffic Manager
Technology	Transport (Layer 4)	DNS
Protocols	Any	Any HTTP/S endpoint needed for endpoint monitoring
Endpoints	Azure VMs and Cloud Services role instances	Azure VMs, Cloud Services, Azure Web Apps, and external endpoints
Network connectivity	Both internet-facing and internal (VNet) applications	Internet-facing only

Lab and Review Questions

Lab - Load Balancer and Traffic Manager

Scenario

Adatum Corporation wants to implement Azure VM-hosted web workloads and facilitate their management for its subsidiary Contoso Corporation in a highly available manner by leveraging load balancing and Network Address Translation (NAT) features of Azure Load Balancer

Objectives

After completing this lab, you will be able to:

- Deploy Azure VMs by using Azure Resource Manager templates.
- Implement Azure Load Balancing.
- Implement Azure Traffic Manager load balancing.

Exercise 0: Deploy Azure VMs by using Azure Resource Manager templates.

The main tasks for this exercise are as follows:

- Deploy management Azure VMs running Windows Server 2016 Datacenter with the Web Server (IIS) role installed into an availability set in the first Azure region by using an Azure Resource Manager template.
- Deploy management Azure VMs running Windows Server 2016 Datacenter with the Web Server (IIS) role installed into an availability set in the second Azure region by using an Azure Resource Manager template.

Result: After you completed this exercise, you have used Azure Resource Manager templates to initiate deployment of Azure VMs running Windows Server 2016 Datacenter with the Web Server (IIS) role installed into availability sets in two Azure regions.

Exercise 1: Implement Azure Load Balancing.

The main tasks for this exercise are as follows:

- Implement Azure load balancing rules in the first region.
- Implement Azure load balancing rules in the second region.
- Implement Azure NAT rules in the first region.
- Implement Azure NAT rules in the second region.
- Verify Azure load balancing and NAT rules.

Result: After you completed this exercise, you have implemented and verified load balancing rules and NAT rules of Azure load balancers in both regions.

Exercise 2: Implement Azure Traffic Manager load balancing.

The main tasks for this exercise are as follows:

- Assign DNS names to public IP addresses of Azure load balancers.
- Implement Azure Traffic Manager load balancing.
- Verify Azure Traffic Manager load balancing.

Result: After you completed this exercise, you have implemented and verified Azure Traffic Manager load balancing.

Module 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?

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

Review Question 2

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 3

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 4

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 5

Azure Traffic Manager is a good solution for load balancing traffic (select three):

- at hosted providers.
- in the same cloud.
- in different Azure regions.
- in on-premises datacenters.
- based on the HTTP protocol.

Review Question 6

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 Content Delivery Network
- Azure Cloud Services

Review Question 7

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?

- 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 8

You have been considering whether to install a Basic or Standard load balancer SKU. Which of the following is true? Select one.

- If you change your mind, you can switch from the Basic to the Standard SKU.
- There is no price difference between the Basic and Standard SKU.
- A Standard load balancer cannot span two virtual networks.
- Load balancer frontends are accessible across global virtual network peering.

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?

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

Explanation

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 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 3

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

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 4

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 5

Azure Traffic Manager is a good solution for load balancing traffic (select three):

- at hosted providers.
- in the same cloud.
- in different Azure regions.
- in on-premises datacenters.
- based on the HTTP protocol.

Explanation

You can use Traffic Manager to load balance between endpoints that are located in different Azure regions, at hosted providers, or in on-premises datacenters. These endpoints can include Azure VMs and Azure websites. You can configure this load-balancing service to support priority or to ensure that users connect to an endpoint that is close to their physical location for faster response.

Review Question 6

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 Content Delivery Network
- Azure Cloud Services

Explanation

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 7

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?

- 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 8

You have been considering whether to install a Basic or Standard load balancer SKU. Which of the following is true? Select one.

- If you change your mind, you can switch from the Basic to the Standard SKU.
- There is no price difference between the Basic and Standard SKU.
- A Standard load balancer cannot span two virtual networks.
- Load balancer frontends are accessible across global virtual network peering.

Explanation

A Load Balancer rule cannot span two virtual networks. Frontends and their related backend instances must be in the same virtual network.

Module 9 Azure Active Directory

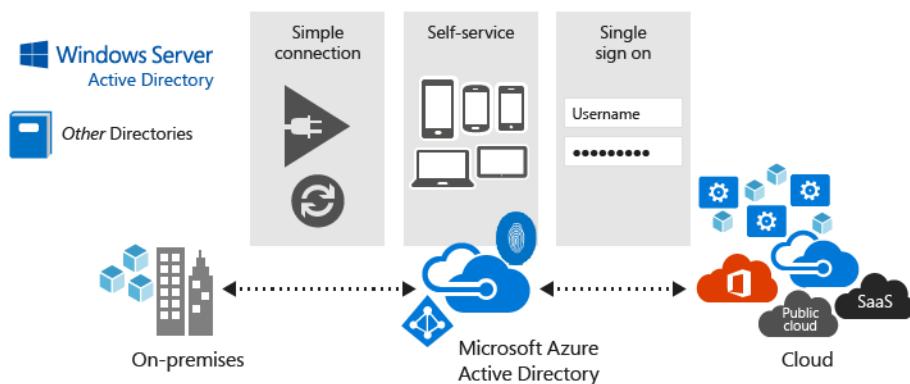
Azure Active Directory

Azure Active Directory

For both IT Admins and Developers

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.com, 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.



Identity manage capabilities and integration

Azure AD also includes a full suite of identity management capabilities including multi-factor authentication, device registration, self-service password management, self-service group management, privileged account management, role-based access control, application usage monitoring, rich auditing and security monitoring, and alerting. These capabilities can help secure cloud-based applications, streamline IT processes, cut costs, and help assure corporate compliance goals are met.

Additionally, Azure AD can be integrated with an existing Windows Server Active Directory, giving organizations the ability to leverage their existing on-premises identity investments to manage access to cloud based SaaS applications.

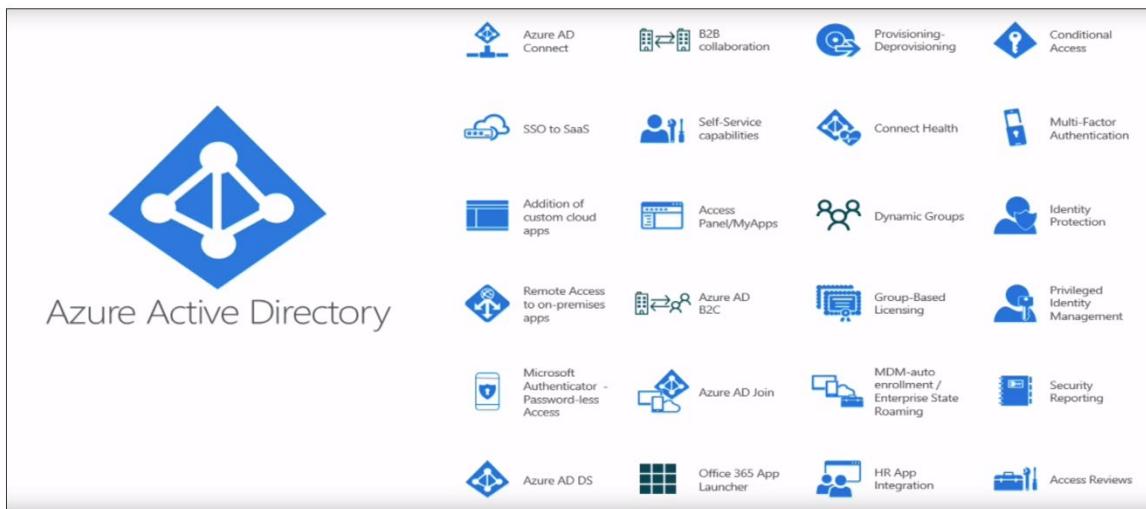
- ✓ If you are an Office365, Azure or Dynamics CRM Online customer, you might not realize that you are already using Azure AD. Every Office365, Azure and Dynamics CRM tenant is already an Azure AD tenant. Whenever you want you can start using that tenant to manage access to thousands of other cloud applications Azure AD integrates with.

For more information:

Azure Active Directory Documentation - <https://docs.microsoft.com/en-us/azure/active-directory/>

Azure Active Directory Benefits

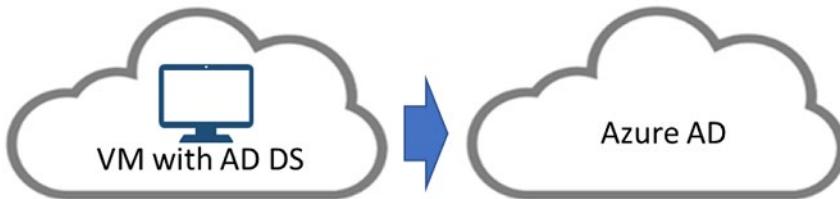
Azure AD has many benefits



- **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.
- ✓ What reasons do you have for considering Azure Active Directory?

Azure Active Directory Differences



Active Directory Domain Services (AD DS)

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**, **Basic**, **Premium P1**, and **Premium P2**. The Free edition is included with an Azure subscription. The Azure Active Directory Basic, Premium P1, and Premium P2 editions are built on top of your existing free directory, providing enterprise class capabilities spanning self-service, enhanced monitoring, security reporting, Multi-Factor Authentication (MFA), and secure access for your mobile workforce.



- **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 Basic** - In addition to the Free features, Basic also provides cloud-centric app access, group-based access management, self-service password reset for cloud apps, and Azure AD Application Proxy, which lets you publish on-premises web apps using Azure AD.
 - **Azure Active Directory Premium P1** - In addition to the Free and Basic 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, Basic, 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](#)¹ 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 Directories (Tenants)

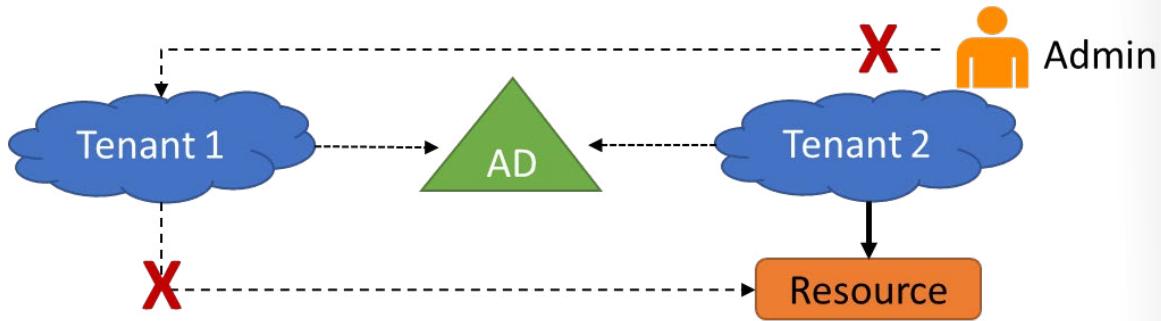
A tenant is a dedicated instance of an Azure AD directory which is created whenever you sign up for a Microsoft cloud service, such as Office 365 or Azure. It is important to note; a tenant is not the same as a subscription. A subscription is typically tied to a credit card for billing, where a tenant is an instance of Active Directory. You can have multiple tenants in your organization, such as Contoso1.com and Contoso2.com .

Each tenant or Azure AD instance is separate and distinct from the other Azure AD directories in your organization. These different tenants could allow for different functions. For example: You could have a tenant for Office 365, another tenant for testing environment, and then another tenant for Microsoft Intune. A tenant houses the users in a company and the information about them - their passwords, user profile data, permissions, and so on. It also contains groups, applications, and other information pertaining to an organization and its security.

Why would you need multiple tenants

Resource independence

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



- 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:

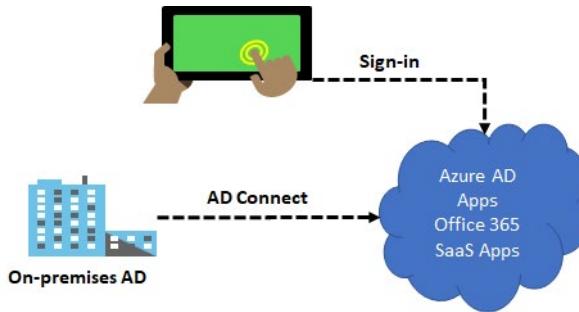
- By default, the user who creates a tenant is added as an external user in that new tenant and assigned the global administrator role in that tenant.
- The administrators of tenant 'Contoso' have no direct administrative privileges to tenant 'Test,' unless an administrator of 'Test' specifically grants them these privileges.

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 or the Forefront Identity Manager Azure Active Tenant Connector.

Azure Active Directory Connect

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 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.

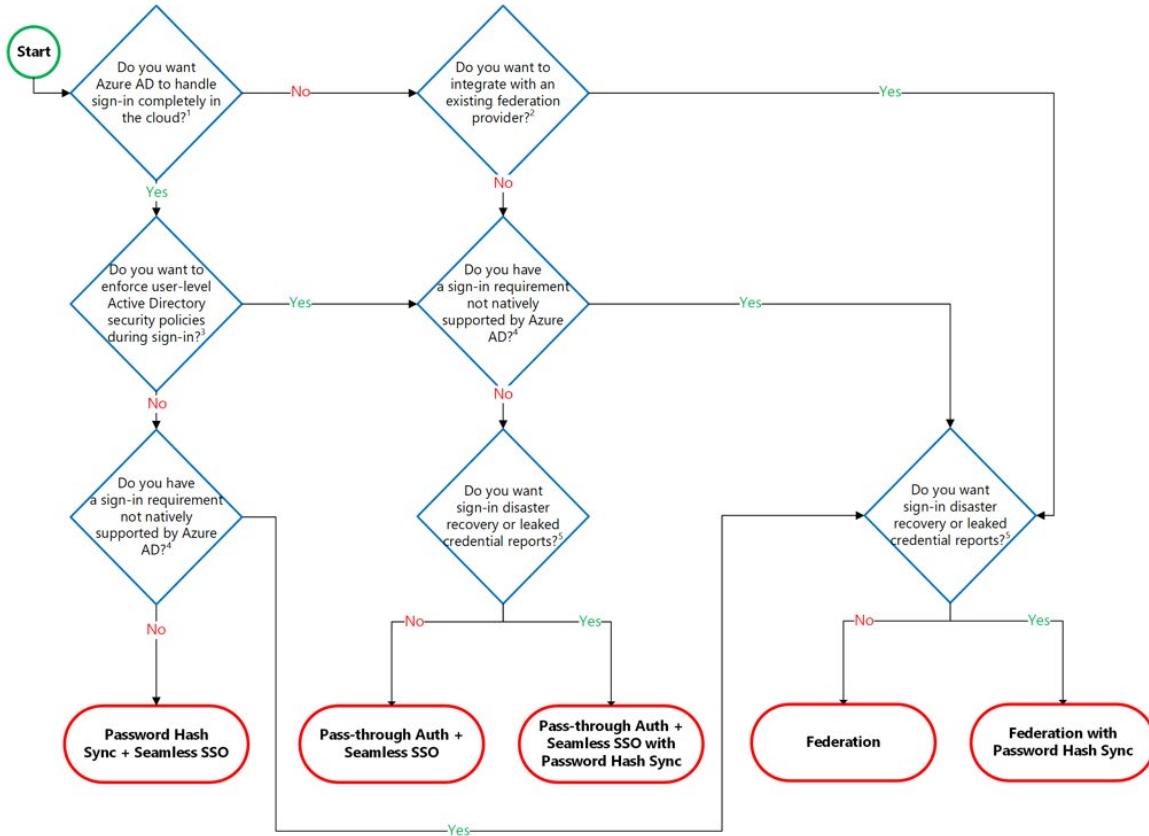
For more information:

Integrate your on-premises directories with Azure Active Directory - <https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect>

Authentication Options

Choosing an Azure AD Authentication method is important as it is one of the first important decisions when moving to the cloud as it will be the foundation of your cloud environment and is difficult to change at a later date.

You can choose cloud authentication which includes: Azure AD password hash synchronization and Azure AD Pass-through Authentication. You can also choose federated authentication where Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password.



Summary

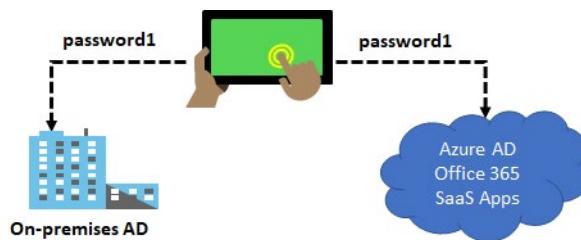
1. Do you need on-premises Active Directory integration? If the answer is No, then you would use Cloud-Only authentication.
2. If you do need on-premises Active Directory integration, then do you need to use cloud authentication, password protection, and your authentication requirements are natively supported by Azure AD? If the answer is Yes, Then you would use **Password Hash Sync** + Seamless SSO.
3. If you do need on-premises Active Directory integration, but you do not need to use cloud authentication, password protection, and your authentication requirements are natively supported by Azure AD, then you would use **Pass-through Authentication** Seamless SSO.
4. If you need on-premises Active Directory integration, have an existing federation provider and your authentication requirements are NOT natively supported by Azure AD, then you would use **Federation** authentication.

For more information:

Video - How to choose the right authentication option in Azure Active Directory - <https://www.youtube.com/watch?v=YtW2cmVqSEw>

Password Hash Synchronization

The probability that you're blocked from getting your work done due to a forgotten password is related to the number of different passwords you need to remember. The more passwords you need to remember, the higher the probability to forget one. Questions and calls about password resets and other password-related issues demand the most helpdesk resources.



Password hash synchronization (PHS) is a feature used to synchronize user passwords from an on-premises Active Directory instance to a cloud-based Azure AD instance. Use this feature to sign in to Azure AD services like Office 365, Microsoft Intune, CRM Online, and Azure Active Directory Domain Services (Azure AD DS). You sign in to the service by using the same password you use to sign in to your on-premises Active Directory instance. Password hash synchronization helps you to:

- Improve the productivity of your users.
- Reduce your helpdesk costs.

How does this work?

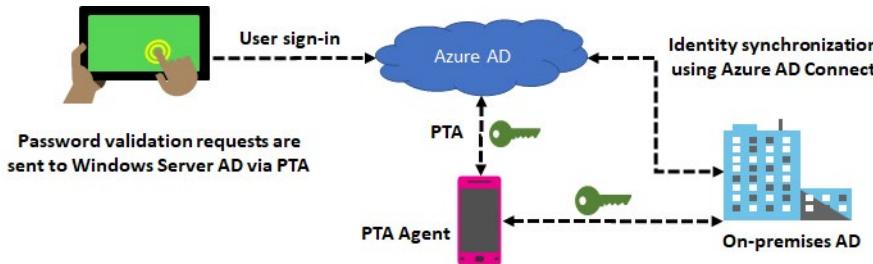
In the background, the password synchronization component takes the user's password hash from on-premises Active Directory, encrypts it, and passes it as a string to Azure. Azure decrypts the encrypted hash and stores the password hash as a user attribute in Azure AD.

When the user signs in to an Azure service, the sign-in challenge dialog box generates a hash of the user's password and passes that hash back to Azure. Azure then compares the hash with the one in that user's account. If the two hashes match, then the two passwords must also match and the user receives access to the resource. The dialog box provides the facility to save the credentials so that the next time the user accesses the Azure resource, the user will not be prompted.

- ✓ It is important to understand that this is **same sign-in**, not single sign-on. The user still authenticates against two separate directory services, albeit with the same user name and password. This solution provides a simple alternative to an AD FS implementation.

Pass-through Authentication

Azure AD Pass-through Authentication (PTA) is an alternative to Azure AD Password Hash Synchronization, and provides the same benefit of cloud authentication to organizations. PTA allows users to sign in to both on-premises and cloud-based applications using the same user account and passwords. When users sign-in using Azure AD, Pass-through authentication validates the users' passwords directly against an organizations on-premise Active Directory.

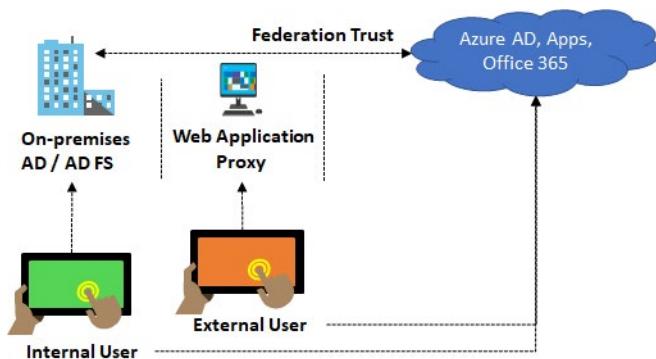


Feature benefits

- Supports user sign-in into all web browser-based applications and into Microsoft Office client applications that use modern authentication.
- Sign-in usernames can be either the on-premises default username (`userPrincipalName`) or another attribute configured in Azure AD Connect (known as Alternate ID).
- Works seamlessly with conditional access features such as Multi-Factor Authentication to help secure your users.
- Integrated with cloud-based self-service password management, including password writeback to on-premises Active Directory and password protection by banning commonly used passwords.
- Multi-forest environments are supported if there are forest trusts between your AD forests and if name suffix routing is correctly configured.
- PTA is a free feature, and you don't need any paid editions of Azure AD to use it.
- PTA can be enabled via Azure AD Connect.
- PTA uses a lightweight on-premises agent that listens for and responds to password validation requests.
- Installing multiple agents provides high availability of sign-in requests.
- PTA protects your on-premises accounts against brute force password attacks in the cloud.
- ✓ This feature can be configured without using a federation service so that any organization, regardless of size, can implement a hybrid identity solution. Pass-through authentication is not only for user sign-in but allows an organization to use other Azure AD features, such as password management, role-based access control, published applications, and conditional access policies.

Federation with Azure AD

Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization. A typical federation might include a number of organizations that have established trust for shared access to a set of resources.



You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises. This method allows administrators to implement more rigorous levels of access control.

- ✓ If you decide to use Federation with Active Directory Federation Services (AD FS), you can optionally set up password hash synchronization as a backup in case your AD FS infrastructure fails.

Password Writeback

Having a cloud-based password reset utility is great but most companies still have an on-premises directory where their users exist. How does Microsoft support keeping traditional on-premises Active Directory (AD) in sync with password changes in the cloud?

Password writeback is a feature enabled with Azure AD Connect that allows password changes in the cloud to be written back to an existing on-premises directory in real time.

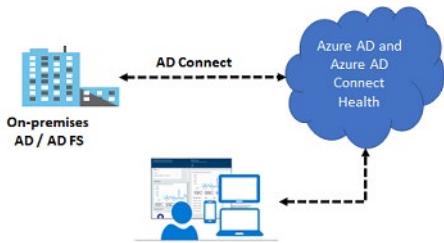


Password writeback provides:

- **Enforcement of on-premises Active Directory password policies.** When a user resets their password, it is checked to ensure it meets your on-premises Active Directory policy before committing it to that directory. This review includes checking the history, complexity, age, password filters, and any other password restrictions that you have defined in local Active Directory.
 - **Zero-delay feedback.** Password writeback is a synchronous operation. Your users are notified immediately if their password did not meet the policy or could not be reset or changed for any reason.
 - **Supports password changes from the access panel and Office 365.** When federated or password hash synchronized users come to change their expired or non-expired passwords, those passwords are written back to your local Active Directory environment.
 - **Supports password writeback when an admin resets them from the Azure portal.** Whenever an admin resets a user's password in the Azure portal, if that user is federated or password hash synchronized, the password is written back to on-premises. This functionality is currently not supported in the Office admin portal.
 - **Doesn't require any inbound firewall rules.** Password writeback uses an Azure Service Bus relay as an underlying communication channel. All communication is outbound over port 443.
- ✓ To use SSPR you must have already configured Azure AD Connect in your environment.

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.



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.

Azure AD Join

Device Management

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.

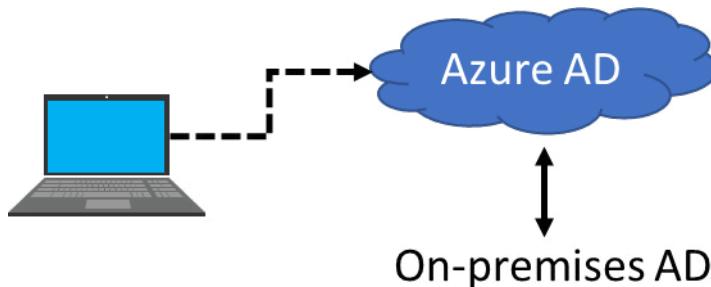
To get a device under the control of Azure AD, you have two options:

- **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.

For more information:

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

Azure AD Joined Devices

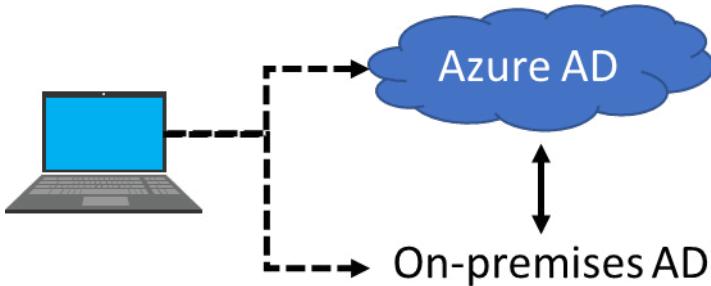


Azure AD Join is designed to provide access to organizational apps and resources and to simplify Windows deployments of work-owned devices. AD Join has these benefits.

- **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 Windows 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.
- ✓ 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.

Hybrid AD Joined Devices



If your environment has an on-premises AD footprint and you also want to benefit from the capabilities provided by Azure Active Directory, you can implement hybrid Azure AD joined devices. These are devices that are joined both to your on-premises Active Directory and your Azure Active Directory.

Joining devices to both directories allows:

- IT departments to manage work-owned devices from a central location.
- Users to sign in to their devices with their Active Directory work or school accounts.

Here is a comparison of Registered, AD Joined, and Hybrid AD Joined devices.

	Registered Devices	Azure AD Joined Devices	Hybrid AD Joined Devices
Device Type	Personal	Organization owned	Organization owned
Registration	Manual	Manual	Automatic
Operating System	Windows 10	Windows 10	Windows 7, 8, and 10

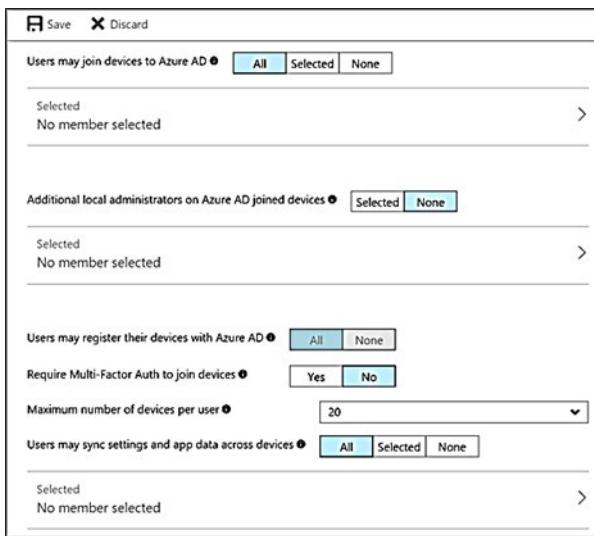
- ✓ Are you understanding the different types of joined devices? Which do you think your organization needs?

For more information:

Hybrid Azure AD joined devices - <https://docs.microsoft.com/en-us/azure/active-directory/device-management-introduction#hybrid-azure-ad-joined-devices>

Configuring Azure AD Join

To manage your devices using the Azure portal, your devices need to be either registered or joined to Azure AD. As an administrator, you can fine-tune the process of registering and joining devices by configuring the device settings.



Users may join devices to Azure AD - This setting enables you to select the users who can join devices to Azure AD. The default is All. This setting is only applicable to Azure AD Join on Windows 10.

Additional local administrators on Azure AD joined devices - You can select the users that are granted local administrator rights on a device. Users added here are added to the Device Administrators role in Azure AD. Global administrators in Azure AD and device owners are granted local administrator rights by default. This option is a premium edition capability available through products such as Azure AD Premium or the Enterprise Mobility Suite (EMS).

Users may register their devices with Azure AD - You need to configure this setting to allow devices to be registered with Azure AD. If you select None, devices are not allowed to register when they are not Azure AD joined or hybrid Azure AD joined. Enrollment with Microsoft Intune or Mobile Device Management (MDM) for Office 365 requires registration. If you have configured either of these services, ALL is selected and NONE is not available.

Require Multi-Factor Auth to join devices - You can choose whether users are required to provide a second authentication factor to join their device to Azure AD. The default is No. We recommend requiring multi-factor authentication when registering a device. Before you enable multi-factor authentication for this service, you must ensure that multi-factor authentication is configured for the users that register their devices. This setting does not impact hybrid join for Windows 10 or Windows 7. This is only applicable to Azure AD Join on Windows 10 and BYO device registration for Windows 10, iOS, and Android.

Maximum number of devices - This setting enables you to select the maximum number of devices that a user can have in Azure AD. If a user reaches this quota, they are not be able to add additional devices until one or more of the existing devices are removed. The device quote is counted for all devices that are either Azure AD joined or Azure AD registered today. The default value is 20.

Users may sync settings and app data across devices - By default, this setting is set to NONE. Selecting specific users or groups or ALL allows the user's settings and app data to sync across their Windows 10 devices. Learn more on how sync works in Windows 10. This option is a premium capability available through products such as Azure AD Premium or the Enterprise Mobility Suite (EMS).

Lab and Review Questions

Lab - Implement Directory Synchronization

Scenario

Adatum Corporation wants to integrate its Active Directory with Azure Active Directory.

Objectives

After completing this lab, you will be able to:

- Deploy an Azure VM hosting an Active Directory domain controller
- Create and configure an Azure Active Directory tenant
- Synchronize Active Directory forest with an Azure Active Directory tenant

Exercise 1: Deploy an Azure VM hosting an Active Directory domain controller.

The main tasks for this exercise are as follows:

- Identify an available DNS name for an Azure VM deployment.
- Deploy an Azure VM hosting an Active Directory domain controller by using an Azure Resource Manager template.

Result: After you completed this exercise, you have initiated deployment of an Azure VM that will host an Active Directory domain controller by using an Azure Resource Manager template.

Exercise 2: Create and configure an Azure Active Directory tenant.

The main tasks for this exercise are as follows:

- Create an Azure Active Directory (AD) tenant.
- Add a custom DNS name to the new Azure AD tenant.
- Create an Azure AD user with the Global Administrator role.

Result: After you completed this exercise, you have created an Azure AD tenant, added a custom DNS name to the new Azure AD tenant, and created an Azure AD user with the Global Administrator role.

Exercise 3: Synchronize Active Directory forest with an Azure Active Directory tenant.

The main tasks for this exercise are as follows:

- Configure Active Directory in preparation for directory synchronization.
- Install Azure AD Connect.
- Verify directory synchronization.

Result: After you completed this exercise, you have configured Active Directory in preparation for directory synchronization, installed Azure AD Connect, and verified directory synchronization.

Module 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).

- 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

Your company recently implemented Azure pass-through authentication. Users are now able to authenticate to Azure using their corporate credentials. The management team wants to enhance the user experience. The team comes up with the following requirements.

- Minimize the number of times that users must manually enter credentials

- Minimize on-premises infrastructure

You need to reconfigure the authentication solution to maintain the existing functionality while adding functionality dictated in the requirements. What should you do? Select one.

- Remove Azure pass-through authentication and deploy Active Directory Federation Services (AD FS).
- Deploy Active Directory Federation Services (AD FS).
- Deploy Azure single sign-on.
- Remove Azure pass-through authentication and deploy Azure single sign-on.

Review Question 5

You are planning to deploy Azure AD in a hybrid environment for an organization. You must implement the following features: MFA, SSO, Self-service Password Reset, seamless access to both on-premises and cloud applications, and self-service Bitlocker recovery. Select one.

- Azure Active Directory Free
- Azure Active Directory Basic
- Azure Active Directory Premium P1
- Azure Active Directory Premium P2

Review Question 6

Compliance requires all your Windows 10 devices to be joined to Azure. Your Azure AD Premium subscription will provide all of the following benefits, except? Select one.

- Management through Group Policy
- Automatic enrollment in device management solutions like Intune
- Self-service BitLocker recovery
- Enterprise State Roaming

Review Question 7

Your company has an on-premises AD DS domain that is synced with Microsoft Azure. The company recently implemented Azure pass-through authentication. Everything is functional. A few weeks later, the network team performs a change to the company's firewalls. Thereafter, pass-through authentication stops functioning. You need to put in an emergency change request to open the minimum number of ports so that pass-through authentication functions.

Which ports should you open? Select one.

- Only inbound TCP port 80 and inbound TCP port 443.
- Only inbound and outbound TCP port 443.
- Only outbound TCP port 80 and outbound TCP port 443.
- Only outbound TCP port 443 and inbound TCP port 80.

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

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

Azure AD Connect Health is an Azure AD Premium feature (Connect is available in Free and Basic, but Health requires Premium) 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).

- 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

Your company recently implemented Azure pass-through authentication. Users are now able to authenticate to Azure using their corporate credentials. The management team wants to enhance the user experience. The team comes up with the following requirements.

You need to reconfigure the authentication solution to maintain the existing functionality while adding functionality dictated in the requirements. What should you do? Select one.

- Remove Azure pass-through authentication and deploy Active Directory Federation Services (AD FS).
- Deploy Active Directory Federation Services (AD FS).
- Deploy Azure single sign-on.
- Remove Azure pass-through authentication and deploy Azure single sign-on.

Explanation

The requirements call for maintaining the existing functionality while minimizing the times that users must manually enter credentials. Thus, Azure pass-through authentication should remain in the environment. By deploying Azure single sign-on, you can minimize the number of times that users must manually enter credentials while maintaining existing functionality. Additionally, you do not need to expand the on-premises infrastructure to support the new functionality. While AD FS could meet the requirement to reduce the number of times users enter credentials, it requires an expansion of the on-premises infrastructure.

Review Question 5

You are planning to deploy Azure AD in a hybrid environment for an organization. You must implement the following features: MFA, SSO, Self-service Password Reset, seamless access to both on-premises and cloud applications, and self-service BitLocker recovery. Select one.

- Azure Active Directory Free
- Azure Active Directory Basic
- Azure Active Directory Premium P1
- Azure Active Directory Premium P2

Explanation

Azure AD Premium P1 is most suitable for your deployment.

Review Question 6

Compliance requires all your Windows 10 devices to be joined to Azure. Your Azure AD Premium subscription will provide all of the following benefits, except? Select one.

- Management through Group Policy
- Automatic enrollment in device management solutions like Intune
- Self-service BitLocker recovery
- Enterprise State Roaming

Explanation

One of the major benefits is seamless access to cloud resources by leveraging SSO. In addition, with Azure AD Premium, you also have support for auto-enrollment into a Mobile Device Management solution, such as Microsoft Intune, self-service BitLocker recovery, and Enterprise State Roaming.

Review Question 7

Your company has an on-premises AD DS domain that is synced with Microsoft Azure. The company recently implemented Azure pass-through authentication. Everything is functional. A few weeks later, the network team performs a change to the company's firewalls. Thereafter, pass-through authentication stops functioning. You need to put in an emergency change request to open the minimum number of ports so that pass-through authentication functions.

Which ports should you open? Select one.

- Only inbound TCP port 80 and inbound TCP port 443.
- Only inbound and outbound TCP port 443.
- Only outbound TCP port 80 and outbound TCP port 443.
- Only outbound TCP port 443 and inbound TCP port 80.

Explanation

Azure pass-through authentication works by having the on-premises agent reach out to Azure to check for pending authentication requests. Only outbound communication must be opened on the firewall. You need to open TCP port 80 and TCP port 443 to enable pass-through authentication.

Module 10 Securing Identities

Multi-Factor Authentication

Azure MFA Concepts

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.

For more information:

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

MFA Authentication Options

multi-factor authentication

users **service settings**

verification options (learn more)

Methods available to users:

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

save

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.

Method	Description
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.

Enabling MFA

To enable MFA, go to the User Properties in Azure Active Directory, and then the Multi-Factor Authentication option. From there, you can select the users that you want to modify and enable for MFA. You can also bulk enable groups of users with PowerShell.

The screenshot shows the 'multi-factor authentication' section of the Azure portal. The 'users' tab is selected. A note at the top states: 'Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.' Below this are filtering options: 'View: Sign-in allowed users' with a dropdown set to 'Any', 'Multi-Factor Auth status: Any' with a dropdown set to 'Disabled', and a 'bulk update' button. A table lists five users:

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input checked="" type="checkbox"/> Adam Barr	AdamB@...	Disabled
<input checked="" type="checkbox"/> Alice Ciccu	AliceC@...	Disabled
<input type="checkbox"/> Amy Rusko	AmyR@...	Disabled
<input type="checkbox"/> Ann Beebe	AnnB@...	Disabled
<input checked="" type="checkbox"/> Ben Smith	BenS@...	Disabled

On the right side of the table, there are three buttons: '3 selected', 'quick steps', and 'Manage user settings'. The '3 selected' button is highlighted.

- ✓ On first-time sign-in, after MFA has been enabled, users are prompted to configure their MFA settings. For example, if you enable MFA so that users must use a mobile device, users will be prompted to configure their mobile device for MFA. Users must complete those steps, or they will not be permitted to sign in, which they cannot do until they have validated that their mobile device is MFA-compliant.

Enabling MFA for Global Admins

Azure MFA is included free of charge for global administrator security. Enabling MFA for global administrators provides an added level of security when managing and creating Azure resources like virtual machines, managing storage, or using other Azure services. Secondary authentication includes phone call, text message, and the authenticator app.

You can use the portal to enable MFA for administrators. MFA configuration is done through the Active Directory blade and the Configure MFA link.

The screenshot shows the 'USERS' blade in the Azure portal. The 'DISPLAY NAME' column shows a user account. The 'SOURCED FROM' column indicates it's from a 'Microsoft account'. At the bottom of the blade, there are several links: 'ADD USER', 'MANAGE MULTI-FACTOR AUTH' (which is highlighted with a red box), and a question mark icon.

Once you have located the global administrator of choice you can Enable MFA.

multi-factor authentication

users service settings

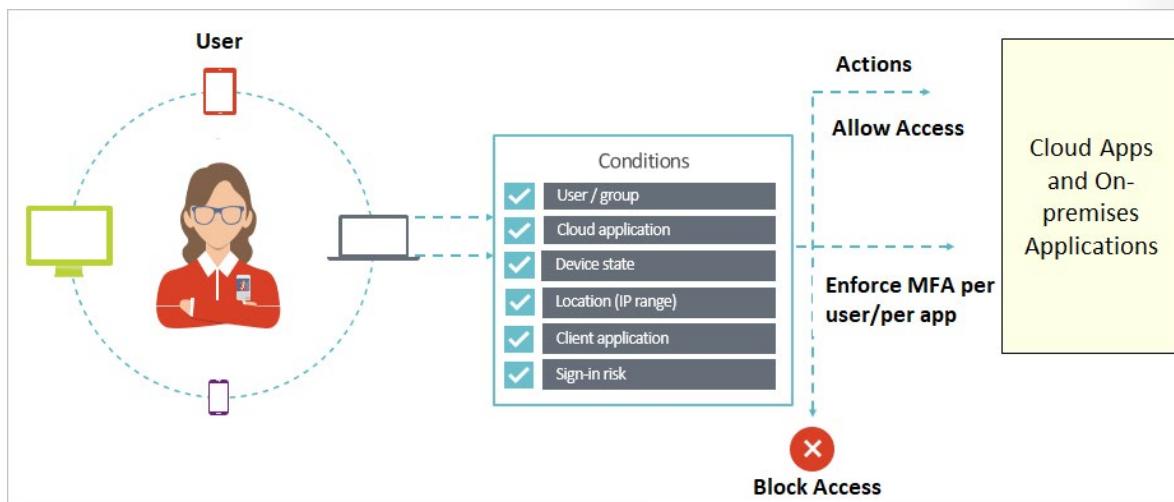
The screenshot shows the 'service settings' for a user named 'Custom Admin'. The 'MULTI-FACTOR AUTH STATUS' is currently 'Disabled'. There are two buttons: 'quick steps' and 'Enable' (which is highlighted with a red box). Below these buttons is a link 'Manage user settings'.

- ✓ Remember you can only enable MFA for organizational accounts stored in Active Directory. These are also called work or school accounts.

Requiring MFA

Conditional access is a capability of Azure AD (with an Azure AD Premium license) that enables you to enforce controls on the access to apps in your environment based on specific conditions from a central location. With Azure AD conditional access, you can factor how a resource is being accessed into an access control decision. By using conditional access policies, you can apply the correct access controls under the required conditions.

Conditional access comes with six conditions: user/group, cloud application, device state, location (IP range), client application, and sign-in risk. You can use combinations of these conditions to get the exact conditional access policy you need. Notice on this image the conditions determine the access control from the previous topic.



With access controls, you can either Block Access altogether or Grant Access with additional requirements by selecting the desired controls. You can have several options:

- Require MFA from Azure AD or an on-premises MFA (combined with AD FS).
- Grant access to only trusted devices.
- Require a domain-joined device.
- Require mobile devices to use **Intune app protection policies**¹.

Requiring additional account verification through MFA is a common conditional access scenario. While users may be able to sign-in to most of your organization's cloud apps, you may want that additional verification for things like your email system, or apps that contain personnel records or sensitive information. In Azure AD, you can accomplish this with a conditional access policy

- ✓ The Users and Groups condition is mandatory in a conditional access policy. In your policy, you can either select All users or select specific users and groups.

Trusted IPs

Trusted IPs is a feature to allow federated users or IP address ranges to bypass two-step authentication. Notice there are two selections in this screenshot.

¹ <https://docs.microsoft.com/intune/app-protection-policy>

multi-factor authentication

users service settings

trusted ips [\(learn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets
 - 192.168.1.0/27
 - 10.0.0.0/24

Which selections you can make depends on whether you have managed or federated tenants.

- **Managed tenants.** For managed tenants, you can specify IP ranges that can skip MFA.
 - **Federated tenants.** For federated tenants, you can specify IP ranges and you can also exempt AD FS claims users .
- ✓ The Trusted IPs bypass works only from inside of the company intranet. If you select the All Federated Users option and a user signs in from outside the company intranet, the user must authenticate by using two-step verification. The process is the same even if the user presents an AD FS claim.

One-time Bypass

The one-time bypass feature allows a user to authenticate a single time without performing two-step verification. The bypass is temporary and expires after a specified number of seconds.

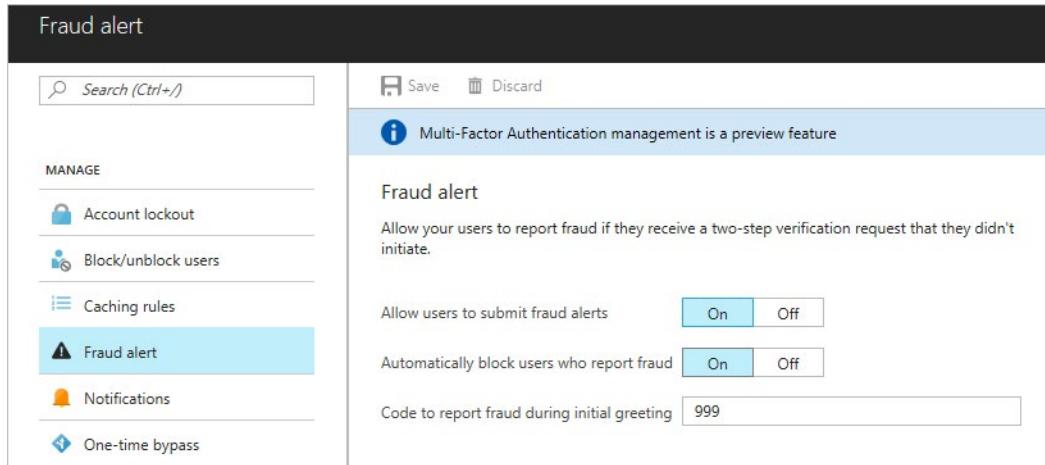
REPLICATION G...	USER	REASON	DATE	SECONDS	ACTION
No results					

- ✓ In situations where the mobile app or phone is not receiving a notification or phone call, you can allow a one-time bypass, so the user can access the desired resource.

Fraud Alerts

Configure the fraud alert feature so that your users can report fraudulent attempts to access their resources. Users can report fraud attempts by using the mobile app or through their phone. Block user when fraud is reported: If a user reports fraud, their account is blocked for 90 days or until an administrator unblocks their account. An administrator can review sign-ins by using the sign-in report and take appropriate action to prevent future fraud. An administrator can then unblock the user's account.

Code to report fraud during initial greeting: When users receive a phone call to perform two-step verification, they normally press # to confirm their sign-in. To report fraud, the user enters a code before pressing #. This code is 0 by default, but you can customize it.



Block user when fraud is reported. If a user reports fraud, their account is blocked for 90 days or until an administrator unblocks their account. An administrator can review sign-ins by using the sign-in report and take appropriate action to prevent future fraud. An administrator can then unblock the user's account.

Code to report fraud during initial greeting. When users receive a phone call to perform two-step verification, they normally press # to confirm their sign-in. To report fraud, the user enters a code before pressing #. This code is 0 by default, but you can customize it.

- ✓ The default voice greetings from Microsoft instruct users to press 0# to submit a fraud alert. If you want to use a code other than 0, record and upload your own custom voice greetings with appropriate instructions for your users.

MFA Licensing and Pricing

There are three pricing methods for Azure MFA.

Consumption based billing. Azure MFA is available as a stand-alone service with per-user and per-authentication billing options.

- **Per user.** You can pay per user. Each user has unlimited authentications. Use this model if you know how many users you have and can accurately estimate your costs.
- **Per authentication.** You can pay for a bundle (10) of authentications. Use this model when you are unsure how many users will participate in MFA authentication.

MFA licenses included in other products. MFA is included in Azure AD Premium, Enterprise Mobility Suite, and Enterprise Cloud Suite.

Direct and Volume licensing. MFA is available through a Microsoft Enterprise Agreement, the Open Volume License Program, the Cloud Solution Providers program, and Direct, as an annual user based model.

- ✓ Which of these licensing options is appropriate for your organization?

For more information:

MFA Pricing - <https://azure.microsoft.com/en-us/pricing/details/multi-factor-authentication/>

Azure AD Identity Protection

Azure AD Identity Protection

Current threat landscape - credential theft

In today's IT environment malicious users use credential theft attacks as one of the main ways to gain access to your environment. Credential theft attacks are those in which an attacker initially gains highest-privilege access to a computer on a network and then uses freely available tooling to extract credentials from the sessions of other logged-on accounts. Depending on the system configuration, these credentials can be extracted in the form of hashes, tickets, or even plaintext passwords. Many IT professionals believe that identity is the new boundary layer for security, supplanting that role from the traditional network-centric perspective.

Securing systems with Azure AD Identity Protection

Microsoft has secured cloud-based identities for more than a decade. Azure AD Identity Protection is a service that helps to ward off compromised user accounts and configuration vulnerabilities. This service enables you to use the same protection systems Microsoft uses to secure identities in your environment.

The service is available from Azure Marketplace and must be set up by an organization's global administrator. Azure AD Identity Protection is available to subscribers to Microsoft's Enterprise Mobility Suite and/or the Azure AD Premium P2 service.

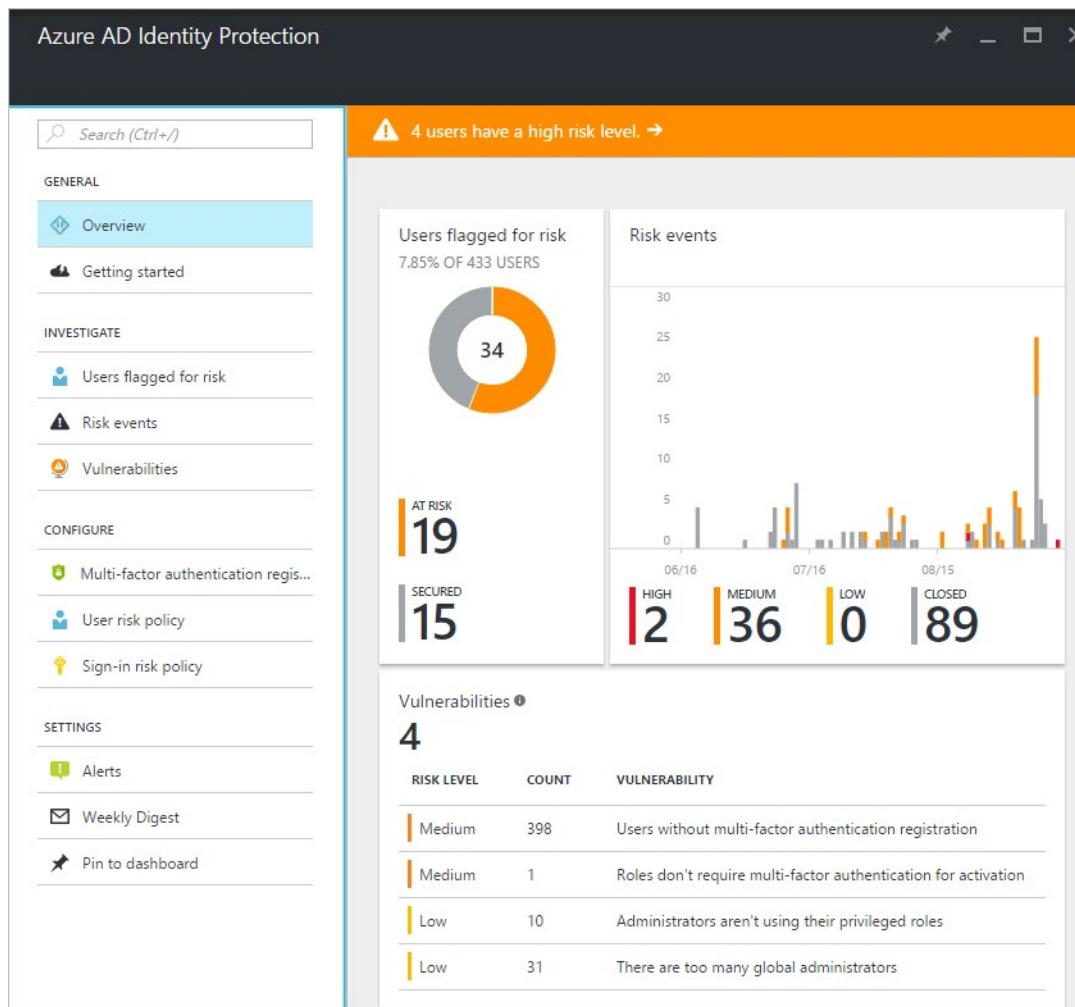
Azure AD Identity Protection enables you to:

- Detect potential vulnerabilities affecting your organization's identities
- Configure automated responses to detected suspicious actions that are related to your organization's identities
- Investigate suspicious incidents and take appropriate action to resolve them

Identity Protection capabilities

- Azure Active Directory Identity Protection analyses your configuration and detects vulnerabilities that can have an impact on your user's identities.
- Azure AD uses adaptive machine learning algorithms and heuristics to detect suspicious actions that are related to your user's identities. The system creates a record for each detected suspicious action. These records are also known as risk events.
- Azure AD Identity Protection lets you set risk-based Conditional Access policies to automatically protect your users. The following topics cover some of these policies in more detail.

The following screenshot shows the Azure AD Identity Protection dashboard.



The dashboard gives access to:

- Reports such as **Users flagged for risk**, **Risk events** and **Vulnerabilities**
- Settings such as the configuration of your **Security Policies**, **Notifications** and **multi-factor authentication registration**

Azure AD Risk Events

The vast majority of security breaches occur when attackers gain access to an environment by stealing a user's identity. Discovering compromised identities is no easy task. Azure Active Directory uses adaptive machine learning algorithms and heuristics to detect suspicious actions that are related to your user accounts. Each detected suspicious action is stored in a record called a **risk event**.

Currently, Azure Active Directory detects six types of risk events:

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials ⓘ	44 of 45	12/7/2016 1:04 AM
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	76 of 78	1/17/2017 2:44 PM
Medium	Offline	Impossible travels to atypical locations ⓘ	11 of 14	1/17/2017 2:44 PM
Medium	Real-time	Sign-in from unfamiliar location ⓘ	0 of 1	11/15/2016 7:18 PM
Low	Offline	Sign-ins from infected devices ⓘ	76 of 78	1/17/2017 2:44 PM

✓ Not shown in the screen shot is the **Sign-ins from IP addresses with suspicious activity** risk event. This risk event type identifies IP addresses from which a high number of failed sign-in attempts were seen, across multiple user accounts, over a short period of time. This matches traffic patterns of IP addresses used by attackers, and is a strong indicator that accounts are either already or are about to be compromised.

- **Leaked credentials.** When cybercriminals compromise valid passwords of legitimate users, they often share those credentials. This is usually done by posting them publicly on the dark web or paste sites or by trading or selling the credentials on the black market. The Microsoft leaked credentials service acquires username / password pairs, and checks them against AAD users' current valid credentials. When a match is found, it means that a user's password has been compromised, and a **leaked credentials risk event** is created.
- **Sign-ins from anonymous IP addresses.** This risk event type identifies users who have successfully signed in from an IP address that has been identified as an anonymous proxy IP address. These proxies are used by people who want to hide their device's IP address, and may be used for malicious intent.
- **Impossible travel to atypical locations.** This risk event type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior. Among several other factors, this machine learning algorithm takes into account the time between the two sign-ins and the time it would have taken for the user to travel from the first location to the second, indicating that a different user is using the same credentials.
- **Sign-in from unfamiliar locations.** This risk event type considers past sign-in locations (IP, Latitude / Longitude and ASN) to determine new / unfamiliar locations. The system stores information about previous locations used by a user, and considers these "familiar" locations. The risk event is triggered when the sign-in occurs from a location that's not already in the list of familiar locations. The system has an initial learning period of 30 days, during which it does not flag any new locations as unfamiliar locations. The system also ignores sign-ins from familiar devices, and locations that are geographically close to a familiar location.
- **Sign-ins from infected devices.** This risk event type identifies sign-ins from devices infected with malware, that are known to actively communicate with a bot server. This is determined by correlating IP addresses of the user's device against IP addresses that were in contact with a bot server.

User Risk Policy

Azure AD analyzes each user-sign in for evidence of a compromised account or any suspicious activity, also known as risk events (described in the previous topic).

For risk events that the system detects, you can resolve those events manually, or you can configure conditional access policies that apply to a specific user risk level or the sign-in risk level. This topic describes the user risk policy and how to configure it.

The system can detect some risk events in real-time but other risk events require more time to analyze pattern and behavior, such as risk events arising from impossible travel to atypical locations. The system needs time to be able to distinguish between a sign-in based on a user's regular behavior and an atypical sign-in. If the locations are geographically distant and the time delay between the sign-ins is insufficient for that user to have attempted to sign in from one location and then the other, that is an indication that the account has likely been compromised and a different user is using the user's credentials.

When the system detects a risk event for a user that hasn't been resolved it is considered an *active risk event*. A user risk is any active risk event associated with a particular user. Azure AD calculates the probability that a user has been compromised and assigns a user risk level of *low*, *medium*, or *high*.

A user risk policy lets you block access to resources or require a password change to reset the user's account to a non-compromised state.

USER	MFA	RISK LEVEL	RISK EVENTS	STATUS	LAST UPDATED (UTC)
Harry Slate		High	0 risk events	Policy: Sign-in blo...	3/1/2016, 8:28 PM
Lex Brown		High	0 risk events	Policy: Sign-in blo...	4/4/2016, 8:43 PM
Liz Bean		High	1 risk event	Policy: Sign-in blo...	9/12/2016, 11:36 PM
Mike Lee		High	7 risk events	Policy: Sign-in blo...	9/3/2016, 4:56 AM
Afroditi K	✓	Medium	17 risk events	At risk	9/7/2016, 12:56 AM

Configure the user risk policy

You access the user risk policy from the Configure section of the **Azure AD Identity Protection** blade. From the **Azure AD Identity Protection - User risk policy** blade, configure the **User risk remediation policy**.

- Select the users and groups the policy applies to
- Assign the condition (**Low and above**, **Medium and above**, or **High**)
- The access type you will enforce for the user based on sign-in risk level
- Set **Enforce Policy** to **On**

Access
USER RISK

Select the controls to be enforced.

Block access
 Allow access

Require password change

Blocking a sign-in:

- Prevents the generation of new user risk events for the affected user
- Enables administrators to manually remediate the risk events affecting the user's identity and restore it to a secure state

Best practices

When setting user risk policy, it is recommended you balance the organizational and productivity impact of a **High** threshold with the less stringent levels of **Medium** and **Low**. A **Medium** threshold provides a balance between usability and security.

When setting the policy:

- Use a **High** threshold during initial policy roll out, or if you must reduce challenges seen by end users.
- Use a **Low** threshold if your organization requires greater security. Selecting a **Low** threshold introduces additional user sign-in challenges, but increased security.

Sign-in Risk Policy

With the user risk, Azure AD detects the probability that a user account has been compromised. As an administrator, you can configure a **user risk conditional access policy**, to automatically respond to a specific user risk level.

Azure AD detects risk event types in real-time and offline. Each risk event that has been detected for a user sign-in of a user contributes to a *risky sign-in*. A risky sign-in signifies a possible attempt to perform a sign-in by someone other than the legitimate owner of the associated user account.

Azure AD analyzes each user sign-in with the intention of detecting suspicious actions, or risk events, that come along with the sign-in. For example, one of the risk events discussed in a previous topic, such as a sign-in attempted through an anonymous IP address. Based on the risk events detected, Azure AD calculates a value representing the probability (low, medium, high) that the sign-in is not performed by the legitimate user. The probability is referred to as *sign-in risk level*.

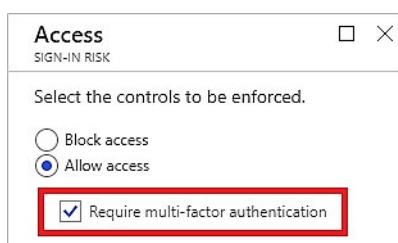
Configure the sign-in risk policy

You access the sign-in risk policy from the Configure section of the **Azure AD Identity Protection** blade. From the **Azure AD Identity Protection - Sign-in risk policy** blade, configure the **Sign-in risk remediation** policy.



- Select the users and groups the policy applies to
- Assign the condition (**Low and above**, **Medium and above**, or **High**)
- The access type you will enforce for the user based on sign-in risk level
- Set **Enforce Policy** to **On**

You can configure a sign-in risk security policy to require MFA:



Important considerations

If you want to require multi-factor authentication (MFA) for risky sign-ins, enable the multi-factor authentication registration policy for the affected users and require those users to sign in to a non-risky session to perform an MFA registration.

In addition to the best practices in the previous topic, also consider:

- Omit users who are likely to generate a lot of false-positives. For example developers, or security analysts.
- Omit users in sites where it's not realistic to enable the policy. For example, no access to helpdesk.
- ✓ The sign-in risk policy is applied to all browser traffic and sign-ins using modern authentication, but not to applications using older security protocols.

Security Best Practices

Many consider identity to be the new boundary layer for security, taking over that role from the traditional network-centric perspective. To help you get started, there is an Azure identity management and access control security best practices page. The best practices were derived from consensus opinion and Azure platform capabilities and feature sets.

- **Centralize your identity management.** Ensure that IT can manage accounts from one single location.
- **Enable Single Sign-On (SSO).** Provide your users the ability to use the same set of credentials to sign in and access the resources that they need, regardless of whether this resource is located on-premises or in the cloud.
- **Deploy password management.** leverage the self-service password reset capability and customize the security options to meet your business requirements.
- **Enforce MFA for users.** Enable Azure MFA for your users. This will add a second layer of security to user sign-ins and transactions.
- **Use role-based access control (RBAC).** Apply the principle of least privileges.
- **Control locations where resources are created using Resource Manager.** Create security policies with definitions that describe the actions or resources that are allowed and denied.
- **Guide developers to leverage identity capabilities for SaaS apps.** Ensure developers use a secure methodology to develop SaaS apps. Register any application that outsources authentication to Azure AD.
- **Actively monitor for suspicious activities.** Use Azure AD Premium [anomaly reports²](#) and Azure AD [identity protection³](#) capabilities.
 - ✓ Take a minute to go through each item in the reference link. Are you following these best practices? In this course we focus on enforcing MFA for users and implementing RBAC, but security is much more than that.

For more information:

Azure Identity Management and access control security best practices - <https://docs.microsoft.com/en-us/azure/security/azure-security-identity-management-best-practices>

² <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-view-access-usage-reports>

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

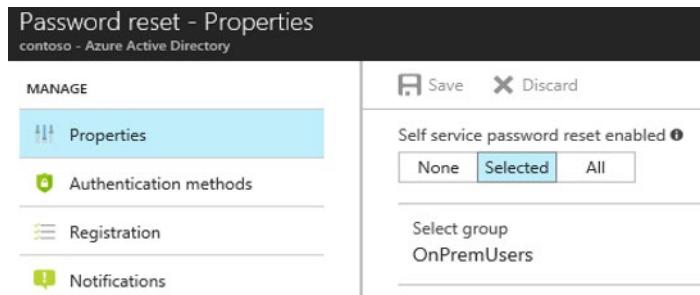
Self-Service Password Reset

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**.

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**.

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

SSPR 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.

The screenshot shows the 'Authentication methods' section of the Azure Active Directory Password reset configuration. It includes settings for the number of methods required to reset (1 selected), available methods (Email, Mobile phone checked), and the number of questions required to register (5 selected). A list of 5 security questions is also shown.

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**⁴. Security questions can be less secure than other methods because some people might know the answers to another user's questions.

- ✓ At the time of this writing Mobile app notification and Mobile app code are in preview.

SSPR Registration

If you want your users to register for password reset, you can require that they register when they sign in through Azure AD. You can enable this option from your directory's Password reset pane by enabling the **Require Users to Register when Signing in** option on the Registration tab. Administrators can require users to re-register after a specific period of time. They can set the Number of days before users are asked to reconfirm their authentication information option to 0 to 730 days. After you enable this option, when users sign in they observe a message that says their administrator has required them to verify their authentication information.

Require users to register when signing in

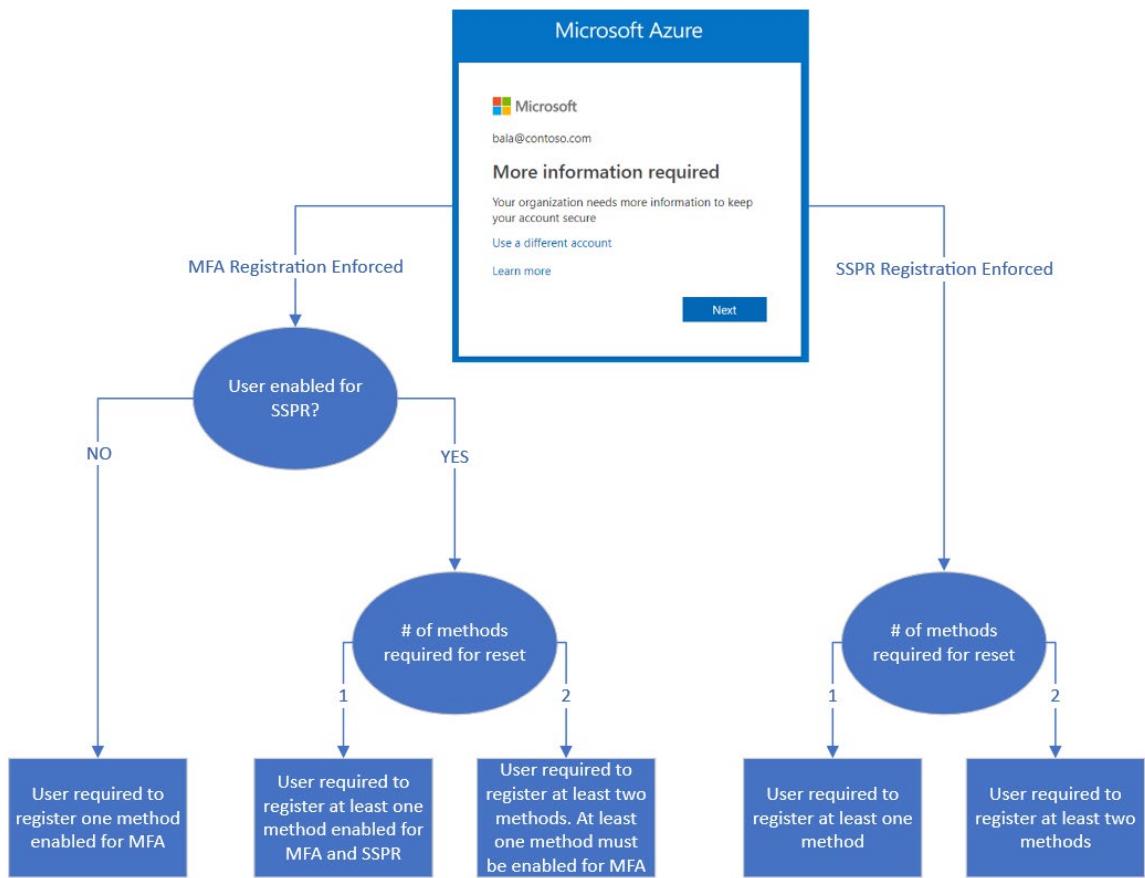
Yes	No
-----	----

There are two modes to register: **interrupt** and **manage**.

- Interrupt mode, is a wizard-like experience, shown to a user when they register or refresh their security info at sign in.
- Manage mode is part of the user's profile and allows them to manage their security info.

Previously, there were two different ways for users to register for Azure MFA and SSPR. Now, in preview, users can register once and get the benefits of both Azure MFA and SSPR.

⁴ <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods#predefined-questions>



- ✓ You should consider pre-populating some authentication data for your users. That way users don't need to register for password reset before they are able to use SSPR. As long as users have provided the authentication data that meets the password reset policy you have defined, they are able to reset their passwords.

For more information:

Video - Deploying self-service password reset | Azure Active Directory - <https://www.youtube.com/watch?v=Pa0eyqjEjvQ>

Comparing SSPR to MFA

Azure AD self-service password reset (SSPR) and MFA may ask for additional information, known as authentication methods or security info, to confirm you are who you say you are when using the associated features.

Administrators can define in policy which authentication methods are available to users of SSPR and MFA. Some authentication methods may not be available to all features.

Microsoft highly recommends Administrators enable users to select more than the minimum required number of authentication methods in case they do not have access to one.

Authentication Method	Usage
Password	MFA and SSPR

Authentication Method	Usage
Security questions	SSPR Only
Email address	SSPR Only
Microsoft Authenticator app	MFA and Public Preview for SSPR
SMS	MFA and SSPR
Voice call	MFA and SSPR
App passwords	MFA only in certain cases

✓ Your Azure AD password is considered an authentication method. It is the one method that cannot be disabled.

Lab and Review Questions

Lab - Azure AD Identity Protection

Scenario

Adatum Corporation wants to take advantage of Azure AD Premium features for Identity Protection.

Objectives

After completing this lab, you will be able to:

- Deploy an Azure VM by using an Azure Resource Manager template.
- Implement Azure MFA.
- Implement Azure AD Identity Protection.

Exercise 0: Prepare the lab environment

The main task for this exercise is as follows:

- Deploy an Azure VM by using an Azure Resource Manager template.

Result: After you completed this exercise, you have initiated a template deployment of an Azure VM az1010401b-vm1 that you will use in the next exercise of this lab.

Exercise 1: Implement Azure MFA.

The main tasks for this exercise are as follows:

- Create a new Azure AD tenant.
- Activate Azure AD Premium v2 trial.
- Create Azure AD users and groups.
- Assign Azure AD Premium v2 licenses to Azure AD users.
- Configure Azure MFA settings, including fraud alert, trusted IPs, and app passwords.
- Validate MFA configuration.

Result: After you have completed this exercise, you will have implemented and validated Azure MFA.

Exercise 2: Implement Azure AD Identity Protection.

The main tasks for this exercise are as follows:

- Enable Azure AD Identity Protection.
- Configure user risk policy.
- Configure sign-in risk policy.
- Validate Azure AD Identity Protection configuration by simulating risk events.

Result: After you completed this exercise, you have enabled Azure AD Identity Protection, configured user risk policy and sign-in risk policy, as well as validated Azure AD Identity Protection configuration by simulating risk events.

Lab - Self-Service Password Reset

Scenario

Adatum Corporation wants to take advantage of Azure AD Premium features including Self-Service Password Reset.

Objectives

After completing this lab, you will be able to:

- Manage Azure AD users and groups.
- Manage Azure AD-integrated SaaS applications.

Exercise 1: Manage Azure AD users and groups.

The main tasks for this exercise are as follows:

- Create a new Azure AD tenant.
- Activate Azure AD Premium v2 trial.
- Create and configure Azure AD users.
- Assign Azure AD Premium v2 licenses to Azure AD users.
- Manage Azure AD group membership.
- Configure self-service password reset functionality.
- Validate self-service password reset functionality.

Result: After you completed this exercise, you have created a new Azure AD tenant, activated Azure AD Premium v2 trial, created and configured Azure AD users, assigned Azure AD Premium v2 licenses to Azure AD users, managed Azure AD group membership, as well as configured and validated self-service password reset functionality.

Exercise 2: Manage Azure AD-integrated SaaS applications.

The main tasks for this exercise are as follows:

- Add an application from the Azure AD gallery.
- Configure the application for a single sign-on.
- Assign users to the application.
- Validate single sign-on for the application.

Result: After you completed this exercise, you have added an application from the Azure AD gallery, configured the application for a single sign-on, assigned users to the application, and validated single sign-on for the application.

Module Review Questions

Review Question 1

Your company has a hybrid environment with some applications and services in an on-premises data center and some applications and services in Microsoft Azure.

The company intends to strengthen identity verification and access controls for Azure administrators by using conditional access. The information security team issues the following requirements:

- If Azure calculates that there is a chance that an unauthorized person is using an account, then multi-factor authentication must be required for the sign-in.

- If any administrators attempt to access Microsoft Azure while off the corporate networks, the sign-ins must be blocked.

You need to configure conditional access to support the requirements.

Which conditional access features should you configure? (Each answer presents part of the solution. Choose two.)

- Device platforms
- Locations
- Sign-in risk
- Client apps
- Score

Review Question 2

A user has reported their cell phone has been stolen. They are unable to receive the MFA text notification. What should you do? Select one.

- Add the IP address of the user to the trusted IPs list.
- Turn on fraud reporting and provide the key to the user.
- Turn off fraud reporting and ask the user to try again.
- Turn off MFA for the user.
- Enable a one-time bypass for the user.

Review Question 3

You are a systems administrator for Alpine Ski House. The company has a large on-premises environment spread across multiple locations. The on-premises environment includes the following technologies:

- Active Directory Domain Services (AD DS)
- Third-party multi-factor authentication service
- Windows 10

The company is planning to implement services across a range of Microsoft Azure services, such as SaaS and PaaS. You are tasked with deploying a hybrid identity solution.

The company has established the following requirements for the project:

- All access to Microsoft Azure must use multi-factor authentication.
- All multi-factor authentication must use the existing MFA service.

- Users must be provided with a single sign-on experience when going to the Azure portal.

You need to implement a solution to meet the requirements. You plan to deploy Azure AD Connect. What else should you do? Select one.

- Implement Active Directory Federation Services (AD FS).
- Implement Azure pass-through authentication and Azure single sign-on.
- Implement Azure multi-factor authentication.
- Implement Azure AD Domain Services.
- Implement Web Application Proxy servers.

Review Question 4

Your company recently implemented Azure conditional access. The company configuration was supposed to include the following elements:

- Multi-factor authentication is required for users when they are not on the company network.
- Only Windows computers are enabled to access Azure.

A user reports that they are getting prompted for MFA when they are on the company network. You check the configuration and notice that an MFA rule is configured for any location.

You need to update the configuration to meet the intended company configuration. What should you do? Select one.

- Update the Include to "All trusted locations".
- Update the Include to "Selected locations".
- Add an Exclude for "All trusted locations".
- Add an Exclude for "Selected location".

Review Question 5

Which of the following is not a feature of Azure AD Identity Protection? Select one.

- A customized list of configuration vulnerabilities.
- Automated responses with Conditional Access policies.
- Self-Service Password Reset (SSPR).
- Machine learning algorithms signaling different security vulnerabilities

Review Question 6

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 7

A user signs in from a proxy IP address with the intent to hide their device's IP address. Under which type of Azure AD risk event would this activity be classified? Select one.

- Leaked credentials.
- Sign-in from infected device.
- Sign-in from unfamiliar location.
- Sign-in from anonymous IP address.

Review Question 8

Your company is planning to use Azure and is investigating whether their Azure AD Basic subscription will work for their needs. Which of the features below is not available in the Basic subscription? Select one.

- Self-Service Password change for cloud users.
- Group-based access management/provisioning.
- Company Branding (Logon Pages/Access Panel customization).
- Multi-Factor Authentication (Cloud and On-premises (MFA Server)).

Answers

Review Question 1

Your company has a hybrid environment with some applications and services in an on-premises data center and some applications and services in Microsoft Azure.

The company intends to strengthen identity verification and access controls for Azure administrators by using conditional access. The information security team issues the following requirements:

You need to configure conditional access to support the requirements.

Which conditional access features should you configure? (Each answer presents part of the solution. Choose two.)

- Device platforms
- Locations
- Sign-in risk
- Client apps
- Score

Explanation

To meet the requirement of requiring multi-factor when an unauthorized person might be using an account, you should use the sign-in risk option. For example, you can require MFA when the sign-in risk is medium or high. To meet the requirement to block off-site access, you need to identify the locations. For example, you can identify the company locations as trusted locations and then exclude those in a rule that blocks access.

Review Question 2

A user has reported their cell phone has been stolen. They are unable to receive the MFA text notification. What should you do? Select one.

- Add the IP address of the user to the trusted IPs list.
- Turn on fraud reporting and provide the key to the user.
- Turn off fraud reporting and ask the user to try again.
- Turn off MFA for the user.
- Enable a one-time bypass for the user.

Explanation

The one-time bypass feature allows a user to authenticate a single time without performing two-step verification. The bypass is temporary and expires after a specified number of seconds.

Review Question 3

You are a systems administrator for Alpine Ski House. The company has a large on-premises environment spread across multiple locations. The on-premises environment includes the following technologies:

The company is planning to implement services across a range of Microsoft Azure services, such as SaaS and PaaS. You are tasked with deploying a hybrid identity solution.

The company has established the following requirements for the project:

You need to implement a solution to meet the requirements. You plan to deploy Azure AD Connect. What else should you do? Select one.

- Implement Active Directory Federation Services (AD FS).
- Implement Azure pass-through authentication and Azure single sign-on.
- Implement Azure multi-factor authentication.
- Implement Azure AD Domain Services.
- Implement Web Application Proxy servers.

Explanation

To support third-party multi-factor authentication, you need to deploy AD FS. While AD FS requires on-premises infrastructure, it offers the most complete authentication solution for a hybrid cloud environment. In some cases, such as the one presented in this scenario, it is the only solution

Review Question 4

Your company recently implemented Azure conditional access. The company configuration was supposed to include the following elements:

A user reports that they are getting prompted for MFA when they are on the company network. You check the configuration and notice that an MFA rule is configured for any location.

You need to update the configuration to meet the intended company configuration. What should you do? Select one.

- Update the Include to "All trusted locations".
- Update the Include to "Selected locations".
- Add an Exclude for "All trusted locations".
- Add an Exclude for "Selected location".

Explanation

In this scenario, MFA should occur when a user is not on a company network. Because you cannot identify every possible location outside of your company networks, you should define your company subnets and exclude them from the MFA rule.

Review Question 5

Which of the following is not a feature of Azure AD Identity Protection? Select one.

- A customized list of configuration vulnerabilities.
- Automated responses with Conditional Access policies.
- Self-Service Password Reset (SSPR).
- Machine learning algorithms signaling different security vulnerabilities

Explanation

Self-service password reset (SSPR) is used as a simple means for IT administrators to enable users to reset their passwords or unlock their accounts. It is not associated with Azure AD Identity Protection.

Azure AD Identity Protection let you protect your organization from compromised accounts, identity attacks, and configuration issues. You can receive detailed notifications of new identity risks, perform recommended

remediation, and automate future response with Conditional Access policies. Machine-learning algorithms generate signals like brute force attacks, leaked credentials, and sign-ins from unfamiliar locations, allowing Azure AD Identity Protection to provide a consolidated view of these suspicious user activities that are detected.

Review Question 6

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

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 7

A user signs in from a proxy IP address with the intent to hide their device's IP address. Under which type of Azure AD risk event would this activity be classified? Select one.

- Leaked credentials.
- Sign-in from infected device.
- Sign-in from unfamiliar location.
- Sign-in from anonymous IP address.

Explanation

The correct answer is sign-in from anonymous IP address. This risk event type identifies users who have successfully signed in from an IP address that has been identified as an anonymous proxy IP address. These proxies are used by people who want to hide their device's IP address, and may be used for malicious intent. The Microsoft leaked credentials service username/password pairs, they are checked against AAD users' current valid credentials. When a match is found, it means that a user's password has been compromised, and a leaked credentials risk event is created.

Review Question 8

Your company is planning to use Azure and is investigating whether their Azure AD Basic subscription will work for their needs. Which of the features below is not available in the Basic subscription? Select one.

- Self-Service Password change for cloud users.
- Group-based access management/provisioning.
- Company Branding (Logon Pages/Access Panel customization).
- Multi-Factor Authentication (Cloud and On-premises (MFA Server)).

Explanation

The Basic Azure AD pricing level does not include Multi-Factor Authentication (Cloud and On-premises (MFA Server)).

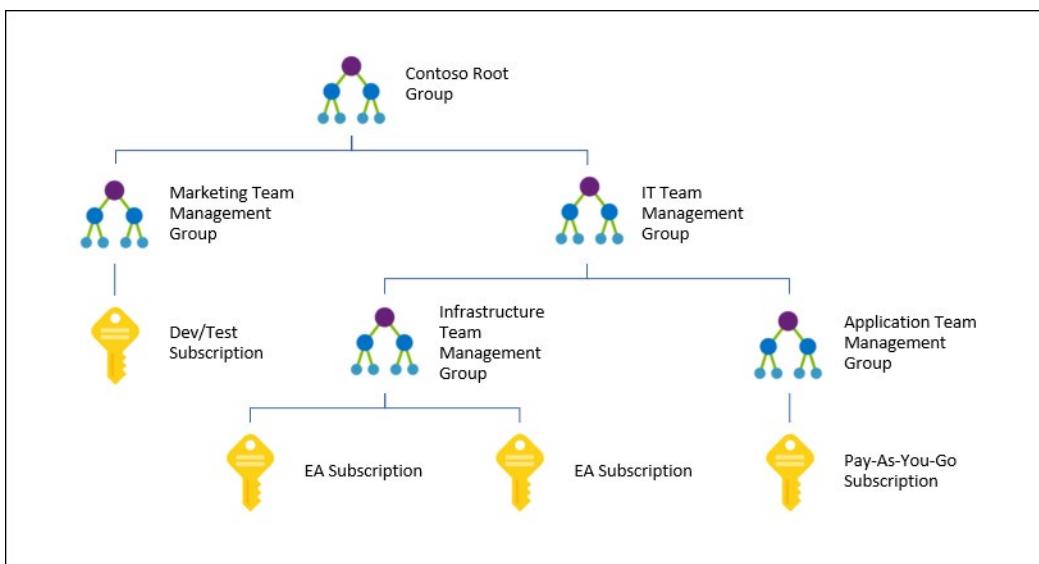
Module 11 Governance and Compliance

Subscriptions and Accounts

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.

- ✓ Management groups is a relatively new concept in Azure.

For more information:

Organize your resources with Azure management groups - <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management-groups-overview>

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.

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.

Within PowerShell, use the **New-AzManagementGroup** cmdlet:

```
New-AzManagementGroup -GroupName 'Contoso'
```

To show a different name for the management group within the Azure portal, add the **DisplayName** parameter with the desired string:

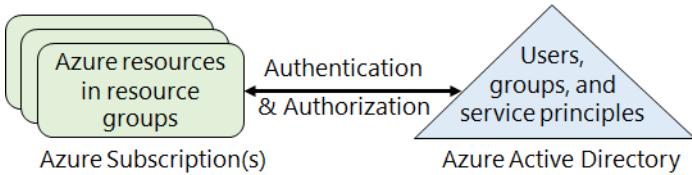
```
New-AzManagementGroup -GroupName 'Contoso' -DisplayName 'Contoso Development'
```

Azure Subscriptions

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

Subscriptions help you organize access to cloud service resources. They also help you control how resource usage is reported, billed, and paid for. Each subscription can have a different billing and pay-

ment 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**¹ 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

¹ <https://azure.microsoft.com/en-us/pricing/enterprise-agreement/>

Buy Azure through the **Open Licensing program²**, 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 now³**.

Partners

Find a **Microsoft partner⁴** 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 account⁵** 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?

For more information:

Solution providers - <https://www.microsoft.com/en-us/solution-providers/home>

Subscription Usage

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

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

Azure free subscription

An Azure free subscription includes a \$200 credit to spend on any service for the first 30 days, free access to the most popular Azure products for 12 months, and access to more than 25 products that are always free. 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

² <https://www.microsoft.com/en-us/licensing/licensing-programs/open-license.aspx>

³ <https://azure.microsoft.com/en-us/offers/ms-azr-0111p/>

⁴ <https://azure.microsoft.com/en-us/partners/directory/>

⁵ <https://azure.microsoft.com/en-us/free/>

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.

Subscription User Types

An Azure account determines how Azure usage is reported and who the Account Administrator is. Accounts and subscriptions are created in the Azure Account Center. The person who creates the account is the Account Administrator for all subscriptions created in that account. That person is also the default Service Administrator for the subscription.

Subscription User Types

There are three roles related to Azure accounts and subscriptions:

Administrative role	Limit	Summary
Account Administrator	1 per Azure account	Authorized to access the Account Center (create subscriptions, cancel subscriptions, change billing for a subscription, change Service Administrator). This role has full control over the subscription and is the account that is responsible for billing.
Service Administrator	1 per Azure subscription	Authorized to access Azure Management Portal for all subscriptions in the account. By default, same as the Account Administrator when a subscription is created. This role has control over all the services in the subscription.
Co-Administrator	200 per subscription (in addition to Service Administrator)	Same as Service Administrator but can't change the association of subscriptions to Azure directories.

Account administrator

The Account Administrator for a subscription is the only person with access to the Account Center. The Account Administrator does not have any other access to services in that subscription; they need to also be the Service Administrator or a Co-Administrator for that. For security reasons, the Account Administrator for a subscription can only be changed with a call to Azure support. The Account Administrator can easily reassign the Service Administrator for a subscription at the Account Center at any time.

Service Administrator and Co-Administrator

The Service Administrator is the first Co-Administrator for a subscription. Like other Co-Administrators, the Service Administrator has management access to cloud resources using the Azure Management Portal, as well as tools like Visual Studio, other SDKs, and command line tools like PowerShell. The Service Administrator can also add and remove other Co-Administrators.

Additionally, Co-Administrators can't delete the Service Administrator from the Azure Management Portal. Only the Account Administrator can change this assignment at the Account Center. The Service

Administrator is the only user authorized to change a subscription's association with a directory in the Azure Management Portal.

- ✓ Account Administrators using a Microsoft account must log in every 2 years (or more frequently) to keep the account active. Inactive accounts are cancelled, and the related subscriptions removed. There are no login requirements if using a work or school account.

Check 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. In this example, there are two Public IP Addresses in South Central US and the limit is 60.

SETTINGS	QUOTA	PROVIDER	LOCATION	USAGE	Request Increase
Resource groups	Network Watchers	Microsoft.Network	West US 2	100 %	1 of 1
Resources	Public IP Addresses	Microsoft.Network	South Central US	3 %	2 of 60
Usage + quotas	Route Tables	Microsoft.Network	West US	2 %	2 of 100
Policies	Virtual Networks	Microsoft.Network	South Central US	2 %	1 of 50

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 [limits](#)⁶. If your current limit is already at the maximum number, the limit can't be increased.

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.

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. For example, you could group virtual machines by cost center and production environment.

⁶ <https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits?toc=%2fazure%2fnetworking%2ftoc.json>

Daily Usage						Tags
Usage Date	Meter Category	Unit	Consume	Resource Group	Instance Id	
5/14/2015	"Virtual Machines"	"Hours"	3.999984	"computeRG"	"virtualMachines/catalogVM"	{\"costCenter\":\"finance\", \"env\":\"prod\"}
5/14/2015	"Virtual Machines"	"Hours"	3.999984	"businessRG"	"virtualMachines/dataVM"	{\"costCenter\":\"hr\", \"env\":\"test\"}

There are a few things to consider about tagging:

- Each resource or resource group can have a maximum of 15 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.

Billing

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

Your Estimate

Virtual Machines

Virtual Machines

REGION: West US OPERATING SYSTEM: Windows TYPE: (OS Only)

TIER: Standard

INSTANCE: D1: 1 Cores(s), 3.5 GB RAM, 50 GB Temporary storage, \$0.140/hour

Billing Alerts help you monitor and manage billing activity for your Azure accounts. Billing alerts are available from the Account portal. 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.

OVERVIEW BILLING HISTORY ALERTS PREVIEW

+ Half way there Not Sent ⚡ Monetary Credits \$80 ⚡ ⚡

+ Some money was spent Not Sent ⚡ Monetary Credits \$120 ⚡ ⚡

+ add alert ⚡

You can setup 3 more alerts

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 ma-

chine, 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.

The screenshot shows a grid of four service reservation options:

- Virtual machine reserved instances**: Save on virtual machine usage by buying reserved instance for 1 or 3 years. Includes a "Select" button.
- Azure Cosmos DB**: Save up to 65% on Cosmos DB by buying reserved throughput capacity for 1 or 3 years. Includes a "Select" button.
- SQL Database**: Save on SQL Database compute costs by buying reserved vCores for 1 or 3 years. Includes a "Select" button.
- SUSE Linux**: Save on SUSE Linux enterprise server cost by pre-purchasing SUSE software for 1 or 3 years. Includes a "Select" button.

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.

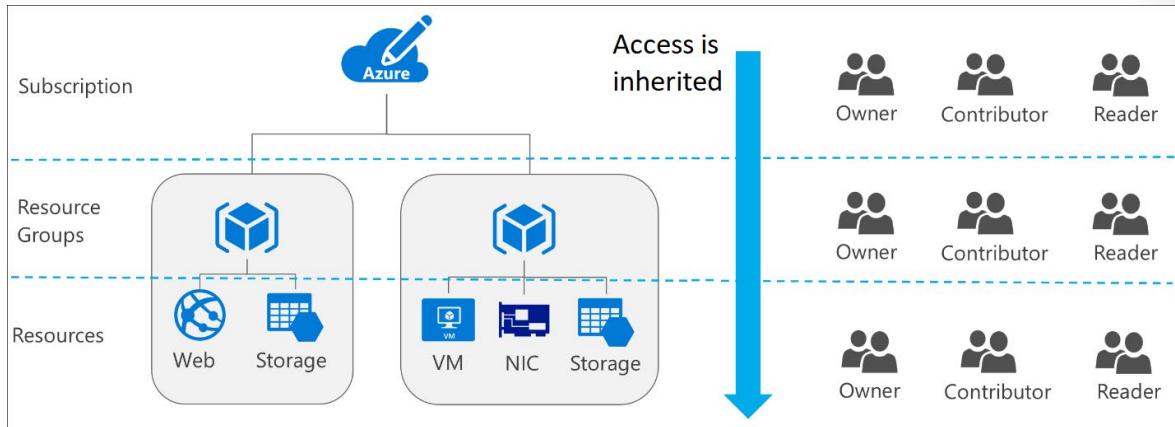
For more information:

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

Role-based Access Control

RBAC Concepts

Managing access to resources in Azure is a critical part of an organization's security and compliance requirements. Role-based access control (RBAC) is the capability for you to grant appropriate access to Azure AD users, groups, and services. RBAC is configured by selecting a role (the definition of what actions are allowed and/or denied), then associating the role with a user, group or service principal. Finally, this combination of role and user/group/service principal is scoped to either the entire subscription, a resource group, or specific resources within a resource group.



RBAC Roles

A role is a collection of actions that can be performed on Azure resources. A user or a service can perform an action on an Azure resource if they have been assigned a role that contains that action. There are many built-in roles. Three of the most common roles are Owner, Contributor and Reader.

Role name	Description
Owner	Owner can manage everything, including access.
Contributor	Contributors can manage everything except access.
Reader	Readers can view everything but can't make changes.

Using the Portal to implement RBAC

You can use the Azure Portal to make your role assignments. In this example, the ContosoBlueAD resource group shows on the Access Control (IAM) blade the current roles and scopes. You can add or remove roles as you need. You can add synced users and groups to Azure roles, which enables organizations to centralize the granting of access.

The screenshot shows the Azure Resource Groups blade for a resource group named 'ContosoBlueAD'. The 'Access control (IAM)' section is highlighted with a red box. The 'Add' button in the top right of the table is also highlighted with a red box.

NAME	TYPE	ROLE	SCOPE
OWNER	User	Owner	Subscription (Inherited)
coreyhynes@outlook.... coreyhynes@outlook....	User	Owner	
VIRTUAL MACHINE CONTRIBUTOR	User	Virtual Machine Contributor	This resource
AD admin admin@contosoblue....	User	Virtual Machine Contributor	This resource

- ✓ Users and groups are sourced from Azure Active Directory, which is commonly populated with credentials from on-premises directories, such as Active Directory. Note that RBAC access that you grant at parent scopes is inherited at child scopes.

Administrator Permissions

Using Azure AD, you can designate separate administrators to serve different functions. Administrators can be designated in the Azure AD portal to perform tasks such as adding or changing users, assigning administrative roles, resetting user passwords, managing user licenses, and managing domain names.

Global administrator

The global administrator has access to all administrative features. By default, the person who signs up for an Azure subscription is assigned the global administrator role for the directory. Only global administrators can assign other administrator roles.

Viewing role membership

You can observe and manage all the members of the administrator roles in the Azure Active Directory portal. When you're viewing a roles members, you can observe the complete list of permissions granted by the role assignment. This includes links to relevant documentation to help guide you through managing directory roles.

The screenshot shows the Azure Active Directory blade. The 'Roles and administrators' section is highlighted with a red box. The 'Your Role' message is also highlighted with a red box. The '...' button next to the 'Application administrator' role is also highlighted with a red box.

ROLE	DESCRIPTION	...
Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	...
Application developer	Can create application registrations independent of the 'Users can register applications' setting.	...
Billing administrator	Can perform common billing related tasks like updating payment information.	...
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	...
Compliance administrator	Can read and manage compliance configuration and reports in Azure AD and Office 365.	...
Conditional access administrator	Can manage conditional access capabilities.	...

Role Assignment

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.

Role Assignment

A role assignment is created that associates a security principal to a role. The role is further used to grant access to a resource scope. This decoupling allows you to specify that a specific role has access to a resource in your subscription and add/remove security principals from that role in a loosely connected manner. Roles can be assigned to the following types of Azure AD security principals:

- **Users.** Roles can be assigned to organizational users that are in the Azure AD with which the Azure subscription is associated. Roles can also be assigned to external Microsoft accounts that exist in the same directory.
- **Groups.** Roles can be assigned to Azure AD security groups. A user is automatically granted access to a resource if the user becomes a member of a group that has access. The user also automatically loses access to the resource after getting removed from the group. A best practice is to manage access through groups by assigning roles to those groups and adding users – instead of assigning roles directly to users.
- **Service principals.** Service identities are represented as service principals in the directory. They authenticate with Azure AD and securely communicate with one another. Services can be granted access to Azure resources by assigning roles through the Azure module for Windows PowerShell to the Azure AD service principal representing that service.

Role Definitions

Role definitions

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. This information is available with the **Get-AzRoleDefinition** cmdlet.

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/elevate-Access/Action ¹

Built-in Role	Action	NotActions
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"
```

Demonstration - RBAC

In this demonstration, you will learn about role assignments.

Locate Access Control blade

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

Review role permissions

- Select the **Roles** tab (top).
- Review the large number of built-in roles that are available.
- Double-click a role, and then select **Permissions** (top).
- Continue drilling into the role until you can view the **Read, Write, and Delete** actions for that role.
- 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>
```

Users and Groups

User Accounts

In Azure AD, all users who require access to resources must have a user account. A user account is an Azure AD user object that contains all the information that's required to authenticate and authorize the user during the sign-in process and build the user's access token.

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

NAME	USER NAME	USER TYPE	SOURCE
Ziaulla	[REDACTED]@macoutlook.com	Guest	Azure Active Directory
Retail Crisis Notifications	[REDACTED]@microsoft.com	Member	Windows Server AD
"Planning & Launch Services OEM Inquir	[REDACTED]@microsoft.com		Windows Server AD
Bert	[REDACTED]@hotmail.com	Guest	Azure Active Directory

Notice the Source in the above screenshot. There are different sources depending on the types of identity, including:

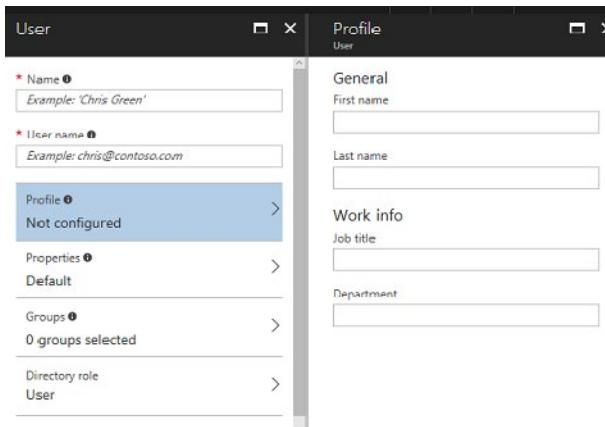
- **Cloud identities (Azure Active Directory).** Users that only exist in Azure AD. For example, administrator accounts or users you are managing yourself.
 - **Directory-synchronized identities (Windows Server AD).** Users brought in to Azure through a synchronization activity using Azure AD Connect. These are users that exist in Windows Server AD.
 - **Guest users (Azure Active Directory).** Users from outside Azure. For example, Google and Microsoft accounts.
- ✓ Have you given any thought as to the type of users you will need?

Adding 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.



Azure PowerShell

You can use the PowerShell **New-AzADUser** command to add cloud-based users.

```
# Create a password object
$PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile

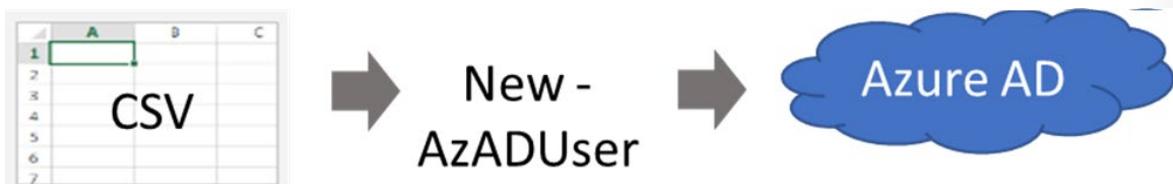
# Assign the password
$PasswordProfile.Password = "<Password>"

# Create the new user
New-AzADUser -AccountEnabled $True -DisplayName "Abby Brown" -PasswordProfile $PasswordProfile -MailNickname "AbbyB" -UserPrincipalName "AbbyB@contoso.com"
```

- ✓ Users can also be added to Azure AD through Office 365 Admin Center, Microsoft Intune admin console, and the CLI. Which of the options mentioned in this topic do you prefer?

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.

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

Group Accounts

A group helps organize users to make it easier to manage permissions. Groups can be easily added through the portal. There are two types of groups: security groups and distribution groups.

- **Security groups** are security-enabled and are used to assign permissions and control access to various resources.
- **Distribution groups** are used mainly by email applications and are not security enabled. You can easily add groups in the portal.

Users and groups - All groups

NAME	GROUP TYPE	MEMBERSHIP TYPE	
GR	Group1	Security	Assigned
GR	Group2	Security	Assigned
GR	Group23	Security	Assigned

Adding Groups

You can also use PowerShell to add a group with the **New-AzADGroup** command.

```
New-AzADGroup -Description "Marketing" -DisplayName "Marketing" -MailEnabled $false -SecurityEnabled $true -MailNickname "Marketing"
```

Adding Members to Groups

There are two ways to add members to Azure groups.

- **Directly Assigned.** In this situation you create the group then you manually add individual user accounts to the group.
 - **Dynamically Assigned.** In this situation you create rules to enable attribute-based dynamic memberships for groups based on characteristics. For example, if a user's Department is Sales, then they are dynamically assigned to the Sales group. You can set up a rule for dynamic membership on security groups or Office 365 groups. This feature requires an Azure AD Premium P1 license.
- ✓ Have you given any thought to which groups you need to create? Would you directly assign or dynamically assign membership?

Adding Group Members

Using Azure Active Directory, you can add and remove group members.

- From the **Groups** page, search for and select the group you want to add the member to.
- Select **Members** from the Manage area.
- Select **Add members**, and then search and select each of the members you want to add to the group.

The screenshot shows the Azure portal interface for managing group members. At the top, there is a breadcrumb navigation: Home > Groups - All groups > Managers - Members. Below this, the title 'Managers - Members' is displayed above a 'Group' section. On the left, a sidebar menu has 'Overview', 'Manage', 'Properties', and 'Members' listed, with 'Members' being the active tab. In the main content area, there is a button labeled '+ Add members' with a red box drawn around it. Below this button, there is a table with a single row showing a user named 'Chris Green' with a profile picture. The table has columns for 'NAME' and 'EMAIL'.

Adding group members with PowerShell

```
# Create a new group
New-AzAdgroup -DisplayName Developers -MailNickname Developers

# Retrieve the group ObjectId for the Developers group
Get-AzADGroup -DisplayName Developers

# Retrieve the user ObjectId for Chris Green
Get-AzureADUser

# Add the user to the group
Add-AzADGroupMember -ObjectId <group ObjectId> -RefObjectId <user ObjectId>

# Verify the members of the group
Get-AzAdGroupMember -GroupObjectId <group ObjectId>
```

Adding a Group Owner

Azure Active Directory (Azure AD) groups are owned and managed by group owners. Group owners are assigned to manage a group and its members by a resource owner (administrator). Group owners aren't required to be members of the group. After a group owner has been assigned, only a resource owner can add or remove owners.

In some cases, you as the administrator might decide not to assign a group owner. In this case, you become the group owner. Additionally, owners can assign other owners to their group, unless you've restricted this in the group settings.

- Select **Azure Active Directory**, select **Groups**, and then select the group for which you want to add an owner.
- Select **Add owners**, and then search for and select the user that will be the new group owner.

The screenshot shows the 'Managers - Owners' blade for a group in the Azure portal. On the left, there's a sidebar with 'Overview', 'Properties', 'Members', and 'Owners'. The 'Owners' tab is highlighted with a blue background. At the top right, there's a 'Add owners' button with a plus sign and a 'Refresh' button. Below the button, there's a 'NAME' input field and a message saying 'No owners have been found'.

Add a group owner in PowerShell

```
# Get the group ObjectId
Get-AzADGroup

# Get the owner (user) RefObjectId
Get-AzADUser

# Add the user as a group owner
Add-AzADGroupOwner -ObjectId <group ID> -RefObjectId <user ID>

# Verify group ownership
Get-AzADGroupOwner -ObjectId <group ID>
```

Demonstration - Users and Groups

In this demonstration, you 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, user@gmail.onmicrosoft.com.

Explore user accounts

1. Select the **Users** blade.
 2. Select **New user**.
 3. Notice the selection to create a **New guest user**.
 4. Create a **New user**. Replace your domain.
- **Name:** *Chris Green*
 - **Address:** *chris@your domain*
 - **Profile information:** Enter first and last name.
 - **Directory Role - User.**
5. Review the **User Settings** blade.
 6. Review the **Audit Logs** blade.

Explore group accounts

1. Select the **Groups** blade.
 2. Add a **New group**.
- **Group type:** *Security*
 - **Group name:** *Managers*
 - **Membership type:** *Assigned*
 - **Members:** Add *Chris Green* to the group.
3. Under **Settings** review the **General** blade.
 4. Under **Activity** review the **Audit Logs** blade.

Explore PowerShell for group management

1. Create a new group called Developers

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

2. Retrieve the Developers group ObjectId

```
Get-AzADGroup
```

3. Retrieve the user ObjectId for the member to add

```
Get-AzADUser
```

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

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

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

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

Azure Policy

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.

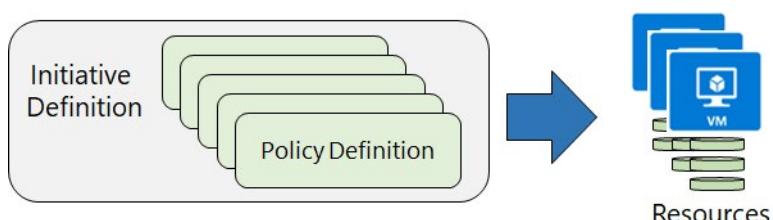
Azure Policy will be important to you if your team runs an environment where you need to govern:

- 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

For more information:

Azure Policy Documentation - <https://docs.microsoft.com/azure/azure-policy/>⁷

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.

⁷ <https://docs.microsoft.com/azure/azure-policy/>

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.

NAME	DEFINITION ID	POLICY ID	TYPE	DEFINITION STATE	CATEGORY
[Preview]: Enable Monitoring in Azure Security Ce...	38		Built-in	Initiative	Security Center
Audit enabling of diagnostic logs in Azure Data L...			Built-in	Policy	Data Lake
Audit VMs that do not use managed disks			Built-in	Policy	Compute
[Preview]: Deploy default CMS VM Extension for ...			Built-in	Policy	Compute
[Preview]: Monitor unencrypted VM Disks in Secur...			Built-in	Policy	Security Center
Audit resource location matches resource group L...			Built-in	Policy	General
Audit transparent data encryption status			Built-in	Policy	SQL
Audit use of classic virtual machines			Built-in	Policy	Compute

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](#)⁸. New Policy Definitions are added almost every day.

- ✓ Policy Definitions have a **specific JSON format**⁹. 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.

⁸ <https://github.com/Azure/azure-policy/tree/master/samples>

⁹ <https://docs.microsoft.com/en-us/azure/azure-policy/policy-definition>

Create Initiative Definitions

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

Initiative definition
New Initiative definition

* Definition location
Visual Studio Enterprise

* Name
cesbranchoffice

Category
 Create new Use existing
General

POLICIES AND PARAMETERS

Initiatives are composed of one or more policies. Add policies to this Initiative from the list on the right.

Audit VMs that do not use managed disks ... This policy audits VMs that do not use managed disks

Require SQL Server version 12.0 ... This policy ensures all SQL servers use version 12.0.

- ✓ What planning will be needed to organize your policy definitions?

Scope the Initiative Definition

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

Home > Policy > Definitions

Policy - Definitions

Assign View definition Edit definition + Initiative definition + Policy definition Refresh

Scope: Contoso Subscription | Definition Type: All types | Category: All categories | Search: Filter by name or id...

Initiative Definitions (2) Policy Definitions (36)

NAME	DEFINITION LOCATION	POLICIES	DESCRIPTION	TYPE	CATEGORY
[Preview]: Enable Monitoring i...		13	Monitor all the available security recommendations ...	Built-in	Security Center ...
Get Secure	Contoso Subscription	5	This initiative has been created to handle all policy ...	Custom	Security Center ...

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

Scope

Subscription
ASC DEMO

Resource Group
Optional choose a Resource Group

- AppServiceRG
- ASCDEMO
- ASCDDEMORG
- ASCDEMORGasclogs
- AzureBackupRG_eastus_1

- ✓ Currently, an Initiative Definition can have up to 100 policies.

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.

The screenshot shows the Azure Policy - Compliance blade. On the left, there's a navigation menu with 'Overview', 'Getting started', and 'Compliance' (which is highlighted with a red box). Below that are sections for 'AUTHORING', 'Assignments', and 'Definitions'. The main area has filters for 'Scope' (Contoso Subsc...), 'Type' (All types), and 'Compliance State' (All compliance states). It displays three counts: 'Non-compliant initiatives' (0 out of 0), 'Non-compliant policies' (0 out of 1), and 'Non-compliant resources' (0). A table below lists a single policy assignment: 'Audit VMs that do not use ...' with a scope of 'Contoso Subscri...', status 'Compliant', and a count of 0 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.

For more information:

Video - Azure Resource Manager (ARM) Policies & RBAC - https://www.youtube.com/watch?v=CGx-NV_qKmqA

Demonstration - Azure Policy

In this demonstration, we will create a policy.

Assign a policy

1. Launch the Azure Policy service in the Azure portal by clicking **All services**, then searching for and selecting **Policy**. This service is under **Management and Governance**.
2. Select **Assignments** on the left side of the Azure Policy page. An assignment is a policy that has been assigned to take place within a specific scope.
3. Select **Assign Policy** from the top of the Policy - Assignments page.
4. Notice the **Scope** which determines what resources or grouping of resources the policy assignment gets enforced on.
5. Select the **Policy definition ellipsis** to open the list of available definitions. Take some time to review the built-in policy definitions.
6. Select **Require SQL Server version 12.0**. This policy ensures all SQL servers use version 12.0. If this policy definition is not available select something else.
7. Leave Create a **Managed Identity** unchecked.
8. Click **Assign** to create your 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 **Require SQL Server version 12.0** 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.

Lab and Review Questions

Lab - Role-Based Access Control

Scenario

Adatum Corporation wants to use Azure Role Based Access Control and Azure Policy to control provisioning and management of their Azure resources. It also wants to be able to automate and track provisioning and management tasks.

Objectives

After completing this lab, you will be able to:

- Configure delegation of provisioning and management of Azure resources by using built-in Role-Based Access Control (RBAC) roles and built-in Azure policies.
- Verify delegation by provisioning Azure resources as a delegated admin and auditing provisioning events.

Exercise 1: Configure delegation of provisioning and management of Azure resources by using built-in Role-Based Access Control (RBAC) roles and built-in Azure policies.

The main tasks for this exercise are as follows:

- Create Azure Active Directory (AD) users and groups.
- Create Azure resource groups.
- Delegate management of an Azure resource group via a built-in RBAC role.
- Assign a built-in Azure policy to an Azure resource group.

Result: After you completed this exercise, you have created an Azure AD user and an Azure AD group, created two Azure resource groups, delegated management of the first Azure resource group via the built-in Azure VM Contributor RBAC role, and assigned to the same resource group the built-in Azure policy restricting SKUs that can be used for Azure VMs.

Exercise 2: Verify delegation by provisioning Azure resources as a delegated admin and auditing provisioning events.

The main tasks for this exercise are as follows:

- Identify an available DNS name for an Azure VM deployment.
- Attempt an automated deployment of a policy non-compliant Azure VM as a delegated admin.
- Perform an automated deployment of a policy compliant Azure VM as a delegated admin.
- Review Azure Activity Log events corresponding to Azure VM deployments.

Result: After you completed this exercise, you have identified an available DNS name for an Azure VM deployment, attempted an automated deployment of a policy non-compliant Azure VM as a delegated admin, performed an automated deployment of a policy compliant Azure VM as the same delegated admin, and reviewed Azure Activity Log entries corresponding to both Azure VM deployments.

Lab - Governance and Compliance

Scenario

Adatum Corporation wants to use Azure policies and initiatives in order to enforce resource tagging in its Azure subscription. Once the environment is compliant, Adatum wants to prevent unintended changes by implementing resource locks.

Objectives

After completing this lab, you will be able to:

- Implement Azure tags by using Azure policies and initiatives.
- Implement Azure resource locks.

Exercise 1: Implement Azure tags by using Azure policies and initiatives.

The main tasks for this exercise are as follows:

- Provision Azure resources by using an Azure Resource Manager template.
- Implement an initiative and policy that evaluate resource tagging compliance.
- Implement a policy that enforces resource tagging compliance.
- Evaluate tagging enforcement and tagging compliance.
- Implement remediation of resource tagging non-compliance.
- Evaluate effects of the remediation task on compliance..

Result: After you completed this exercise, you have implemented an initiative and policies that evaluate, enforce, and remediate resource tagging compliance. You also evaluated the effects of policy assignment.

Exercise 2: Implement Azure resource locks.

The main tasks for this exercise are as follows:

- Create resource group-level locks to prevent accidental changes.
- Validate functionality of the resource group-level locks.

Result: After you completed this exercise, you have created a resource group-level lock to prevent accidental changes and validated its functionality.

Module Review Questions

Review Question 1

Your team, the cloud administration team, is creating custom Azure roles as part of a role-based access implementation in Microsoft Azure. One of the other administrators is tasked with creating a custom role based on the Contributor built-in role. The only difference will be that the custom role will not be able to create new VMs.

The other administrator creates a role named Role1. During Role1 testing, a new VM could be created under the new role. You use the Get-AzRoleDefinition cmdlet to view details of the role, and you find the following configuration:

```
Actions      : {*}
NotActions   : {}
AssignableScopes: {}
```

You need to update the configuration, while minimizing administrative overhead, to ensure that it meets the requirements. What should you do? Select one.

- Recreate the role.
- Update the Actions value.
- Update the NotActions value.
- Update the AssignableScopes value.

Review Question 2

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 3

You have created a new group called Managers. You would like any user account that has the name Manager in their Job Title to be placed in the new Manager group. Which of the following do you need to implement? Select one.

- Directly assigned groups
- Dynamically assigned groups
- RBAC assigned groups
- Taxonomy assigned groups
- Azure policy assigned groups

Review Question 4

Your organization has a large number of users. The user data is currently in a SQL database. You would like to import the user data into Azure. What format should you use? Select one.

- CSV
- DBX
- JSON
- XML

Review Question 5

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
- Consolidate subscriptions

Review Question 6

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.

Review Question 7

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 8

Your organization is considering migrating workloads to Azure. You need to provide a cost estimation for the project. The estimate should include all areas of Azure including compute, networking, storage, web, and databases. You would like the estimate to be in your country's currency. What should you do? Select one.

- Create a free Azure subscription and use the Billing blade.
- Enter your workloads in the Pricing Calculator.
- Review the pricing page for each workload and create a spreadsheet of estimated costs.
- Enter your workloads in the Total Cost of Ownership Calculator.

Review Question 9

Your company hires a new IT administrator. She needs to manage a resource group with first-tier web servers. However, she should not be able to control access to the resource group. Additionally, she should not have access to other resource groups. 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 10

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

- Create a billing alert.
- Create an Azure reservation.
- Create a management group.
- Create a monthly budget.

Answers

Review Question 1

Your team, the cloud administration team, is creating custom Azure roles as part of a role-based access implementation in Microsoft Azure. One of the other administrators is tasked with creating a custom role based on the Contributor built-in role. The only difference will be that the custom role will not be able to create new VMs.

The other administrator creates a role named Role1. During Role1 testing, a new VM could be created under the new role. You use the Get-AzRoleDefinition cmdlet to view details of the role, and you find the following configuration:

```
Actions      : {*}
NotActions   : {}
AssignableScopes: {}
```

You need to update the configuration, while minimizing administrative overhead, to ensure that it meets the requirements. What should you do? Select one.

- Recreate the role.
- Update the Actions value.
- Update the NotActions value.
- Update the AssignableScopes value.

Explanation

*In this scenario, based on the output of the cmdlet, Role1 has unlimited actions (represented by *), without restrictions via NotActions (represented by the value being empty), and with all scopes (represented by the /). To meet the requirements of not being able to create VMs, you should update the NotActions value.*

Review Question 2

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

Review Question 3

You have created a new group called Managers. You would like any user account that has the name Manager in their Job Title to be placed in the new Manager group. Which of the following do you need to implement? Select one.

- Directly assigned groups
- Dynamically assigned groups
- RBAC assigned groups
- Taxonomy assigned groups
- Azure policy assigned groups

Explanation

Dynamically assigned groups use rules to assign members based on profile characteristics.

Review Question 4

Your organization has a large number of users. The user data is currently in a SQL database. You would like to import the user data into Azure. What format should you use? Select one.

- CSV
- DBX
- JSON
- XML

Explanation

There are several ways you can use PowerShell to import data into your directory, but the most commonly used method is to use a 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.

Review Question 5

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
- Consolidate subscriptions

Explanation

Management groups can be used to organize and manage subscriptions.

Review Question 6

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

You should 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.

Review Question 7

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

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 8

Your organization is considering migrating workloads to Azure. You need to provide a cost estimation for the project. The estimate should include all areas of Azure including compute, networking, storage, web, and databases. You would like the estimate to be in your country's currency. What should you do? Select one.

- Create a free Azure subscription and use the Billing blade.
- Enter your workloads in the Pricing Calculator.
- Review the pricing page for each workload and create a spreadsheet of estimated costs.
- Enter your workloads in the Total Cost of Ownership Calculator.

Explanation

The pricing calculator can provide an estimate of costs before you create an Azure resource. The Pricing Calculator provides estimates in all areas of Azure including compute, networking, storage, web, and databases.

Review Question 9

Your company hires a new IT administrator. She needs to manage a resource group with first-tier web servers. However, she should not be able to control access to the resource group. Additionally, she should not have access to other resource groups. 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

The IT person needs Contributor access to the resource group. This will allow her to manage the virtual machines in the resource group, but not be able to add or remove access to the group.

Review Question 10

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

- Create a billing alert.
- Create an Azure reservation.
- Create a management group.
- Create a monthly budget.

Explanation

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.

Module 12 Data Services

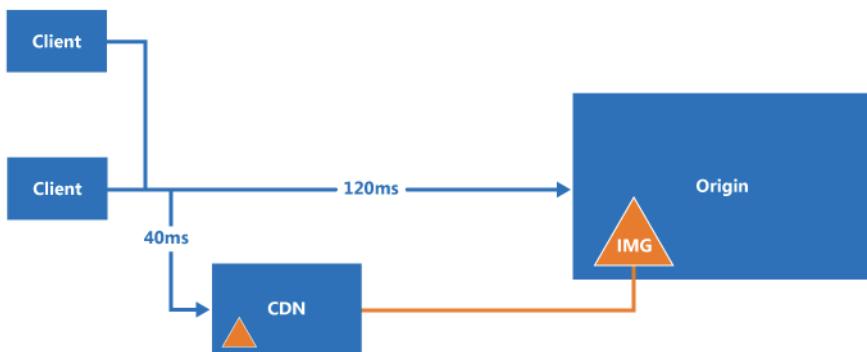
Content Delivery Network

CDN Benefits

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver content to users. CDNs store cached content on edge servers that are close to end-users.

CDNs are typically used to deliver static content such as images, style sheets, documents, client-side scripts, and HTML pages. The main benefits of using a CDN are:

- Lower latency and faster delivery of content to users, regardless of their geographical location in relation to the datacenter where the application is hosted.
- Helps to reduce load on a server or application, because it does not have to service requests for the content that is hosted in the CDN.



Typical uses for a CDN include:

- Delivering static resources for client applications, often from a website.
- Delivering public static and shared content to devices such as cell phones and tablet computers.
- Serving entire websites that consist of only public static content to clients, without requiring any dedicated compute resources.

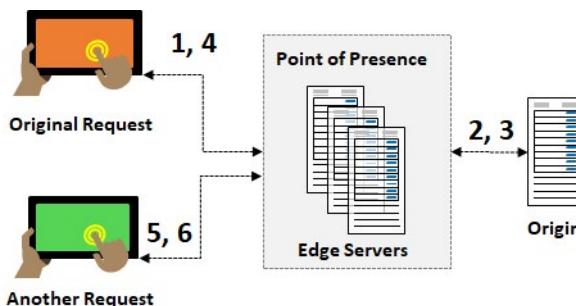
- Streaming video files to the client on demand.
 - Generally improving the experience for users, especially those located far from the datacenter hosting the application.
 - Supporting IoT (Internet of Things) solutions, such as distributing firmware updates.
 - Coping with peaks and surges in demand without requiring the application to scale, avoiding the consequent increased running costs.
- CDN provides a faster, more responsive user experience. Do you think your organization would be interested in this feature?
- Use the following link to review some of the challenges with deploying CDN including security, deployment, versioning, and testing.

For more information:

Content Delivery Network Documentation - <https://docs.microsoft.com/en-us/azure/cdn/cdn-overview>

How CDN Works

You can enable Azure Content Delivery Network to cache content for the user. The Azure CDN is designed to send audio, video, images, and other files faster and more reliably to customers using servers that are closest to the users. This dramatically increases speed and availability, resulting in significant user experience improvements.



1. A user (Alice) requests a file (also called an asset) using a URL with a special domain name, such as endpointname.azureedge.net. DNS routes the request to the best performing Point-of-Presence (POP) location, which is usually the POP that is geographically closest to the user.
2. If the edge servers in the POP do not have the file in their cache, the edge server requests the file from the origin. The origin can be an Azure Web App, Azure Cloud Service, Azure Storage account, or any publicly accessible web server.
3. The origin returns the file to the edge server, including optional HTTP headers describing the file's Time-to-Live (TTL).
4. The edge server caches the file and returns the file to the original requestor (Alice). The file remains cached on the edge server until the TTL expires. Azure CDN automatically applies a default TTL of seven days unless you've set up caching rules in the Azure portal.
5. Additional users may then request the same file using that same URL and may also be directed to that same POP.
6. If the TTL for the file hasn't expired, the edge server returns the file from the cache.

- ✓ After you enable CDN access to a storage account, all publicly available objects are eligible for CDN edge caching. If you modify an object that's currently cached in the CDN, the updated content will not be available via CDN until CDN refreshes its content after the time-to-live period for the cached content expires.

CDN Profiles

A CDN profile is a collection of CDN endpoints with the same pricing tier and provider (origin). You may create multiple profiles to organize endpoints. For example, you could have profiles with endpoints to different internet domains, web applications, or storage accounts. You can create up to 8 CDN profiles per subscription.

CDN profile

* Name
DevCDN

* Subscription
Visual Studio Enterprise

* Resource group
ASH

Create new

* Resource group location ⓘ
South Central US

* Pricing tier (View full pricing details)

All Available Pricing

- Standard Microsoft
- Standard Verizon
- Standard Akamai
- Premium Verizon

You can create a CDN profile from the Azure portal.

The CDN service is global and not bound to a location, however you must specify a resource group location where the metadata associated with the CDN profile will reside. This location will not have any impact on the runtime availability of your profile.

Several pricing tiers are available. At the time of this writing, there are four tiers: Azure CDN Standard from Microsoft, Azure CDN Standard from Akamai, Azure CDN Standard from Verizon, and Azure CDN Premium from Verizon. Pricing is based on TBs of outbound data transfers.

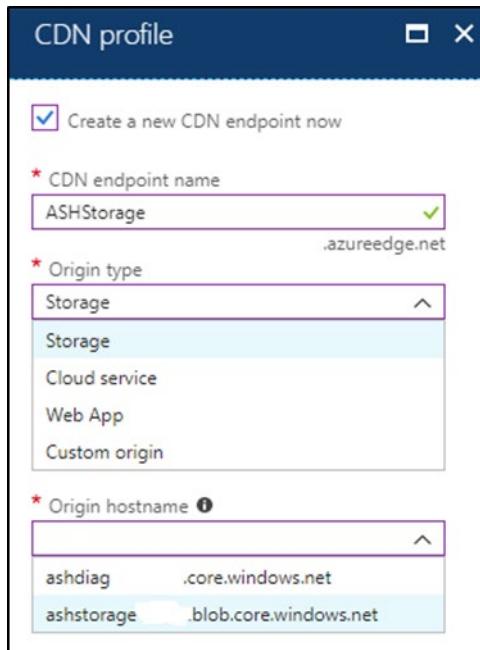
Notice you can create your first profile endpoint directly from this blade (last checkbox, not shown).

- ✓ Can you think of different scenarios that would require different CDN profiles?

CDN Endpoints

When you create a new CDN endpoint directly from the CDN profile blade you are prompted for CDN endpoint name, Origin type, and Origin hostname. To access cached content on the CDN, use the CDN URL provided in the portal. In this case,

```
ASHStorage.azureedge.net/<myPublicContainer>/<BlobName>
```



There are four choices for Origin type: Storage, Cloud Service, Web App, and Custom origin. In this course we are focusing on storage CDNs.

When you select Storage as the Origin type, the new CDN endpoint uses the host name of your storage account as the origin server.

There are additional CDN features for your delivery, such as compression, query string, and geo filtering. You can also add custom domain mapping to your CDN endpoint and enable custom domain HTTPS. These options are configured in the Settings blade for the endpoint.

- ✓ Because it takes time for the registration to propagate, the endpoint isn't immediately available for use. For Azure CDN from Akamai profiles, propagation usually completes within one minute. For Azure CDN from Verizon profiles, propagation usually completes within 90 minutes, but in some cases can take longer.

CDN Time-to-Live

Any publicly accessible blob content can be cached in Azure CDN until its time-to-live (TTL) elapses. The TTL is determined by Cache-directive headers in the HTTP response from the origin server. If the Cache-Control header does not provide the TTL information, or if you prefer, you can configure caching rules to set the **Cache Expiration Duration**.

- **Global caching rules.** You can set the Cache Expiration Duration for each endpoint in your profile, which affects all requests to the endpoint. TTL is configured as days, hours, minutes, and seconds.

Global caching rules
These rules affect the CDN caching behavior for all requests, and can be overridden using Custom Cache Rules below for certain scenarios. Note that the Query string caching behavior setting does not affect files that are not cached by the CDN.

Caching behavior: Set if missing

Cache expiration duration: Days 10, Hours 0, Minutes 0, Seconds 0

Query string caching behavior: Ignore query strings

- **Custom caching rules.** You can also create custom caching rules for each endpoint in your profile. Custom caching rules match specific paths and file extensions, are processed in order, and override the global caching rule.

Custom caching rules
Create caching rules based on specific match conditions. These rules override the default settings above, and are evaluated from top to down. This means that rules lower on the list can override rules above it in the list, as well as the global caching rules and default behavior. Therefore it makes more sense to have more specific rules towards the bottom of the list so they are not overwritten by a general rule under them. For example a rule for path '/folder/images/*' should be below a rule for path '/folder/'.

Match Condition	Match Value(s)	Caching Behavior	Days	Hours	Minutes	Seconds
Path	/images/*.jpg	Override	30	0	0	0
			0	0	0	0

CDN Compression

File compression is a simple and effective method to improve file transfer speed and increase page-load performance by reducing a file's size before it is sent from the server. File compression can reduce bandwidth costs and provide a more responsive experience for your users.

There are two ways to enable file compression:

- Enable compression on your origin server. In this case, the CDN passes along the compressed files and delivers them to clients that request them.
- Enable compression directly on the CDN edge servers. In this case, the CDN compresses the files and serves them to end users.

Enabling compression in the standard tiers

In the Azure portal, you can enable Compression and modify the MIME types list to tune which content formats to compress.

Configure

Compression: On

Formats to compress

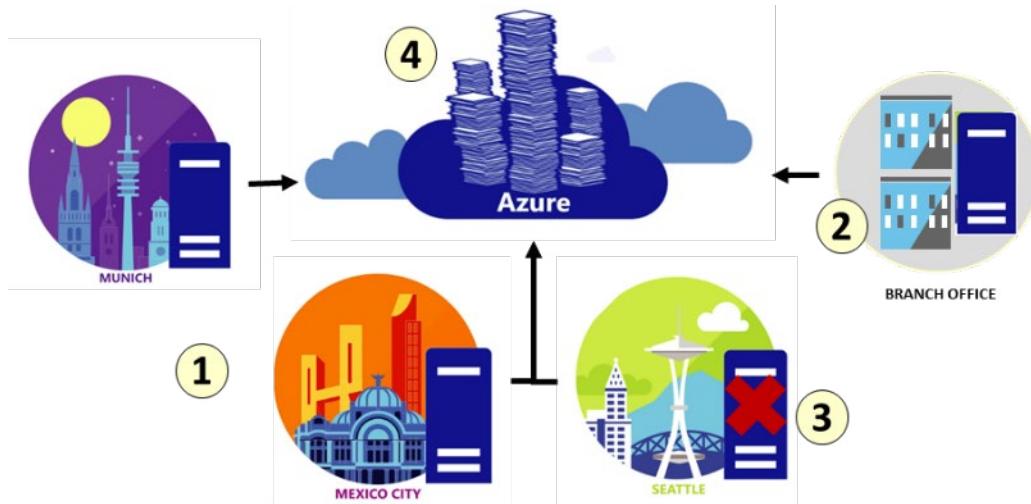
- text/plain
- text/html
- text/css
- text/javascript

- ✓ Although, it is not recommended to apply compression to compressed formats, for example, ZIP, MP3, MP4, or JPG.

File Sync

Azure 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.

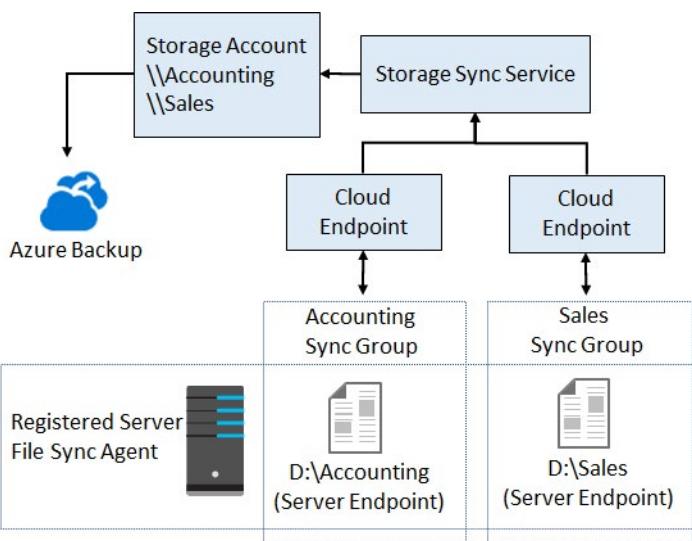
- Lift and shift.** The ability to move applications that require access between Azure and on-premises systems. Provide write access to the same data across Windows Servers and Azure Files. This lets companies with multiple offices have a need to share files with all offices.
 - Branch Offices.** Branch offices need to backup files, or you need to setup a new server that will connect to Azure storage.
 - 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.
 - 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 deployment - <https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-planning>

File Sync Components

To gain the most from Azure File Sync, it's important to understand the terminology.



Storage Sync Service. The Storage Sync Service is the top-level Azure resource for Azure File Sync. The Storage Sync Service resource is a peer of the storage account resource, and can similarly be deployed to Azure resource groups. A distinct top-level resource from the storage account resource is required because the Storage Sync Service can create sync relationships with multiple storage accounts via multiple sync groups. A subscription can have multiple Storage Sync Service resources deployed.

Sync group. A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. If, for example, you have two distinct sets of files that you want to manage with Azure File Sync, you would create two sync groups and add different endpoints to each sync group. A Storage Sync Service can host as many sync groups as you need.

Registered server. The registered server object represents a trust relationship between your server (or cluster) and the Storage Sync Service. You can register as many servers to a Storage Sync Service instance as you want. However, a server (or cluster) can be registered with only one Storage Sync Service at a time.

Azure File Sync agent. The Azure File Sync agent is a downloadable package that enables Windows Server to be synced with an Azure file share. The Azure File Sync agent has three main components:

- FileSyncSvc.exe: The background Windows service that is responsible for monitoring changes on server endpoints, and for initiating sync sessions to Azure.
- StorageSync.sys: The Azure File Sync file system filter, which is responsible for tiering files to Azure Files (when cloud tiering is enabled).
- PowerShell management cmdlets: PowerShell cmdlets that you use to interact with the Microsoft StorageSync Azure resource provider. You can find these at the following (default) locations:
 - C:\Program Files\Azure\StorageSyncAgent\StorageSync.Management.PowerShell.Cmdlets.dll
 - C:\Program Files\Azure\StorageSyncAgent\StorageSync.Management.ServerCmdlets.dll

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

endpoint are skipped. You can create a server endpoint on the system volume but, there are two limitations if you do so:

- Cloud tiering cannot be enabled.
- Rapid namespace restore (where the system quickly brings down the entire namespace and then starts to recall content) is not performed.

Cloud endpoint. A cloud endpoint is an Azure file share that is part of a sync group. The entire Azure file share syncs, and an Azure file share can be a member of only one cloud endpoint. Therefore, an Azure file share can be a member of only one sync group. If you add an Azure file share that has an existing set of files as a cloud endpoint to a sync group, the existing files are merged with any other files that are already on other endpoints in the sync group.

File Sync - Initial Steps

There are a few things that need to be configured before you synchronize your files.



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.

Home > Deploy Storage Sync

Deploy Storage Sync

* Name: StorageSync1

* Subscription: Visual Studio Enterprise

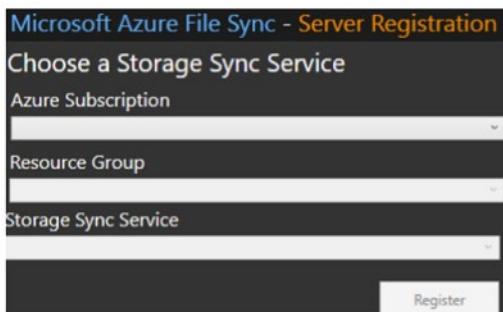
* Resource group: ASH

* Location: South Central US

Create Automation options

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.



- ✓ Continue to the next topic for an explanation of how files are synchronized.

File Sync - Synchronization

Before synchronizing your files, you will need to do two other things.

Create a sync group with a cloud endpoint

In this step you will create a sync group with at least one cloud endpoint. The cloud endpoint is a pointer to an Azure file share. All server endpoints will sync with a cloud endpoint, making the cloud endpoint the hub. The storage account for the Azure file share must be located in the same region as the Storage Sync Service. Notice you will need a storage account and a file share.

The entirety of the Azure file share will be synced, with one exception: A special folder, comparable to the hidden "System Volume Information" folder on an NTFS volume, will be provisioned. This directory is called ".SystemShareInformation". It contains important sync metadata that will not sync to other endpoints. Do not use or delete it!

Sync group

Start by specifying an Azure file share to sync with - this is the sync group's first cloud endpoint. You can specify a folder on your servers you want to sync later.

Sync group name	<input type="text"/>
1st Cloud endpoint	
Subscription	<input type="text" value="Visual Studio Enterprise"/>
Storage account	<input type="button" value="Select storage account"/>
<input type="text" value="Azure storage account ID"/>	
<div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <div style="display: flex; align-items: center;"> ! If you have previously configured Azure Data Box to import data to the cloud, do not specify a file share that contains that data. Instead, use an empty file share as a cloud endpoint. </div> <div style="margin-top: 5px;"> Specify the share with Azure Data Box content when you add the server endpoint later. </div> </div>	
Azure File Share	<input type="text" value="Provide an Azure File Share name."/>
<input type="button" value="Create"/>	<input type="button" value="Cancel"/>

Create server endpoints

Creating a server endpoint requires:

- **Registered server.** The name of the server or cluster where you want to create the server endpoint.
- **Path.** The Windows Server path to be synced as part of the sync group. The path should not be the root volume.
- **Cloud Tiering.** A switch to enable or disable cloud tiering. Regardless of whether cloud tiering is enabled, your Azure file share always has a complete copy of the data in the sync group.
- **Volume Free Space.** The amount of free space to reserve on the volume on which the server endpoint is located. For example, if volume free space is set to 50% on a volume that has a single server endpoint, roughly half the amount of data is tiered to Azure Files.

The screenshot shows the 'Add server endpoint' dialog box with the following fields:

- Registered server:** A dropdown menu showing 'FileServer'.
- Path:** An input field containing the path '\'.
A tooltip 'Path' is visible above the input field.
- Cloud Tiering:** A toggle switch between 'Enabled' (grayed out) and 'Disabled' (selected).
- Volume Free Space (%):** A slider bar set to 50%.

- ✓ Azure File Sync moves file data and metadata exclusively over HTTPS and requires port 443 to be open outbound. Based on policies in your datacenter, branch or region, further restricting traffic over port 443 to specific domains may be desired or required.
- ✓ There is a lot to consider when synchronizing large amounts of files. For example, you may want to copy the server files to the Azure file share before you configure file sync. You will on-board and monitor File Sync in the lab.

Import and Export Service

Import and Export Service

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files. With the Azure Import/Export service, you supply your own disk drives and transfer data yourself.

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.
- ✓ A single job can include up to 10 disks. You can create jobs directly from the Azure portal. You can also accomplish this programmatically by using Azure Storage Import/Export REST API.

For more information:

Azure Import and Export Service - <https://azure.microsoft.com/en-us/documentation/articles/storage-import-export-service/>

Components and Requirements

This topic lists the components that make up Import/Export service and the requirements for using the service.

Import and Export service components

- **Import/Export service.** This service available in Azure portal helps the user create and track data import (upload) and export (download) jobs.
- **WAImpoerExport tool.** This is a command-line tool that does the following:
 - Prepares your disk drives that are shipped for import.
 - Facilitates copying your data to the drive.
 - Encrypts the data on the drive with BitLocker.
 - Generates the drive journal files used during import creation.
 - Helps identify numbers of drives needed for export jobs.

Note: The WAImpoerExport tool is available in two versions, version 1 and 2. We recommend that you use:

Version 1 for import/export into Azure Blob storage.

Version 2 for importing data into Azure files.

- **Disk Drives.** You can ship Solid-state drives (SSDs) or Hard disk drives (HDDs) to the Azure datacenter. When creating an import job, you ship disk drives containing your data. When creating an export job, you ship empty drives to the Azure datacenter.

Requirements

Operating systems

- Windows Server 64-bit OS that supports BitLocker Drive Encryption.
- Windows clients that have .NET Framework 4.5.1 and BitLocker.

Supported storage accounts

- General Purpose v2 storage accounts (recommended for most scenarios)
- Blob Storage accounts
- General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments)

Supported storage types

- Import jobs can include Azure Blob storage, Azure File storage, Blob blobs, and Page blobs.
- Export jobs can include Azure Blob storage, Block blobs, Page blobs, and Append blobs. Azure Files not supported.

Supported disks

Disk type	Size	Supported	Not supported
SSD	2.5"	All	
HDD	2.5" and 3.5"	SATA II, SATA III	External HDD with built-in USB adaptor and disks inside the casing of an external HDD.

Import and Export Tool

The **Microsoft 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 WAImportExport tool from that computer. The WAImportExport 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.

What is a journal file?

Each time you run the WAImportExport tool to copy files to the hard drive, the tool creates a copy session. The state of the copy session is written to the journal file. If a copy session is interrupted (for example, due to a system power loss), it can be resumed by running the tool again and specifying the journal file on the command line.

For each hard drive that you prepare with the Azure Import/Export Tool, the tool will create a single journal file with name DriveID.xml where DriveID is the serial number associated to the drive that the tool reads from the disk. You will need the journal files from all of your drives to create the import job. The journal file can also be used to resume drive preparation if the tool is interrupted.

Simple Import Example

```
WAImportExport.exe PrepImport /j:<JournalFile> /id:<SessionId> /DataSet:<-
dataset.csv>
```

- **PrepImport.** Indicates the tool is preparing drives for an import job.
- **JournalFile.** Path to the journal file that will be created. A journal file tracks a set of drives and records the progress in preparing these drives. The journal file must always be specified.
- **SessionId.** The session Id is used to identify a copy session. It is used to ensure accurate recovery of an interrupted copy session.
- **DataSet.** A CSV file that contains a list of directories and/or a list of files to be copied to target drives.
- ✓ The WAImportExport tool is available from Microsoft Download site at <https://aka.ms/Welhs7>.

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.

Your job will be configured in the Portal. Notice the need for the journal file, created by the Import/Export tool, and a storage account to receive the data. Not shown is the return shipping information.

Create import/export job		Job details				
* Type <input checked="" type="radio"/> Import into Azure <input type="radio"/> Export from Azure		Data source Upload journal files ⓘ <input type="button" value="Select a file"/> <input type="button" value="Delete"/> <table border="1"> <thead> <tr> <th>DRIVE ID</th> <th>JOURNAL FILE</th> </tr> </thead> <tbody> <tr> <td colspan="2">No files uploaded.</td> </tr> </tbody> </table>	DRIVE ID	JOURNAL FILE	No files uploaded.	
DRIVE ID	JOURNAL FILE					
No files uploaded.						
* Name <input type="text" value="ImportTest"/> 						
* Subscription <input type="text" value="Azure Pass - Sponsorship"/>		Import destination * Storage account <input type="text" value="rgtest11"/>  <hr/> * Drop-off location <input type="text" value="West US"/>				
* Resource group <input type="text" value="rgtest"/>  Create new						
<input checked="" type="checkbox"/> Save verbose log in the 'waimportexport' blob container						

To perform an import, follow these steps:

1. Create an Azure Storage account.
2. Identify the number of disks that you will need to accommodate all the data that you want to transfer.

3. 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 WAImpoerExport tool.
4. Run the WAImpoerExport tool to copy the data, encrypt the drive with BitLocker, and generate journal files.
5. 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.
6. Ship the disks to the destination that you specified when creating the import job and update the job by providing the shipment tracking number.
7. 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.

Create import/export job	Job details
<p>* Type <input type="radio"/> Import into Azure <input checked="" type="radio"/> Export from Azure</p> <p>* Name <input type="text" value="ExportTest"/> </p> <p>* Subscription <input type="text" value="Azure Pass - Sponsorship"/> </p> <p>* Resource group <input type="text" value="rgtest"/>  Create new</p>	<p>Data source</p> <p>* Storage account <input type="text" value="rgtest11"/> </p> <p>* Drop-off location <input type="text" value="West US"/> </p> <p>Blobs to export</p> <p><input checked="" type="radio"/> Export all <input type="radio"/> Selected containers and blobs <input type="radio"/> Export from blob list file (XML format)</p> <p><input checked="" type="checkbox"/> Save verbose log in the 'waimportexport' blob container</p>



In order to perform an export, follow these steps:

1. Identify the data in the Azure Storage blobs that you intend to export.
2. Identify the number of disks that you will need to accommodate all the data you want to transfer.
3. 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.
4. Ship the required number of disks to the Azure region hosting the storage account. Update the job by providing the shipment tracking number.
5. 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.

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.

What's new

- 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:

Download and install AzCopy on Windows - <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy#download-and-install-azcopy-on-windows>¹

Demonstration - AzCopy

In this demonstration, we will explore AzCopy.

¹ <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy>

Install the AzCopy tool

1. Download the Windows 8.1 version - <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy?toc=%2fazure%2fstorage%2ftables%2ftoc.json#download-and-install-azcopy-on-windows>.
2. Install and launch the tool.

Explore the help

1. Launch the Microsoft Azure Storage AzCopy tool.
2. View the help.

```
azcopy /?
```

3. Scroll to the top of the Help information and read about the **Common options**, like: source, destination, source key, and destination key.
4. Scroll down the **Samples** section. We will be trying several of these examples. Are any of these examples particularly interesting to you?

Download a blob from Blob storage to the file system

Note: This example requires an Azure storage account with blob container and blob file. You will also need to capture parameters in a text editor like Notepad.

1. Access the Azure portal.
2. Access your storage account with the blob you want to download.
3. Select **Access keys** and copy the **Key Key1** value. This will be the *sourcekey*: value.
4. Drill down to the blob of interest, and view the file **Properties**.
5. Copy the **URL** information. This will be the *source*: value.
6. Locate a local destination directory. This will be the *dest*: value. A filename is also required.
7. Construct the command using your values.

```
azcopy /source:sourceURL /dest:destinationdirectoryandfilename /sourcekey:"key"
```

8. If you have errors, read them carefully and make corrections.
9. Verify the blob was downloaded to your local directory.

Upload files to Azure blob storage

Note: The example continues from the previous example and requires a local directory with files.

1. The *source*: for the command will be a local directory with files.
2. The *dest*: will the blob URL used in the previous example. Be sure to remove the filename, just include the storage account and container.
3. The *destkey*: will the key used in the previous example.
4. Construct the command using your values.

```
azcopy /source:source /dest:destinationcontainer /destkey:key
```

5. If you have errors, read them carefully and make corrections.

-
6. Verify your local files were copied to the Azure container.
 7. Notice there are switches to recurse subdirectories and pattern match.

MCT USE ONLY. STUDENT USE PROHIBITED

Data Box

Data Box

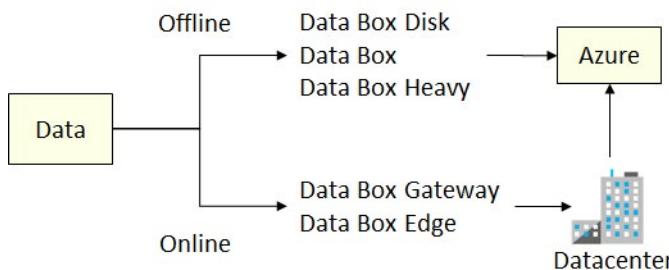
Move stored or in-flight data to Azure quickly and cost-effectively: Data Box offline devices easily move data to Azure when busy networks aren't an option. Data Box online appliances transfer data to and from Azure over the network.

Try 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. 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.

Try 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.



Offline data transfer Data Box

Data Box offers a few offline data transfer products:

- Data Box.
- Data Box Disk.
- Data Box Heavy.

Online data transfer

For online data transfer, there are two primary Data Box options:

- Data Box Edge.
- Data Box Gateway.

For more information:

Azure Data Box Products - <https://azure.microsoft.com/en-us/services/storage/databox/>

Azure Data Box - <https://docs.microsoft.com/en-us/azure/databox-family/>

Offline – Use Cases

There are many scenarios where **offline** Data Box products can be used.

One-time migration. When large amounts of on-premises data is moved to Azure. Examples include:

- 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.

Incremental transfer. After an initial bulk transfer, moving new data. For example, backup solutions partners such as Commvault and Data Box are used to move initial large historical backup to Azure. Once complete, the incremental data is transferred via network to Azure storage.

Periodic uploads. When a large amount of data is generated periodically and needs to be moved to Azure. For example, in energy exploration, where video content is generated on oil rigs and windmill farms.

For more information:

Video -Case Study: Azure Data Box | Oceaneering Intl - <https://www.youtube.com/watch?v=y0nGRH-w3Zqc>

Offline - Data Box Products

Data is being generated at record levels, and moving stored or in-flight data to the cloud can be challenging. Azure Data Box products provide both offline and online solutions for moving your data to the cloud. In this topic we will concentrate on the offline data products.



Data Box



Data Box Disk



Data Box Heavy

Offline solutions transfer large amounts of data to Azure where there is limited or no network bandwidth.

Data Box

- 100 TB total capacity per order
- 80 TB usable capacity per order
- One device per order
- Supports Azure Blob or Files
- Copy data to 10 storage accounts
- 1x1/10 Gbps RJ45, 2x10 Gbps SFP+ interface
- Uses AES 256-bit encryption
- Copy data using standard NAS protocols (SMB/NFS)

Data Box Disk

- 40 TB total capacity per order
- 35 TB usable capacity per order
- Up to five disks per order
- Supports Azure Blob
- Copy data to one storage account
- USB/SATA II, III interface
- Uses AES 128-bit encryption
- Copy data using Robocopy or similar tools

Data Box Heavy (Preview)

- 1 PB total capacity per order
- 800 TB usable capacity per order
- One device per order
- Supports Azure Blob or Files
- Copy data to 10 storage accounts
- 1x1/10 Gbps RJ45, 4x40 Gbps QSFP+ interface
- Uses AES 256-bit encryption
- Copy data using standard NAS protocols (SMB/NFS)

Offline - Product Selection

Data Box is designed to move large amounts of data to Azure with no impact to the network. When selecting an offline product consider speed and security.

Speed. 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.

Product	Network Interfaces
Data Box Disk	USB 3.0 connection
Data Box	1 Gbps or 10 Gbps network interfaces
Data Box Heavy	High performance 40 Gbps network interfaces

Security. All products can only be unlocked with a password provided in the Azure portal. All services are protected by Azure security features. Ensure your selection meets your organization's security requirements.

Product	Physical security	Encryption
Data Box Disk	The disks are tamper-resistant and support secure update capability.	The data is secured with AES 128-bit encryption.
Data Box	Rugged device casing secured by tamper-resistant screws and tamper-evident stickers.	The data is secured with AES 256-bit encryption.

Product	Physical security	Encryption
Data Box Heavy	Rugged device casing secured by tamper-resistant screws and tamper-evident stickers.	The data is secured with AES 256-bit encryption.

- ✓ Once your data is uploaded to Azure, the disks on the device are wiped clean, in accordance with NIST 800-88r1 standards.

Offline - Implementation Offline Products

The implementation workflow is the same for Data Box, Data Box Disk, and Data Box Heavy.

1. **Order**². Create an order in the Azure portal, provide shipping information, and the destination Azure storage account for your data. If the device is available, Azure prepares and ships the device with a shipment tracking ID.
 2. **Receive, unpack, connect, and unlock**³. Once the device is delivered, cable the device for network and power using the specified cables. Turn on and connect to the device. Configure the device network and mount shares on the host computer from where you want to copy the data.
 3. **Copy and validate the data**⁴. Copy data to Data Box shares.
 4. **Return, upload, verify**⁵. Prepare, turn off, and ship the device back to the Azure datacenter. Data is automatically copied from the device to Azure. The device disks are securely erased as per the National Institute of Standards and Technology (NIST) guidelines.
- ✓ Take a few minutes to review each link. The links are for Data Box, there are similar pages for Data Box Disk and Data Box Heavy.
 - ✓ Throughout this process, you are notified via email on all status changes.

Online - Data Box Gateway



Data Box Gateway

- Virtual device provisioned in your hypervisor
- Supports storage gateway, SMB, NFS, Azure blob, files
- Virtual network transfer appliance (VM), runs on your choice of hardware

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.

² <https://docs.microsoft.com/en-us/azure/databox/data-box-deploy-ordered>

³ <https://docs.microsoft.com/en-us/azure/databox/data-box-deploy-set-up>

⁴ <https://docs.microsoft.com/en-us/azure/databox/data-box-deploy-copy-data>

⁵ <https://docs.microsoft.com/en-us/azure/databox/data-box-deploy-picked-up>

Use cases

- **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.

Benefits

- **Easy data transfer.** Makes it easy to move data in and out of Azure storage as easy as working with a local network share.
- **High speed performance.** Takes the hassle out of network data transport with high-performance transfers to and from Azure.
- **Fast access.** Caches most recent files for fast access of on-premises files.
- **Limited bandwidth usage.** Data can be written to Azure even when the network is throttled to limit usage during peak business hours.

Features

- Virtual device provisioned in your hypervisor
- Storage gateway
- Supports SMB or NFS protocols
- Supports Azure Blob or Files
- Supports Hyper-V or VMware

Online - Data Box Edge



Data Box Edge

- Local Cache Capacity: ~12TB
- Includes Data Box Gateway and Azure IoT Edge
- Data Box Edge manages upload to Azure and can pre-process data prior to upload.

Data Box Edge

This 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

- **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. Preprocessing can be used to:

- Aggregate data.
- Modify data, for example to remove Personally Identifiable Information (PII).
- Subset and transfer the data needed for deeper analytics in the cloud.
- Analyze and react to IoT Events.
- **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.

Benefits

- **Easy data transfer.** Makes moving data in and out of Azure storage as easy as working with a local network share.
- **High speed performance.** Enables high-performance transfers to and from Azure.
- **Fast access.** Caches most recent files for fast access of on-premises files.
- **Limited bandwidth usage.** Data can be written to Azure even when the network is throttled to limit usage during peak business hours.
- **Transform data.** Enables analysis, processing, or filtering of data as it moves to Azure.

Features

- AI-enabled edge compute
- Physical device shipped by Microsoft
- Storage gateway
- Supports SMB or NFS protocols
- Supports Azure Blob or Files
- 1U chassis, 2x10 core CPU, 64 GB RAM
- 12 TB local NVMe SSD storage
- 4x25 GbE network interfaces

Online – Implementation Online Products

The following steps outline the workflow for using Data Box Gateway:

1. **Prepare. Create and configure your Data Box Gateway resource prior to provisioning a Data Box Gateway virtual device⁶.** This includes: checking prerequisites, creating a new Data Box Gateway in the portal, downloading the virtual device image for Hyper-V or VMware, and obtaining the activation key. This key is used to activate and connect your Data Box Gateway device with the resource.
2. **Provision.** For **Hyper-V⁷**, provision and connect to a Data Box Gateway virtual device on a host system running Hyper-V on Windows Server 2016 or Windows Server 2012 R2. For **VMware⁸**, provi-

⁶ <https://docs.microsoft.com/en-us/azure/databox-online/data-box-gateway-deploy-prep>

⁷ <https://docs.microsoft.com/en-us/azure/databox-online/data-box-gateway-deploy-provision-hyperv>

⁸ <https://docs.microsoft.com/en-us/azure/databox-online/data-box-gateway-deploy-provision-vmware>

sion and connect to a Data Box Gateway virtual device on a host system running VMware ESXi 6.0 or 6.5. For both hypervisors you will: verify requirements, provision the device, start the device, and get the IP address.

3. **Connect, setup, and activate.** (<https://docs.microsoft.com/en-us/azure/databox-online/data-box-gateway-deploy-connect-setup-activate>). Connect to the local web UI setup page. Provide the device name and activation key. The Network settings, Web proxy settings, and Time settings are optional.
4. **Add, connect to the share.** (<https://docs.microsoft.com/en-us/azure/databox-online/data-box-gateway-deploy-add-shares>). Your share can be SMB or NFS. There are settings for both in the portal. Once the share is created you can connect and begin transferring data.
 - ✓ Be sure to view the documentation for each step.
 - ✓ The steps for Data Box Edge are the same with the addition of the IoT device.

For more information:

Tutorial: Prepare to deploy Azure Data Box Edge - <https://docs.microsoft.com/en-us/azure/databox-online/data-box-edge-deploy-prep>

Lab and Review Questions

Lab - Azure File Sync

Scenario

Adatum Corporation hosts its file shares in on-premises file servers. Considering its plans to migrate majority of its workloads to Azure, Adatum is looking for the most efficient method to replicate its data to file shares that will be available in Azure. To implement it, Adatum will use Azure File Sync.

Objectives

After completing this lab, you will be able to:

- Deploy an Azure VM by using an Azure Resource Manager template.
- Prepare Azure File Sync infrastructure.
- Implement and validate Azure File Sync.

Exercise 0: Prepare the lab environment

The main task for this exercise is as follows:

- Deploy an Azure VM by using an Azure Resource Manager template

Result: After you completed this exercise, you have initiated a template deployment of an Azure VM az1000201b-vm1 that you will use in the next exercise of this lab.

Exercise 1: Prepare Azure File Sync infrastructure

The main tasks for this exercise are as follows:

- Create an Azure Storage account and a file share.
- Prepare Windows Server 2016 for use with Azure File Sync.
- Run Azure File Sync evaluation tool.

Result: After you completed this exercise, you have created an Azure Storage account and a file share, prepare Windows Server 2016 for use with Azure File Sync, and run Azure File Sync evaluation tool

Exercise 2: Implement Azure File Sync

The main tasks for this exercise are as follows:

- Deploy the Storage Sync Service.
- Install the Azure File Sync Agent.
- Register the Windows Server with Storage Sync Service.
- Create sync groups and a cloud endpoint.
- Create a server endpoint.
- Validate Azure File Sync operations.

Result: After you completed this exercise, you have deployed the Storage Sync Service, installed the Azure File Sync Agent, registered the Windows Server with Storage Sync Service, created a sync group and a cloud endpoint, created a server endpoint, and validated Azure File Sync operations.

Module Review Questions

Review Question 1

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 2

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 3

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

Review Question 4

You need to improve the content delivery performance of a specific Azure blob using Azure Content Delivery Network (CDN), specifically the time-to-live (TTL) of the blob. What should you configure? Select one.

- The blob's LeaseDuration property
- The cacheControlMaxAge property in the web.config file
- The clientCache section in the web.config file
- The blob's CacheControl property

Review Question 5

You are planning to use the Import/Export service. Which of the following is not true. Select one.

- Windows Servers must have a 64-bit OS that supports BitLocker Drive Encryption
- Windows clients must have .NET Framework 4.5.1 and BitLocker
- General Purpose v2 storage accounts are recommended for most scenarios
- Solid-state drives are required

Review Question 6

Your organization is using CDN. The content you are delivering changes frequently and you need to ensure the latest content is provided to the user. What should you do? Select one.

- Configure the Cache Expiration Duration setting
- Configure the Caching Behaviour setting
- Configure the Query String Caching Behaviour setting
- Configure a matching rule with a TTL value

Review Question 7

Your organization wants to ensure frequently accessed files are cached locally on the server while all other files are cached to Azure Files based on policy settings. What should you do? Select one.

- Configure file synchronization settings
- Configure file archiving settings
- Configure file time-to-live settings
- Configure cloud tiering

Review Question 8

Before using Azure File Sync you decide to use the Azure File Sync evaluation tool. The tool does many things, except which of the following? Select one.

- Checks for unsupported characters
- Checks for unsupported OS versions
- Checks for storage space.
- Uses an Azure PowerShell cmdlet.

Answers

Review Question 1

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 2

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 Edge. This product is an offline solution which meets the limited bandwidth requirements. The product is designed for scenarios where there is more than 500 TBs that needs to be moved to Azure. Security logs and encryption are built-in.

Review Question 3

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.

Review Question 4

You need to improve the content delivery performance of a specific Azure blob using Azure Content Delivery Network (CDN), specifically the time-to-live (TTL) of the blob. What should you configure? Select one.

- The blob's LeaseDuration property
- The cacheControlMaxAge property in the web.config file
- The clientCache section in the web.config file
- The blob's CacheControl property

Explanation

Configure the CacheControl property of the blob as that property determines the TTL. You should not use the web.config file to configure the TTL as the web.config file is used to manage a web application, and in this case you need to configure the TTL on a blob, not on a web application. The LeaseDuration property is not used to manage the TTL, instead it's used to manage the locks when accessing a blob.

Review Question 5

You are planning to use the Import/Export service. Which of the following is not true. Select one.

- Windows Servers must have a 64-bit OS that supports BitLocker Drive Encryption
- Windows clients must have .NET Framework 4.5.1 and BitLocker
- General Purpose v2 storage accounts are recommended for most scenarios
- Solid-state drives are required

Explanation

Solid state drives (SSDs) are not required. You can ship SSDs or Hard disk drives (HDDs) to the Azure datacenter.

Review Question 6

Your organization is using CDN. The content you are delivering changes frequently and you need to ensure the latest content is provided to the user. What should you do? Select one.

- Configure the Cache Expiration Duration setting
- Configure the Caching Behaviour setting
- Configure the Query String Caching Behaviour setting
- Configure a matching rule with a TTL value

Explanation

Cache Expiration Setting. Any publicly accessible blob content can be cached in Azure CDN until its time-to-live (TTL) elapses. The TTL is determined by Cache-directive headers in the HTTP response from the origin server. If the Cache-Control header does not provide the TTL information, or if you prefer, you can configure caching rules to set the Cache Expiration Duration.

Review Question 7

Your organization wants to ensure frequently accessed files are cached locally on the server while all other files are cached to Azure Files based on policy settings. What should you do? Select one.

- Configure file synchronization settings
- Configure file archiving settings
- Configure file time-to-live settings
- Configure cloud tiering

Explanation

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.

Review Question 8

Before using Azure File Sync you decide to use the Azure File Sync evaluation tool. The tool does many things, except which of the following? Select one.

- Checks for unsupported characters
- Checks for unsupported OS versions
- Checks for storage space.
- Uses an Azure PowerShell cmdlet.

Explanation

Before deploying Azure File Sync, you should evaluate whether it is compatible with your system using the Azure File Sync tool. This tool is an Azure PowerShell cmdlet that checks for potential issues with your file system and dataset, such as unsupported characters or an unsupported OS version.